UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

Aspectos combinatorios de las curvas elípticas

Presentado por:
Carmen Lissette Lovato Panameño

Para optar al grado de:
Licenciada en Matemática

Bajo la dirección de:
Dr. Gabriel Alexander Chicas Reyes

Ciudad Universitaria, Enero 2025

UNIVERSIDAD DE EL SALVADOR

M.Sc. Juan Rosa Quintanilla
Rector

Dra. Evelyn Beatriz Farfán
Virrectora Académica

M.Sc. Roger Arias
Virrector Administrativo

Lic. Pedro Rosalío Escobar Castaneda
Secretario General

Lic. Carlos Amílcar Serrano Rivera
Fiscal General

Licda. Ana Ruth Avelar
Defensora de los Derechos Universitarios

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

Dr. Luis Gilberto Parada Gómez
Decano

Dr. José Nerys Funes Torres
Vicedecano

Licda. Angela Gudelia Portillo de Pérez
Secretaria de Facultad

ESCUELA DE MATEMÁTICA

Dr. Dimas Noé Tejada Tejada
Director

Licda. Claudia Patricia Corcio de Beltrán
Secretaria de Escuela

TRIBUNAL CALIFICADOR

Dr. Gabriel Alexander Chicas Reyes
Asesor de tesis

M.Sc. María Cecilia Martínez Reyes
Jurado

Dr. Simón Alfredo Peña Aguilar
Jurado

Dra. Graciela Reyes Ahumada
Revisora externa

Agradecimientos

A mi mamá Elena Panameño, por apoyarme en mis proyectos personales y motivarme a seguir aprendiendo cosas nuevas.

A mis abuelos Elias Panameño y María Díaz, por estar pendientes de mi y compartir conmigo palabras de ánimo en el momento adecuado.

A mi asesor de tesis Dr. Gabriel Alexander Chicas Reyes, por su dedicación y compromiso mostrado durante el desarrollo del proyecto de tesis por medio de sus consejos, sugerencias de mejora y por transmitirme parte de su conocimiento.

A mis jurados y revisora externa: M.Sc. María Cecilia Martínez Reyes, Dr. Simón Alfredo Peña Aguilar y a la Dra. Graciela Reyes Ahumada, por su ayuda y disponibilidad para leer el documento escrito de la tesis y brindar comentarios o correcciones para enriquecer la estructura del proyecto de tesis.

A Beatriz Bran, por estar siempre disponible para conversar y mostrar interés sobre mi progreso durante el desarrollo de la tesis.

A mis amigos/as y compañeros/as de la carrera: por invitarme a estudiar y compartir experiencias.

Índice general

Resumen

Lovato Panameño, Carmen Lissette. 2025. *Aspectos combinatorios de las curvas elípticas*. Trabajo de graduación de Licenciatura en Matemática. San Salvador, Universidad de El Salvador.
El presente trabajo consiste en el estudio de las curvas elípticas sobre un campo finito $\mathbb{F}_q$ y sus propiedades combinatorias. Una estrategia para la enumeración de los puntos N_k de una curva C sobre las distintas extensiones $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ consiste en estudiar una función generadora (función zeta asociada a la curva C). Esto permite establecer propiedades que conectan distintas áreas de la matemática con la teoría combinatoria. Un problema interesante es la relación de N_k con los $(q,t)-$ análogos de los números de Lucas, Fibonacci y los grafos de rueda W_k, abordada a partir de la teoría de funciones simétricas y la operación del pletismo dando lugar a nuevas identidades.

Palabras clave: curva, curva elíptica, función generatriz, pletismo, grafo, árbol generador, función simétrica, función elemental, función completa, función de potencias, dualidad, campo finito.

Introducción

La enumeración de puntos N_k de una curva C sobre un campo finito $\mathbb{F}_q$, es un problema que tiene sus raíces en geometría algebraica, teoría de números y combinatoria, el cual tomó relevancia a partir del siglo XX con los aportes de matemáticos de la época como Hasse y André Weil. En particular, el desarrollo de este trabajo se centra en la enumeración de puntos en curvas elípticas E sobre un campo finito $\mathbb{F}_q$, por medio de funciones generatrices. El proyecto está dividido en cuatro capítulos con el objetivo de conocer los aspectos combinatorios de las curvas elípticas:

El Capítulo 1 tiene como finalidad brindar una introducción a los elementos básicos sobre curvas elípticas tales como su definición, su estructura de grupo, la función generatriz asociada a una curva $C/\mathbb{F}_q$ (función zeta de una curva) y las conjeturas de Weil.

