0.1 Curvas elípticas

En esta sección repasamos algunas definiciones y resultados que vamos a requerir acerca de las curvas elítpicas. No demostramos todas las propiedades para mantener esta sección breve, pero habrá referencias para las pruebas omitidas.

0.1.1 Definiciones preliminares

Definición 1. Una *curva elíptica* $E = (E, O)$ es una curva proyectiva suave de género 1 con un punto distinguido $O \in E$. Decimos que E *está definido sobre* un campo K, si E está definido sobre K como variedad proyectiva; esto lo denotamos por E/K. Una función no constante $\varphi : E \to E'$ entre curvas elípticas sobre K es una *isogenia* si φ es un morfismo de variedades sobre K tal que $\varphi(O) = O'$.

A cada curva elíptica se le puede asociar una ecuación de la forma

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

donde, si E está definido sobre K, $a_i \in K$. De hecho, la homogenización de esta ecuación es el polinomio que define la imagen de E bajo un encaje $E \hookrightarrow \mathbb{P}^2(K)^*$, es decir E se puede encajar como una curva cúbica suave en $\mathbb{P}^2(K)$ con ecuación

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Si la característica de K es distinto de 2 o 3, entonces hay un cambio de coordenadas que cambia la ecuación de Weierstrass a la siguiente forma:

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

Definición 2. Sea E una curva elíptica sobre K. El *discriminante* (denotado por Δ) y el *j-invariante* (denotado por $j(E)$) de la curva E se definen como:

$$\Delta = -16(4A^3 + 27B^2) \qquad j(E) = -1728\frac{64A^3}{\Delta}.$$

El j-invariante obtiene su nombre gracias al siguiente teorema importante:

Teorema 1. *Sean E y E' curvas elípticas definidas sobre un campo K algebraicamente cerrado. Entonces*

$$E \cong E' \quad \iff \quad j(E) = j(E').$$

(cf. [**?**, §3.1, proposición 1.4] o [**?**, capítulo IV, teorema 4.1] para una prueba usando herramientas de geometría algebraica)

Los puntos de E forman un grupo abeliano (cf. [**?**, §3.2]). La operación se define de la siguiente manera: sean $P, Q \in E$ y tomamos la recta $L \subset \mathbb{P}^2$ que une ambos puntos (o la recta tangente si $P = Q$). Como la ecuación de E es cúbica, L interseta a E en exactamente tres puntos (en dos puntos distintos cuando $P = Q$) P, Q y un tercer punto $R \in E$; esto se sigue del famoso teorema

*El espacio proyectivo de dimensión n sobre K se define como el espacio cociente $(K^{n+1} - \{0\})/K^*$ donde la acción $K^* \curvearrowright (K^{n+1} - \{0\})$ es por multiplicación escalar $(\lambda, v) \mapsto \lambda v$.

de Bezout. Ahora toma $L' \subset \mathbb{P}^2$ como la recta que une R y O. Otra vez existe un tercer punto sobre $L' \cap E$ y este lo definimos como $P + Q$.

El neutro de la operación es $O \in E$. Esta definición es exclusivamente geométrico y por eso es difícil probar que esta operación es una operación de grupo; la asociatividad es particularmente difícil. Lo bueno de esta definición es que se puede generalizar fácilmente a curvas elípticas definidas sobre cualquier campo K.

Otra manera de definir la suma de E es con divisores:

Definición 3. Un *divisor* D de E es un elemento del grupo libre abeliano generado por los puntos de E, es decir D es una suma formal de la forma:

$$D = \sum_{P \in E} n_p(P)$$

donde $n_P \in \mathbb{Z}$ y $n_P = 0$ para casi toda $P \in E$. Aquí estamos escribiendo (P) como el divisor asociado al punto P (i.e. donde $n_Q = 0$ para toda $Q \neq P$ y $n_P = 1$). Al conjunto de todos los divisores de E lo denotamos $\mathrm{Div}(E)$.

Por ejemplo, si f es una función racional de E, es decir un elemento de $K(E)$ distinto de cero, entonces podemos definir un divisor:

$$\mathrm{div}(f) := \sum_{P \in E} \nu_P(f)(P)$$

donde ν_P es la valoración asociada a $K[E]_P$, la localización de $K[E]$ (el anillo de coordenadas de E) en el ideal maximal $\mathfrak{m}_P = \{f \in K[E] \mid f(P) = 0\}$. Recuerda que como E es suave, $K[E]_P$ es un anillo de valoración discreto.[†] De esta manera, para un $f \in K[E]_P$ la valoración $\nu_P(f)$ se define como el único entero n tal que $f \in \mathfrak{m}_P^n$ pero $f \notin \mathfrak{m}_P^{n+1}$.