En el Capítulo 2, se abordarán los aspectos elementales sobre funciones simétricas homogéneas, algunas de estas funciones son: elemental, completa y de potencias. Además, se define la operación de pletismo de las funciones simétricas que puede ser entendida como un producto de funciones simétricas.

En el Capítulo 3, está enfocado en estudiar y analizar los coeficientes N_k de la función zeta de una curva, por medio de las propiedades de los números de Fibonacci, Lucas y la enumeración de los árboles generadores de un grafo de rueda W_k, tomando de base los aportes brindados por Musiker en el artículo [12].

Finalmente, el Capítulo 4 está conformado por la deducción de identidades y propiedades que derivan de los coeficientes N_k. Se presentan las identidades de Newton para las funciones simétricas elemental, completa y de potencias. Además, se estudian las expresiones de las funciones simétricas completa y de potencias por medio de determinantes. Por último, se definen los polinomios simétricos de Macmahon y propiedades con el fin de establecer expresiones con los coeficientes N_k.

Objetivos del proyecto

- **Objetivo general**
  - Conocer los aspectos combinatorios de las curvas elípticas, a través de nociones básicas sobre Álgebra, Geometría, Teoría de Números y Combinatoria de modo que permita establecer conexiones entre curvas elípticas y grafos.
- **Objetivos específicos**
  - Estudiar resultados básicos sobre curvas elípticas y grafos.
  - Utilizar la teoría de funciones simétricas para el estudio de la función zeta.
  - Realizar cálculos con la función zeta de curvas elípticas.

Capítulo 1

Curvas elípticas

En este capítulo estudiamos resultados básicos relacionados con curvas elípticas que van ser de especial importancia para el desarrollo del presente trabajo.

1.1. Espacio proyectivo

En este apartado se aborda la definición de espacio proyectivo y su relación con el espacio afín.

Definición 1.1.1. *Sea* $\mathbf{K}$ *un campo. Definimos el* ***plano afín*** *como el conjunto de* 2*-uplas sobre* $\mathbf{K} \times \mathbf{K}$

$$\mathbb{A}^2_{\mathbf{K}} := \{(x, y) \in \mathbf{K} \times \mathbf{K}\}.$$

Definición 1.1.2. *Sea* $\mathbf{K}$ *un campo. El* ***espacio proyectivo*** 2***-dimensional sobre*** $\mathbf{K}$*, denotado por* $\mathbb{P}^2_{\mathbf{K}}$*, es definido por las clases de equivalencia de ternas* (X, Y, Z) *con* $X, Y, Z \in \mathbf{K}$ *con al menos una de las* X, Y, Z *distinto del elemento neutro* 0 *de* $\mathbf{K}$*. Dos ternas* (X_1, Y_1, Z_1) *y* (X_2, Y_2, Z_2) *se dice equivalentes si existe* $\lambda \in \mathbf{K}/\ \{0\}$*, tal que*

$$(X_1, Y_1, Z_1) = (\lambda X_2, \lambda Y_2, \lambda Z_2).$$

De la definición (1.1.2), diremos que $[X : Y : Z]$ es una clase dada por la relación de equivalencia $\sim$ y son llamados **puntos** en $\mathbb{P}^2_{\mathbf{K}}$.

$$[X : Y : Z] = \{(\lambda X, \lambda Y, \lambda Z) : \lambda \in \mathbf{K}^\times = \mathbf{K}/\ \{0\}\}.$$

Cada elemento (X, Y, Z) de la clase de equivalencia $[X : Y : Z]$ son llamadas **coordenadas homogéneas** para el punto $[X : Y : Z] \in \mathbb{P}^2_K$.

Una vez ya definido el espacio proyectivo podemos mencionar otros aspectos que interesa estudiar en el presente trabajo .

Sabemos que en el conjunto $\mathbb{P}^2_{\mathbf{K}}$, la coordenada $(0,0,0)$ no pertenece a ningún punto de $\mathbb{P}^2_{\mathbf{K}}$; entonces analizamos el punto $[X:Y:Z] \in \mathbb{P}^2_K$ donde al menos uno de los X, Y, Z es distinto a $0 \in \mathbf{K}$. Por lo que nos preguntamos qué sucedería si dividimos entre Z. De aquí resultan dos casos: cuando $Z = 0$ y $Z \neq 0$. Como se muestra en el siguiente definición.