Definición 4. Un divisor D de E es *principal* si existe una función racional $f \in K(E)$ distinto de cero tal que $D = \mathrm{div}(f)$. Además hay una relación de equivalencia sobre $\mathrm{Div}(E)$: decimos que D y D' son *linealmente equivalentes*, i.e. $D \sim D'$, si $D - D'$ es un divisor principal. El conjunto de clases de equivalencia es un grupo abeliano, se llama el *grupo de Picard* de E y se denota por $\mathrm{Pic}(E)$.

Observa que el conjunto de divisores principales es un subgrupo de $\mathrm{Div}(E)$ y $\mathrm{Pic}(E)$ es el grupo cociente con el subgrupo de divisores principales. Enunciamos una caracterización de ser divisor principal:

Proposición 1. *Sea E una curva elíptica y $D = \sum n_P(P)$ un divisor de E. Entonces D es principal si y solo si $\sum n_P = 0$ y $\sum [n_p]P = O$ (la segunda suma es en E).*

(cf. [**?**, capítulo III, §3, corolario 3.5])

Ahora regresamos a la operación algebraica de E. Para $P, Q \in E$ se puede probar que $P + Q$ es el único punto $R \in E$ tal que $(P) + (Q) \sim (R) + (O)$.

[†]Por definición, un punto x en una variedad X es no-singular si el anillo local $\mathcal{O}_{x,X}$ es un anillo *regular* (i.e. el $(\mathcal{O}_{x,X}/\mathfrak{m}_{x,X})$-espacio vectorial $\mathfrak{m}_{x,X}/\mathfrak{m}_{x,X}^2$ es de dimensión $\dim(\mathcal{O}_{x,X})$). Como las curvas elípticas son de dimensión 1, ser regular es equivalente a ser un anillo de valoración discreta (cf. [**?**, §9,proposición 9.2]).

Como E es un grupo abeliano, E es un $\mathbb{Z}$-módulo, es decir hay multiplicación por $N \in \mathbb{Z}$. Más precisamente, existen los morfismos de multiplicación:

$$[N] : E \longrightarrow E \quad \text{definido por} \quad [N]P = \underbrace{P + \cdots + P}_{N \text{ veces}} \quad (N > 0).$$

Si $N < 0$ definimos $[N]P := -\big([|N|]P\big)$ y si $N = 0$ definimos $[0]P = O$. La múltiplicación por $N \in \mathbb{Z}$ nos permite estudiar el grupo de torsión de E.

Definición 5. Al subgrupo de elementos de E/K de orden N lo denotamos por:

$$E[N] = \ker[N] = \{P \in E(K) \mid [N]P = O\}.$$

El grupo de torsión de E es simplemente la unión de todas las $E[n]$. De la misma manera, definimos

$$E[N](\overline{K}) = \{P \in E(\overline{K}) \mid [N]P = O\}.$$

La estructura de $E[N]$ es relativamente sencilla:

Proposición 2. *Sea E una curva elíptica sobre K y sea $c = \mathrm{char}(K)$, entonces:*

$$E[N] \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}$$

si $c = 0$ o si $c \nmid N$ cuando $c > 0$.

Proof. Nada más probamos el caso cuando $K \subseteq \mathbb{C}$. Por el teorema de uniformización (teorema 3), existe una latiz tal que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ pero este cociente es isomorfo a $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. Por lo tanto $E[N]$ es un subgrupo de $E[N](\mathbb{C}) = \{P \in E(\mathbb{C}) \mid [N]P = O\}$ que a su vez es un subgrupo (cuyos elementos son de orden N) de $\mathbb{R}/\mathbb{Z}\times\mathbb{R}/\mathbb{Z}$. El único subgrupo que cumple esto es $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$. □

En particular, si ℓ es un número primo, entonces $[\ell] : E \to E$ se restringe a un morfismo de grupos $[\ell] : E[\ell^{m+1}] \to E[\ell^m]$ para toda $m > 1$. La familia de morfismos

$$\cdots \longrightarrow E[\ell^{m+2}] \xrightarrow{[\ell]} E[\ell^{m+1}] \xrightarrow{[\ell]} E[\ell^m] \xrightarrow{[\ell]} \cdots \xrightarrow{[\ell]} E[\ell]$$

es un sistema inverso. Por lo tanto existe su límite inverso:

Definición 6. Sea E/K una curva elíptica y ℓ un número primo distinto de la característica de K. El *módulo de Tate ℓ-ádico* de E se define como:

$$T_\ell(E) = \varprojlim_m E[\ell^m]$$

Observa que $\mathbb{Z}_\ell$, los enteros ℓ-ádicos, son el límite inverso de los cocientes $\mathbb{Z}/\ell^m\mathbb{Z}$, entonces:

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \quad (\mathrm{char}(K) \neq \ell).$$

En particular $T_\ell(E)$ es un $\mathbb{Z}_\ell-$módulo libre de rango 2. Si elegimos una $\mathbb{Z}_\ell$-base, entonces todos los $v \in T_\ell(E)$ se pueden expresar como $v = (v_1, v_2) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Entonces el determinante $\det : T_\ell(E) \times T_\ell(E) \to \mathbb{Z}_\ell$, definido por

$$\det(v, v') := \det \begin{pmatrix} v_1 & v_1' \\ v_2 & v_2' \end{pmatrix} = v_1 v_2' - v_1' v_2$$

es una función bilineal no-degenerada y alternante sobre el módulo de Tate (y es independiente de la elección de la $\mathbb{Z}_\ell-$base). Hay otra función bilineal no-degenerada alternante sobre $T_\ell(E)$ que resulta más útil que el determinante: el emparejamiento de Weil. Para poder definirlo, necesitamos regresar a $E[m]$, construir ahí el emparejamiento de Weil y después pasar al límite inverso.

Sean $P, Q \in E[m]$ (donde posiblemente $P = Q$). Elige $g \in \overline{K}(E)$ tal que:

$$\operatorname{div}(g) = [m]^*(Q) - [m]^*(O)$$

donde

$$[m]^* : \operatorname{Div}(E) \to \operatorname{Div}(E) \quad \text{se define en generadores como} \quad (R) \mapsto \sum_{S \in [m]^{-1}(R)} e_{[m]}(S)(S)$$

donde $e_{[m]}(R)$ es el índice de ramificación de $[m] : E \to E$ en $R \in E$. Con esto definimos el emparejamiento de Weil como:

$$e_m : E[m] \times E[m] \to \mu_m \quad \text{definido por} \quad e_m(P, Q) = \frac{g(X + P)}{g(X)}$$

donde $\mu_m \subset \mathbb{C}$ es el grupo de raices m-ésimas de la unidad y $X \in E$ es un punto elegido de tal manera que g está bien definido en $X+P$ y en X. La función e_m está bien definida y no depende de la elección de g ni de X (cf. [**?**, capítulo III, §8]). La función e_m cumple las siguientes propiedades:

Proposición 3. *El emparejamiento de Weil e_m es una función bilineal, alternante, no-degenerada, invariante bajo la acción del grupo de Galois* $\operatorname{Gal}(\overline{K}|K)$ *y cumple:*

$$e_{mm'}(P, Q) = e_m\big([m']P, Q\big) \tag{1}$$

cf. [**?**, capítulo III, proposición 8.1]).

Ahora fijamos un primo ℓ (distinto de la característica de K). Recuerde que los grupos μ_{ℓ^n}, junto con los morfismos $\mu_{\ell^{n+1}} \to \mu_{\ell^n}$ (definidos por $\zeta \mapsto \zeta^\ell$) forman un sistema inverso: definimos

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}.$$

Para ver que podemos tomar límites inversos de ambos lados de $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$, debemos probar que el diagrama

$$\begin{array}{ccc} E[\ell^{n+1}] \times E[\ell^{n+1}] & \xrightarrow{[\ell]\times[\ell]} & E[\ell^n] \times E[\ell^n] \\ \Big\downarrow{\scriptstyle e_{\ell^{n+1}}} & & \Big\downarrow{\scriptstyle e_{\ell^n}} \\ \mu_{\ell^{n+1}} & \xrightarrow[\hat{}\ell]{} & \mu_{\ell^n} \end{array}$$

es conmutativo: sean $P, Q \in E[\ell^{n+1}]$, entonces

$$\big(e_{\ell^{n+1}}(P, Q)\big)^\ell = e_{\ell^{n+1}}(P, [\ell]Q) = e_{\ell^n}([\ell]P, [\ell]Q),$$

donde la primera igualdad es por la linealidad en la segunda variable (escrita multiplicativamente) y la segunda igualdad es por la fórmula (1); esto prueba la conmutatividad del diagrama anterior.

Por lo tanto e_{ℓ^n} pasa al límite y obtenemos una función:

$$e_\ell : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

que hereda las propiedades de las e_{ℓ^n}, es decir e_ℓ es bilineal, no-degenerada, alternante e invariante bajo la acción del grupo de Galois G_K.