Definición 1.1.3. *Sea* $\mathbf{K}$ *un campo y* $[X:Y:Z] \in \mathbb{P}^2_K$.

1. *Si* $Z \neq 0$*, entonces* $[X:Y:Z] = [X/Z : Y/Z : 1]$ *son llamados "puntos finitos" en* $\mathbb{P}^2_K$.
2. *Si* $Z = 0$ *consideramos* ∞ *en* X *o* Y *y los puntos* $[X:Y:0]$ *son llamados "puntos al infinito" en* $\mathbb{P}^2_K$.

Notemos que (1.1.3) es una de las posibles formas de trabajar el plano proyectivo ya que el análisis anterior sigue siendo válido para una de las coordenadas restantes X o Y.

Por otra parte, los puntos $[1:0:0], [0:1:0]$ y $[0:Y:0]$ con $Y \neq 0$ son ejemplos de elección de representantes de la clase $[X:Y:0]$ y por lo tanto son " puntos al infinito". Además, los "puntos finitos" del plano afín $\mathbb{A}^2_K$ se pueden describir por medio de puntos en el espacio proyectivo.

Proposición 1.1.1. *Sea* $\mathbf{K}$ *un campo. Se tiene la siguiente inclusión entre el espacio proyectivo y el plano afín:*

$$\begin{aligned} \mathbb{A}^2_K &\hookrightarrow \mathbb{P}^2_K \\ (x,y) &\mapsto [x:y:1]. \end{aligned}$$

Definición 1.1.4. *Sea* $\mathbf{K}$ *un campo . Un polinomio* $F \in \mathbf{K}[X,Y,Z]$ *de grado* n*, donde*

$$F = \sum_{i,j,k} a_{ijk} X^i Y^j Z^k, \text{ con } a_{ijk} \in \mathbf{K},$$

es ***homogéneo*** *si cada término* $a_{ijk}X^iY^jZ^k$ *satisface que* $i+j+k = n$*.*

Ejemplo 1.1.1. Un ejemplo de polinomio homogéneo sobre el campo $\mathbf{K}$ es

$$F_1(X,Y,Z) = 2XY^2 + 4X^2Y + 3X^3.$$

Por otra parte, el polinomio

$$F_2(X,Y,Z) = 2XY + 4X^2Y + 3X^3,$$

no es homogéneo ya que la suma de las potencias del monomio $2XY$ es $1+1=2$ y el grado de F_2 es 3.

Proposición 1.1.2. *Sea* $\mathbf{K}$ *un campo. Si un polinomio* $F \in \mathbf{K}[X,Y,Z]$ *es homogéneo de grado* n*, entonces*

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x,y,z) \text{ con } \lambda \in \mathbf{K}.$$

Más aún, el conjunto de ceros de un polinomio homogéneo F sobre un campo $\mathbf{K}$ está bien definido. Por ejemplo

$$\begin{aligned}(x_1, y_1, z_1) \sim (x_2, y_2, z_2) &\Leftrightarrow (x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)\\ &\Rightarrow F(x_1, y_1, z_1) = 0 \Leftrightarrow F(x_2, y_2, z_2) = 0.\end{aligned}$$

Un polinomio F con coordenadas en el plano afín se puede pasar a coordenadas homogéneas del espacio proyectivo agregando una variable Z adecuada y viceversa, como se muestra en el siguiente resultado.

Proposición 1.1.3. *Sea $F \in \mathbf{K}[X, Y, Z]$ un polinomio homogéneo de grado n entonces*

$$F(x, y, z) = z^n f(x, y) \text{ donde } f(x, y) = F(x, y, 1),\ \forall [x : y : z] \in \mathbb{P}^2_{\mathbf{K}} \text{ con } z \neq 0.$$

Ejemplo 1.1.2 (Rectas que se intersecan en el infinito)**.** Sea $\mathbf{K}$ un campo.