La ventaja de usar módulos de Tate y el aparejamiento de Weil, es que podemos calcular los grados de una isogenia. Sea $\varphi : E \to E$ una isogenia. Como φ es además un homomorfismo de grupos, induce un homomorfismo $\varphi_{\ell^n} : E[\ell^n] \to E[\ell^n]$ y pasando al límite inverso obtenemos una función $\mathbb{Z}_\ell$ lineal $\varphi_\ell : T_\ell(E) \to T_\ell(E)$. En general tenemos una función $\mathrm{End}(E) \to \mathrm{End}(T_\ell(E))$. Con esta notación tenemos:

Proposición 4. *Sea $\varphi \in \mathrm{End}(E)$ y $\varphi_\ell \in \mathrm{End}(T_\ell(E))$ el morfismo inducido, entonces*

$$\det \varphi_\ell = \deg \varphi \quad \text{y} \quad \mathrm{tr}\varphi_\ell = 1 + \deg \varphi - \deg(1 - \varphi)$$

Proof. cf. [**?**, capítulo III, §8, proposición 8.6] □

0.1.2 Curvas elípticas sobre $\mathbb{C}$

En el caso "geométrico" ($K = \mathbb{C}$), las curvas elípticas también se pueden describir usando latices. Un subgrupo aditivo $\Lambda \subset \mathbb{C}$ es una *retícula* si $\Lambda \cong \mathbb{Z}z_1 + \mathbb{Z}z_2$ donde z_1 y z_2 son $\mathbb{R}$-linealmente independiente o equivalentement $\mathrm{Im}\,(z_1/z_2) \neq 0$. El cociente $\mathbb{C}/\Lambda$ es una superficie de Riemann compacta y como es de esperar, el anillo de funciones meromorfas sobre $\mathbb{C}/\Lambda$ nos dice mucho sobre su estructura como variedad. Recuerda que como grupo aditivos:

$$\frac{\mathbb{C}}{\Lambda} \cong \frac{\mathbb{R} \oplus \mathbb{R}}{\mathbb{Z} \oplus \mathbb{Z}} \cong \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}}$$

Definición 7. Una función meromorfa $f : \mathbb{C} \to \mathbb{C}$ es *elíptica* (con respecto de Λ) si es Λ-periódica, es decir

$$f(z + \lambda) = f(z) \qquad \forall \lambda \in \Lambda$$

Al conjunto de funciones elípticas lo denotamos $\mathbb{C}(\Lambda)$. Observa que una función elíptica define una función meromorfa sobre $\mathbb{C}/\Lambda$

La función elíptica más importante para clasificar curvas elípticas con latices es la función $\wp$ de Weierstrass (asociada a Λ) definida por:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

La función $\wp$ de Weierstrass es una función meromorfa cuyos polos (todos de residuo 0) son exactamente de los puntos de la retícula (cf. [**?**, §1.6, teorema 1.10] o [**?**, capítulo 7, §3]). Por lo tanto induce una función meromorfa sobre $\mathbb{C}/\Lambda$.

La importancia de $\wp$ es que, junto con su derivada, genera a todas las funciones elípticas. Más precisamente, si escibimos $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ como la $\mathbb{C}$-subálgebra de $\mathbb{C}(\Lambda)$ generada por $\wp_\Lambda$ y su derivada $\wp_\Lambda$, entonces tenemos que:

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda),$$

(cf. [**?**, capítlo VI, teorema 3.2]).

Además $\wp := \wp_\Lambda$ satisface la ecuación diferencial

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

donde $g_2 = g_2(\Lambda)$ y $g_3 = g_3(\Lambda)$ son complejos que dependen de la retícula Λ. Esta ecuación polinomial se parece a la fórmula de Weierstrass simplificada; esto no es una coincidencia:

Teorema 2. *Sea $\Lambda \subset \mathbb{C}$ una retícula y sean $g_2 = g_2(\Lambda)$ y $g_3 = g_3(\Lambda)$ los coeficientes de la ecuación diferencial que cumple $\wp_\Lambda$. Entonces la curva $E/\mathbb{C}$ definida por $y^2 = 4x^3 - g_2x - g3$ es elíptica (i.e. suave) y $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ como variedades complejas bajo la función*

$$z + \Lambda \mapsto [\wp_\Lambda(z), \wp'_\Lambda(z), 1] \in \mathbb{P}^2(\mathbb{C})$$

*donde estamos identificando a $E(\mathbb{Q})$ con su encaje en $\mathbb{P}^2(\mathbb{C})$. (cf. [**?**, capítulo VI, proposición 3.6])*

Este teorema le asocia a cada retícula Λ una curva elíptica $E/\mathbb{C}$. El resultado inverso es el teorema de uniformización:

Teorema 3. *Sean $A, B \in \mathbb{C}$ tales que $4A^3 - 27B^2 \neq 0$, entonces existe una retícula $\Lambda \subset \mathbb{C}$ tal que $g_2(\Lambda) = A$ y $g_3(\Lambda) = B$. En particular para cada curva elíptica $E : y^2 = x^3 + Ax + B$ existe una retícula Λ tal que $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ como variedades complejas.*

Los isomorfismos en los teoremas 2 y 3 también son homomorfismos de grupo (i.e. de grupos de Lie)

0.1.3 Curvas elípticas sobre campos finitos

Para esta sección fijamos un número primo impar p y fijamos una potencia $q = p^n$ de p. De manera usual, denotamos al campo de Galois de orden q por $\mathbb{F}_q$. También fijamos una curva elíptica E definida sobre $\mathbb{F}_q$. Vamos a estar interesados en calcular la cantidad de puntos en $E(\mathbb{F}_q)$.

Un resultado famoso, debido a Hasse, dice que $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$ (cf. [**?**, capítulo V, teorema 1.1]). En esta sección calcularemos $\#E(\mathbb{F}_q)$ usando la traza del mapeo de Frobenius que está definido para cualquier curva elíptica sobre un campo finito.

El mapeo de Frobenius usual $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, definido por $x \mapsto x^q$, induce un automorfismo de E (que denotamos igual) definido en coordenadas afines por $P = (x, y) \mapsto (x^q, y^q)$. Con esto tenemos:

Teorema 4. *Sea $E/\mathbb{F}_q$ una curva elíptica, $\varphi : E \to E$ el mapeo de Frobenius de orden q y escribe $a_q(E) := q + 1 - \#E(\mathbb{F}_q)$. Entonces el morfismo inducido $\varphi_\ell : T_\ell(E) \to T_\ell(E)$ en los módulos de Tate ($\ell \neq p$) tiene polinomio característico $T^2 - a_q(E)T + q$. En particular el mapeo de Frobenius satisface $\varphi^2 - a_q(E)\varphi + q = 0 \in \mathrm{End}(E)$.*

Proof. Como el grupo absoluto de Galois $G_{\mathbb{F}_q}$ es generado topológicamente por el mapeo de Frobenius de orden q sobre $\overline{\mathbb{F}}_q$, entonces $P \in E(\mathbb{F}_q)$ si y solamente si $\varphi(P) = \varphi(x, y) = (x^q, y^q) = (x, y) = P$ o equivalentemente $E(\mathbb{F}_q) = \ker(1 - \varphi)$.

Ahora como $p \nmid 1$, la isogenia $1 - \varphi$ es separable (cf. [**?**, capítulo III, corolario 5.5]) y las isogenias separables cumplen que $\#\ker\varphi = \deg\varphi$ (cf. [**?**, capítulo III, teorema 4.10.c]), tenemos que

$$\#E(\mathbb{F}_q) = \#\ker(1 - \varphi) = \deg(1 - \varphi). \tag{2}$$

Nota. Como $\deg\varphi = q$ y $\deg : \mathrm{End}(E) \to \mathbb{Z}$ es una forma cuadrática positiva definida, la desigualdad de Hasse mencionada anteriormente se sigue de la fórmula anterior después de aplicar una versión adecuada de la desigualdad de Cauchy-Schwarz para deg.

Luego aplicamos la proposición 4 a 2 y tenemos que $\det\varphi_\ell = \deg\varphi = q$ y

$$\mathrm{tr}\varphi_\ell = 1 + \deg\varphi - \deg(1-\varphi) = 1 + q - \#E(\mathbb{F}_q) = a_q(E).$$

Por lo tanto el polinomio característico de φ_ℓ es $T^2 - a_q(E)T + q$.

Por el teorema de Cayley-Hamilton, $\varphi_\ell^2 - a_q(E)\varphi_\ell + q = 0$. Volvemos a aplicar la proposición 4 para concluir que:

$$\deg(\varphi^2 - a_q(E)\varphi + q) = \det(\varphi_\ell^2 - a_q(E)\varphi_\ell + q) = 0.$$

La única isogenia de grado cero es $[0] \in \mathrm{End}(E)$ y acabamos. □

Curvas elípticas sobre campos finitas también surgen de curvas elípticas definidas sobre $\mathbb{Q}$ o en general sobre campos locales (i.e. localmente compactos con respecto de una topología no discreta, por ejemplo cualquier extensión finita de $\mathbb{Q}_p$ para algún primo p).

Sea $E/\mathbb{Q}$ una curva elíptica con una ecuación $y^2 = ax^3 + bx^2 + cx + d$ y sea p primo. Entonces bajo el cambio de coordenadas $x = ux' + v$, $y = wy'$ (para algunas $u, v, w \in \mathbb{Q}$) la nueva curva elíptica E' definida por

$$(y')^2 = aw^{-2}(ux'+v)^3 + bw^{-2}(ux'+v)^2 + cw^{-2}(ux'+v) + dw^{-2} = a'(x')^3 + b'(x')^2 + c'x' + d'$$

es isomorfa a E y los números $u, v, w \in \mathbb{Q}$ se pueden tomar de tal manera que los denominadores de los nuevos coeficientes sean primos relativos con p, ie $a', b', c', d' \in \mathbb{Z}_{(p)}$ (la localización de $\mathbb{Z}$ en el ideal primo $p\mathbb{Z}$).