Caso 1: Consideremos $Y = mX + c_1$ y $Y = mX + c_2$ con $c_1 \neq c_2$ constantes en $\mathbf{K}$. Notemos que ambas ecuaciones no son polinomios homogéneos. Entonces pasamos a su forma homogénea como se establece (1.1.3),

$$Y = mX + c_1 Z \quad Y = mX + c_2 Z.$$

Luego de homogenizar, se sustituye un punto $[x : y : z] \in \mathbb{P}^2_{\mathbf{K}}$. Encontramos la intersección de ambas ecuaciones

$$\begin{aligned}zc_1 &= zc_2\\ z(c_1 - c_2) &= 0, \quad \text{donde } 0 \text{ es el elemento neutro de } \mathbf{K}.\\ \Rightarrow z &= 0,\ \ y = mx.\end{aligned}$$

Recordemos que $x,\ y$ no pueden ser ambos 0 por la definición 1.1.2, por lo tanto, las rectas se intersecan en el punto $[x : mx : 0] = [1 : m : 0]$ que por definición es punto al infinito en $\mathbb{P}^2_{\mathbf{K}}$. Ver figura 1.1.

Caso 2: Y en el caso que tengamos dos rectas $x = c_1$ y $x = c_2$ con $c_1 \neq c_2 \in \mathbf{K}$.

$$\Rightarrow x = zc_1,\ \ x = zc_2.$$

Ahora calculamos la intersección

$$zc_1 = zc_2.$$

Luego obtenemos que $z = 0$. Así, la intersección de las rectas es el punto al infinito $[0 : 1 : 0] \in \mathbb{P}^2_{\mathbf{K}}$. Ver figura 1.2.

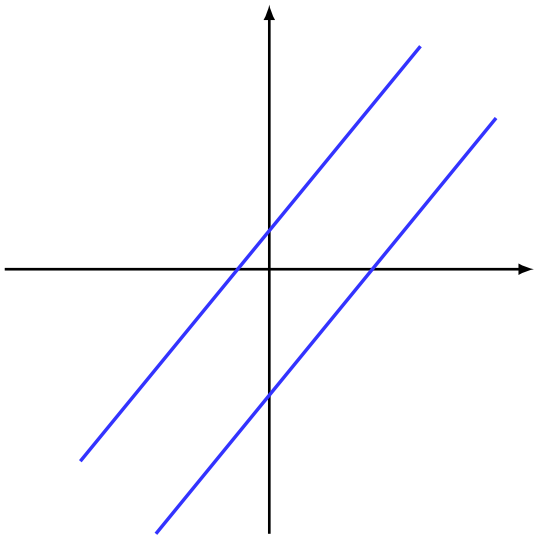


Figura 1.1: Rectas en $\mathbb{A}^2_{\mathbf{K}}$ caso 1.

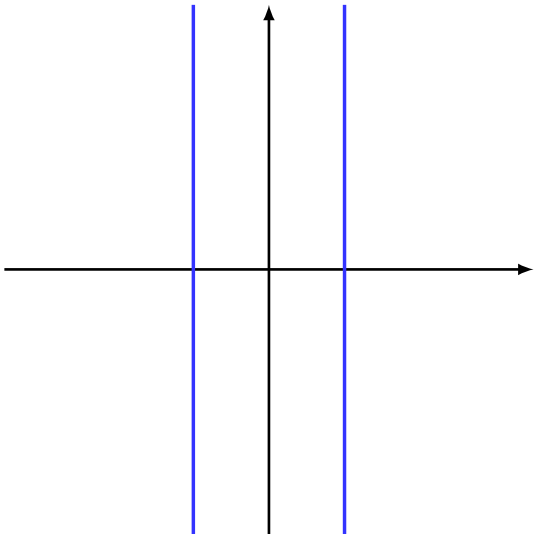


Figura 1.2: Rectas en $\mathbb{A}^2_{\mathbf{K}}$ caso 2.

1.2. Ecuaciones de Weierstrass y definición de curva elíptica

Los resultados brindados en el apartado anterior servirán como herramienta para estudiar con mayor naturalidad las generalidades de curvas elípticas que se menciona a continuación.

Definición 1.2.1. *Una curva elíptica E es la gráfica de una ecuación de la forma*

$$y^2 = x^3 + Ax + B, \tag{1.1}$$

donde A, B son constantes en un campo $\mathbf{L}$ y $\Delta := -(4A^3 + 27B^2) \neq 0$.

A la ecuación (1.1) se le llama **ecuación de Weierstrass corta o reducida**. Y la cantidad definida por Δ es llamado **discriminante** de una ecuación en su forma de Weierstrass corta que brinda información sobre las raíces repetidas de una ecuación cúbica.