El anillo $\mathbb{Z}_{(p)}$ tiene un morfismo de reducción módulo p:

$$\mathbb{Z}_{(p)} \xrightarrow{\mathrm{mod}\, p} \tfrac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong \tfrac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p.$$

Por lo tanto si tomamos el polinomio $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ que define E (después de un cambio de coordenadas adecuado) podemos aplicar la reducción módulo p a cada coeficiente, i.e. aplicar el morfismo $\mathbb{Z}_{(p)}[x, y] \twoheadrightarrow \mathbb{F}_p[x, y]$ para obtener un polinomio con coeficientes en $\mathbb{F}_p$. En ciertos casos, este procedimiento produce una curva elíptica E_p definida sobre un campo finito. Veamos bajo qué condiciones sucede esto.

Definición 8. Sea $E/\mathbb{Q}$ una cuva elíptica y p un primo impar.

1. E tiene *buena reducción* módulo p si existe un cambio de variable tal que la nueva ecuación que define a E cumple $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ y además $a \in \mathbb{Z}_{(p)}^*$, de tal manera que la curva elíptica $E_p/\mathbb{F}_p$ es suave (o equivalentemente que la ecuación $y^2 = ax^3 + bx^2 + cx + d \pmod p$ tiene tres raices diferentes).

2. E tiene *reducción multiplicativa* módulo p si existe un cambio de variable tal que la nueva ecuación que define a E cumple $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ y además $a \in \mathbb{Z}_{(p)}^*$, de tal manera que la ecuación $y^2 = ax^3 + bx^2 + cx + d \pmod p$ tiene una raiz de multiplicidad dos y otra raiz simple.

3. E tiene *reducción aditiva* módulo p si existe un cambio de variable tal que la nueva ecuación que define a E cumple $y^2 - ax^3 - bx^2 - cx - d \in \mathbb{Z}_{(p)}[x, y]$ y además $a \in \mathbb{Z}^*_{(p)}$, de tal manera que la ecuación $y^2 = ax^3 + bx^2 + cx + d \pmod p$ tiene una raiz de multiplicidad tres.

Decimos que E tiene *reducción mala* si satisface 2 o 3. Si E tiene reducción multiplicativa, decimos que la reducción es *partida* si las direcciones de las tangentes en el nodo son elementos de $\mathbb{F}_p$ y decimos que es *no-partida* en otro caso.

Definición 9. Una curva elíptica $E/\mathbb{Q}$ es semiestable en un primo p si tiene reducción buena en p o reducción multiplicativa partida en p. Decimos que E es *semiestable* si es semiestable en todo primo.

0.1.4 Curvas modulares y espacios moduli

En esta sección definimos la curva $X_0(N)$ y vemos que parametriza ciertas clases de isomorfismo de curvas elípticas. Fijamos $N > 1$.

Sea E una curva elíptica sobre el campo $\mathbb{Q}(x)$ tal que $j(E) = x$. Sea $P \in E$ un punto de orden n y sea $C = \{O, P, 2P, \ldots, (N-1)P\}$ el subgrupo de E generado por P. Toma $K \subset \overline{\mathbb{Q}(x)}$ como el campo fijo del subgrupo $H = \{\sigma \in G_{\mathbb{Q}(x)} \mid \sigma(C) = C\}$.

Como $(G_{\mathbb{Q}(x)} : H) < \infty$ (porque C es finito), entonces K es una extensión finita de $\mathbb{Q}(x)$. En particular es una extensión de $\mathbb{Q}$ finitamente generada. Ahora, si $\overline{\mathbb{Q}} \cap K = \mathbb{Q}$ (estamos identificando a $\overline{\mathbb{Q}}$ con su inclusión en $\overline{K}$) entonces K es una extensión de $\mathbb{Q}$ finitamente generada de grado de trascendencia 1. De esta manera, como la categoría de curvas proyectivas suaves definidas sobre $\mathbb{Q}$ (con morfismos dominantes) y la categoría de extensiones de $\mathbb{Q}$ finitamente generadas de grado de trascendencia 1 (cf. [**?**, §1.6, corolario 6.12]), podemos asociar a K una curva proyectiva suave definida sobre $\mathbb{Q}$ que llamamos $X_0(N)$.

Hay que probar que la elección de $X_0(N)$ está bien definida, es decir que no depende de E ni de el subgrupo $C \subset E$ y además que efectivamente $\overline{\mathbb{Q}} \cap K = \mathbb{Q}$ para que K realmente sea un campo de funciones de una curva. Estas tres proposiciones se siguen del siguiente teorema:

Sea E una curva elíptica sobre $\mathbb{Q}$ y definimos a $\mathbb{Q}(E[N])$ como la extensión de Galois generada por las coordenadas afines de los puntos de $E[N]$. La acción natural $G_{\mathbb{Q}(E[N])} \curvearrowright E[N]$ induce una representación $\rho : G_{\mathbb{Q}(E[N])} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (gracias a la estructura de $E[N]$ dada en la proposición 2).

Teorema 5. *Sea E una curva elíptica definida sobre $k = \mathbb{Q}(x)$ tal que $j(E) = x$. Con la notación del párrafo anterior, la representación ρ es un isomorfismo, es decir:*

$$G_{\mathbb{Q}(x,E[N])} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Además, $\overline{\mathbb{Q}} \cap \mathbb{Q}(x, E[N]) = \mathbb{Q}(\mu_N)$ donde $\mu_N \subset \mathbb{C}$ es el conjunto de las N-ésimas raices de la unidad.

Nota. Este resultado es una versión débil del caso $k = \mathbb{C}(x)$ donde el isomorfismo es $\mathrm{Gal}(\mathbb{Q}(x, E[N]) \mid \mathbb{Q}(x)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ (cf. [**?**, capítulo III, §1, teorema 1 y su corolario])

Ahora explicamos porque la elección $X_0(N)$ está bien definida:

Corolario 6. *La curva elíptica $X_0(N)$ sobre $\mathbb{Q}$ existe y no depende de E ni del subgrupo C.*

Proof. Como mencionamos antes, basta robar que $\overline{\mathbb{Q}} \cap K = \mathbb{Q}$ para que K efectivamente sea una extensión finitamente generada sobre $\mathbb{Q}$ de grado de trascendencia 1. Sea $P \in E$ el generador de C. Observa que $\{P\} \subset E[N]$ se puede extender a una base ordenada de tal manera que el isomorfismo $G_{\mathbb{Q}(x,E[N])} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ del teorema 5 hace que $H' := \{\sigma \in G_{\mathbb{Q}(x,E[N])} \mid \sigma(C) = C\}$ sea isomorfo a las matrices triangulares inferiores, i.e.

$$H \cong \left\{ \begin{pmatrix} a & 0 \\ b & d \end{pmatrix} : a, d \in (\mathbb{Z}/N\mathbb{Z})^*,\ b \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Ahora, la función determinante $\det : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^*$ restringida a H sigue siendo sobre. Por lo tanto $\mathbb{Q}(\mu_N) \cap K = \mathbb{Q}$.... Si sustituimos la igualdad de la segunda parte del teorema 5 en esta fórmula obtenemos:

$$\mathbb{Q} = \left(\overline{\mathbb{Q}} \cap \mathbb{Q}(x, E[N])\right) \cap K = \mathbb{Q}(x, E[N]) \cap \left(\overline{\mathbb{Q}} \cap K\right) = \overline{\mathbb{Q}} \cap K$$

ya que $\overline{\mathbb{Q}} \cap K \subset \mathbb{Q}(x, E[N])$.

Ahora probamos que $X_0(N)$ es independiente de la elección de C. Cambiar de subgrupo C es cambiar de punto P de orden N. Sean $P' \in E$ otro punto de orden N, $C' \subset E[N]$ el subgrupo cíclico generado por P' y H' el subgrupo de $G_{\mathbb{Q}(x,E[N])}$ de fija a C'. De la misma manera extendemos $\{P'\}$ a otra base de $E[N]$. Este cambio de base modifica el isomorfismo $G_{\mathbb{Q}(x,E[N])} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ mediante una conjugación por la matriz de cambio de base. En particular la imagen de H' en $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ es un conjugado de la imagen de H. Por lo tanto existe un $\sigma \in G_{\mathbb{Q}(x,E[N])}$ tal que $H' = \sigma H \sigma^{-1}$. Por lo tanto el campo fijo K' de H' es simplemente $\sigma(K)$, es decir $K \cong K'$. Gracias a la equivalencia de categorías mencionada al principio de la sección, $X_0(N)$ es isomorfo a cualquier curva proyectiva suave con campo de funciones K' y por lo tanto $X_0(N)$ es independiente de la elección de C.

Por último probamos que $X_0(N)$ es independiente de la elección de la curva $E/\mathbb{Q}(x)$.... □

Como consecuencia de este corolario, cada curva proyectiva $X_0(N)$ sobre $\mathbb{Q}$ tiene asociado una curva elíptica $E/\mathbb{Q}(x)$ (con $j(E) = x$) y un subgrupo cíclico $C \subset E$ de orden N tal que el campo de funciones K de $X_0(N)$ es el campo fijo de $H = \{\sigma \in G_{\mathbb{Q}(x)} \mid \sigma(C) = C\}$. La inclusión $\mathbb{Q}(x) \hookrightarrow K$ induce un morfismo de curvas $X_0(N) \to \mathbb{P}^1(\mathbb{Q})$. A un punto en la imagen inversa de $\infty \in \mathbb{P}^1(\mathbb{Q})$ se le llama una *cúspide* de $X_0(N)$.