La siguiente definición es para una curva elíptica definida sobre un campo en la forma (1.1):

Definición 1.2.2. *Sea $\mathbf{K} \supseteq \mathbf{L}$ un campo. Una curva elíptica sobre el campo $\mathbf{K}$ está dada por*

$$E(\mathbf{K}) = \{\infty\} \cup \left\{(x, y) \in \mathbf{K} \times \mathbf{K} : y^2 = x^3 + Ax + B\right\}.$$

Con A, B constantes en $\mathbf{L}$ y $\Delta \neq 0$.

La definición de curva elíptica (1.2.1) es de utilidad cuando se trabaja con curvas en el plano afín. En cambio la definición anterior (1.2.2) será necesaria más adelante para trabajar con la ley de grupo.

Ejemplo 1.2.1. Consideremos las siguientes curvas definidas sobre $\mathbf{K} = \mathbb{R}$.

- $y^2 = x^3 - x$.
  Para encontrar las raíces de esta ecuación factorizamos el polinomio cúbico

  $$x^3 - x = x(x+1)(x-1) = 0.$$

  Obtenemos tres raíces reales y distintas las cuales son: $0, \pm 1$ (ver figura 1.3). Si calculamos el discriminante resulta que

  $$-(4A^3 + 27B^2) = -(4(-1)^3 + 27(0)^2) = 4 \neq 0.$$

  Para este caso, se satisface la definición de curva elíptica (1.2.1).

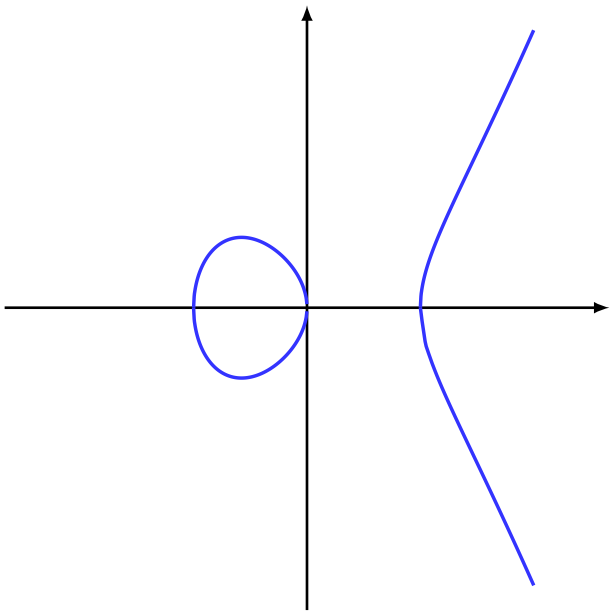


Figura 1.3: Gráfica de $y^2 = x^3 - x$ con $\Delta \neq 0$.

- Consideremos la ecuación

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

  Notemos que esta ecuación (ver figura 1.4) tiene una raíz de multiplicidad tres y su discriminante es

  $$-(4A^3 + 27B^2) = 0.$$

  Por lo tanto, no satisface la definición de curva elíptica (1.2.1).

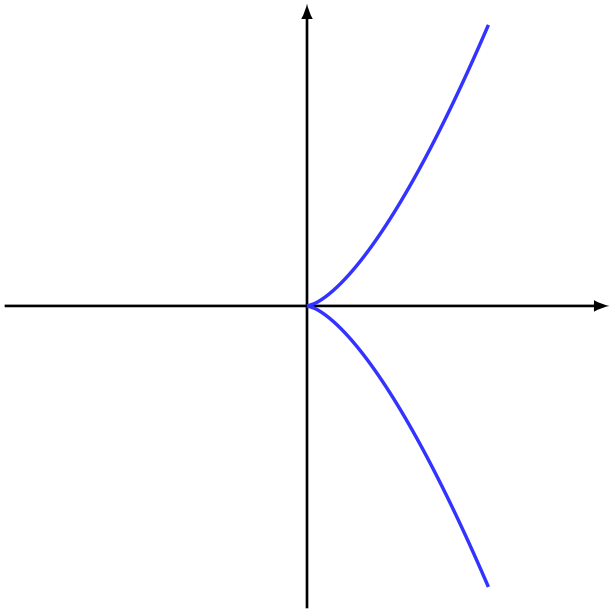


Figura 1.4: Gráfica de $y^2 = x^3$ con $\Delta = 0$.

Otra forma que se puede describir una curva elíptica E sobre un campo $\mathbf{K}$, es por medio de la gráfica de la ecuación

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ donde } a_1, \ldots, a_6 \text{ son constantes,} \qquad (1.2)$$

llamada la **ecuación de Weierstrass generalizada**.
Es posible llevar esta ecuación a la forma (1.1) realizando cambios de variables. Primero notemos que podemos agrupar términos

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6.$$

Ahora dividimos entre 2 el término $(a_1x + a_3)$ y completamos cuadrados

$$\begin{aligned} y^2 + (a_1x + a_3)y + \left(\frac{a_1x + a_3}{2}\right)^2 &= x^3 + a_2x^2 + a_4x + a_6 + \left(\frac{a_1x + a_3}{2}\right)^2 \\ \left(y + \frac{a_1x + a_3}{2}\right)^2 &= x^3 + a_2x^2 + a_4x + a_6 + \left(\frac{a_1x + a_3}{2}\right)^2 \\ \left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 &= x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + (a_4 + \frac{a_1a_3}{2})x + \left(a_6 + \frac{a_3^2}{4}\right). \end{aligned}$$

Realizando el cambio de variables $\frac{1}{2}(y - a_1x - a_3)$ la ecuación queda de la forma

$$\begin{aligned}\left(\frac{1}{2}(y - a_1x - a_3) + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 &= x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + (a_4 + \frac{a_1a_3}{2})x + \left(a_6 + \frac{a_3^2}{4}\right)\\ \left(\frac{y}{2}\right)^2 &= x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + (a_4 + \frac{a_1a_3}{2})x + \left(a_6 + \frac{a_3^2}{4}\right)\\ y^2 &= 4x^3 + \left(4a_2 + a_1^2\right)x^2 + (4a_4 + 2a_1a_3)x + \left(4a_6 + a_3^2\right)\\ y^2 &= 4x^3 + b_2x^2 + b_4x + b_6\end{aligned}$$

donde

$$b_2 = 4a_2 + a_1^2,\ \ b_4 = 4a_4 + 2a_1a_3,\ \ b_6 = 4a_6 + a_3^2.$$

Finalmente, realizamos otro cambio de variable de modo que y es $y/108$ y reemplazamos x por $(x - 3b_2)/36$

$$\left(\frac{y}{108}\right)^2 = 4\left(\frac{x - 3b_2}{36}\right)^3 + b_2\left(\frac{x - 3b_2}{36}\right)^2 + b_4\left(\frac{x - 3b_2}{36}\right) + b_6.$$

Desarrollando las expresiones se obtiene:

$$\begin{aligned}y^2 &= x^3 + 27(-b_2^2 + 12b_4)x + 54(b_2^3 - 18b_4b_2 + 216b_6)\\ y^2 &= x^3 + Ax + B.\end{aligned}$$

donde

$$\begin{aligned}A &= 27(-b_2^2 + 12b_4)\\ B &= 54(b_2^3 - 18b_4b_2 + 216b_6).\end{aligned}$$

Los cambios de variables realizados para obtener la ecuaciones de Weierstrass en su forma corta son válidos cuando el campo $\mathbf{K}$ en el que está definida la curva elíptica es de característica distinta de 2 y 3. Para el lector interesado véase la sección 2.8 de [18].

1.2.1. Ley de grupo

Uno de los resultados interesantes sobre curvas elípticas es que si tomamos dos puntos podemos producir un nuevo punto que siempre va pertenecer a dicha curva por medio de una operación que se llama suma de puntos sobre una curva elíptica. Como veremos más adelante, esta operación da al conjunto de puntos de la curva elíptica una estructura de grupo abeliano.

Definición 1.2.3. *Sea E una curva elíptica sobre $\mathbf{K}$ descrita por la gráfica de una ecuación de Weierstrass de la forma*

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

Y sean $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$, definimos la suma de los puntos de $E(\mathbf{K})$, que denotaremos por $+$, como la que se obtiene de trazar la recta l que pasa por P_1 y P_2 que interseca a E en un tercer punto P_3'. Y la reflexión de P_3' respecto al eje x es un punto P_3 resultado de sumar P_1 y P_2, es decir

$$P_1 + P_2 = P_3.$$

Analicemos los pasos para calcular la suma de dos puntos sobre una curva elíptica E sobre $\mathbf{K}$ y en su forma de ecuación de Weierstrass (1.1). Sean $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ en E.