También podemos considerar a $X_0(N)$ como una curva proyectiva sobre $\mathbb{C}$; en este caso su campo de funciones es $K \otimes_{\mathbb{Q}} \mathbb{C}$. Como en el párrafo anterior, la inclusión $\mathbb{C}(x) \hookrightarrow K \otimes \mathbb{C}$ determina un morfismo $X_0(N)(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. Sea $S \subseteq \mathbb{P}^1(\mathbb{C})$ un subconjunto y S^{c} su complemento en $\mathbb{P}^1(\mathbb{C})$. Denotamos $X_0(N)(\mathbb{C})_S$ como la imagen inversa de S^{c} bajo $X_0(N)(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.

Estamos en posición de estudiar cómo parametriza $X_0(N)$ a algunas curvas elípticas, pero primero debemos definir una categoría nueva. Los objetos son parejas (E, C) donde $E/\mathbb{C}$ es una curva elíptica y $C \subset E$ es un subgrupo cíclico de orden N. Los morfismos $(E, C) \to (E', C')$ son isomorfismos de curvas $\varphi : E \to E'$ tales que $\varphi(C) = C'$. A la clase de isomofismo de (E, C) la denotamos por $[E, C]$ y al conjunto de clases de isomorfismo lo denotamos por $\mathrm{El}_0(N)(\mathbb{C})$. Además, si $S \subseteq \mathbb{P}^1(\mathbb{C})$ entonces escribimos

$$\mathrm{El}_0(N)(\mathbb{C})_S := \{[E, C] \in \mathrm{El}_0(N)(\mathbb{C}) \mid j(E) \notin S\}.$$

Similarmente denotamos por $\mathrm{Toro}_0(N)$ al conjunto de clases de isomorfismo de parejas (T, C) donde T es un toro complejo de dimensión 1 (i.e. $T \cong \mathbb{C}/\Lambda$ para alguna retícula) y $C \subset T$ es un subgrupo cíclico de orden N.

Ahora, sea $x \in X_0(N)(\mathbb{C})$. Como $X_0(N)(\mathbb{C})$ es una curva suave, x determina un anillo de valoración discreta $\mathcal{O}_x \subset K \otimes \mathbb{C}$ con ideal maximal $\mathfrak{m}_x$. Si E tiene buena reducción en $\mathfrak{m}_x$, entonces la reducción módulo $\mathfrak{m}_x$ produce una curva elíptica $E_x/\mathbb{C}$. La restricción de la reducción módulo $\mathfrak{m}_x$ a $E[n] \to E_x[N]$ es inyectiva y así la reducción módulo $\mathfrak{m}_x$ del punto $P \in E[N]$ es un punto $P_x \in E_x[N]$ de orden N que genera un subgrupo cíclico $C_x \subset E_x$ de orden N.

Con estas consideraciones podemos enunciar el resultado más importante de esta sección:

Teorema 7. *Sean $E/\mathbb{Q}(x)$ una curva elíptica tal que $j(E) = x$, $S \subseteq \mathbb{P}^1(\mathbb{C})$ un subconjunto que contiene a todos los lugares donde E tiene mala reducción, $\{Q, P\}$ una $\mathbb{Z}/N\mathbb{Z}$-base de $E[N]$ y $C \subset E$ el subgrupo cíclico generado por P, entonces tenemos el siguiente diagrama conmutativo de funciones biyectivas:*

$$\begin{array}{ccc} X_0(N)(\mathbb{C})_S & \xrightarrow{(i)} & \mathrm{El}_0(N)(\mathbb{C})_S \\ \Big\downarrow{\scriptstyle (ii)} & & \Big\downarrow{\scriptstyle (iv)} \\ \mathbb{H}/\Gamma_0(N) & \xrightarrow[(iii)]{} & \mathrm{Toro}_0(N) \end{array}$$

donde las funciones están dadas por:

i) $x \mapsto [E_x, C_x]$.

ii) *La restricción del isomorfismo $X_0(N)(\mathbb{C}) \cong \mathbb{H}^*/\Gamma_0(N)$ de superficies de Riemann.*

iii) $[z] \mapsto [\mathbb{C}/\Lambda_z, \langle \frac{1}{N} + \Lambda_z \rangle]$ *donde $\Lambda_z := z\mathbb{Z} \oplus \mathbb{Z}$ es una retícula de $\mathbb{C}$.*

iv) $[E, C] \mapsto [E(\mathbb{C}), C]$.

Proof. La prueba de que (i) es biyectiva se sigue de [**?**, capítulo III, §1.3, proposición 1], la biyectividad de (ii) se sigue de [**?**, capítulo III, §1.10, proposición 6], la biyectividad de (iii) se sigue de [**?**, capítulo III, §1.10, proposición 7] y la biyectividad de (iv) se sigue de [**?**, capítulo III, §1.8, proposición 5]. □

Definición 10. Una curva elíptica $E/\mathbb{Q}$ es *modular* si existe una función holomorfa no constante $X_0(N) \to E$ para alguna N.