Caso 1 : Si $P_1 \neq P_2 \neq \infty$, trazamos una recta l (ver figura 1.5) que pasa por P_1 y P_2 con pendiente

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

- Si $x_1 \neq x_2$ entonces la ecuación de la recta l es

$$y = m(x - x_1) + y_1.$$

Sustituimos y en la ecuación de E dada de la forma (1.1)

$$\begin{aligned} (m(x - x_1) + y_1)^2 &= x^3 + Ax + B \\ m^2(x - x_1)^2 + 2m(x - x_1)y_1 + y_1^2 &= x^3 + Ax + B. \end{aligned}$$

Reordenando términos se obtiene

$$\begin{aligned} (x^3 + Ax + B) - (m^2(x - x_1)^2 + 2m(x - x_1)y_1 + y_1^2) &= 0 \\ x^3 - m^2(x - x_1)^2 + (Ax + B) - 2m(x - x_1)y_1 + y_1^2) &= 0 \\ x^3 - m^2x^2 + bx + c &= 0, \end{aligned}$$

donde

$$\begin{aligned} b &= (A + 2x_1 - 2my_1) \\ c &= B - x_1^2 + 2mx_1y_1 + y_1^2. \end{aligned}$$

Nuestro objetivo hasta este punto es encontrar una tercera raíz del polinomio cúbico

$$x^3 - m^2x^2 + bx + c = 0.$$

Notemos que x_1 y x_2 son raíces de este polinomio y al factorizar obtendremos

$$(x-x_1)(x-x_2)(x-x_3) = x^3 + (-x_1-x_2-x_3)x^2 + b'x + c', \text{ donde}$$
$$b' = x_1x_2 + x_3x_1 + x_2x_3$$
$$c' = -x_1x_2x_3.$$

Y x_3 es la tercera raíz que buscamos.
Observemos que

$$x^3 - m^2x^2 + bx + c = x^3 + (-x_1-x_2-x_3)x^2 + b'x + c'$$
$$\Rightarrow -m^2 = -x_1 - x_2 - x_3.$$

De este modo x_3 es

$$\Rightarrow x_3 = m^2 - (x_1 + x_2). \tag{1.3}$$

Luego, la expresión para la coordenada y_3 es

$$y_3 = m(x_3 - x_1) + y_1.$$

Entonces,

$$P_3 = (x_3, y_3) = (m^2 - (x_1 + x_2), m(x_3 - x_1) + y_1).$$

Finalmente, encontramos la reflexión del punto P_3 respecto al eje de las x (ver figura 1.5). Por lo tanto

$$P_1 + P_2 = (x_3, -y_3).$$

- Si $x_1 = x_2$ y $y_1 \neq y_2$. En este caso la recta que pasa por P_1 y P_2 es vertical y por lo tanto la intersección con E es ∞. Así

$$P_1 + P_2 = \infty.$$

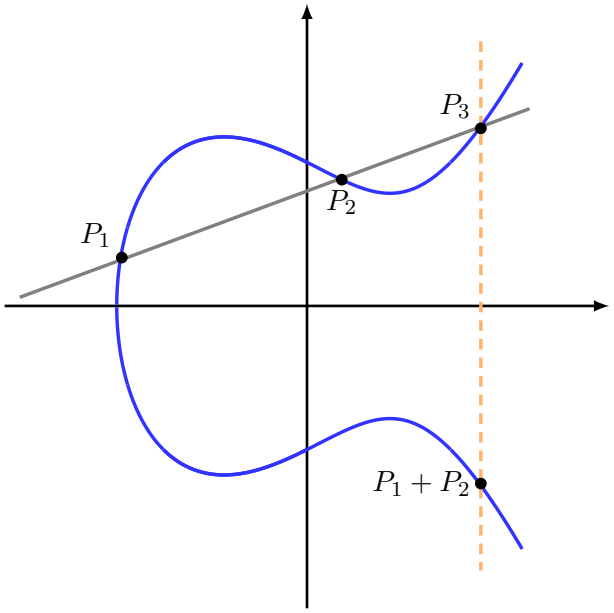


Figura 1.5: Suma de puntos en una curva elíptica E con $P_1 \neq P_2$.

Caso 2 : Si $P_1 = P_2 = (x_1, y_1) \neq \infty$. Para este caso basta con encontrar la recta tangente l a la curva en el punto P_1.
Entonces la pendiente de la recta l la calculamos por medio de la derivada implícita de $y^2 = x^3 + Ax + B$

$$2y\frac{dy}{dx} = 3x^2 + A$$
$$\Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

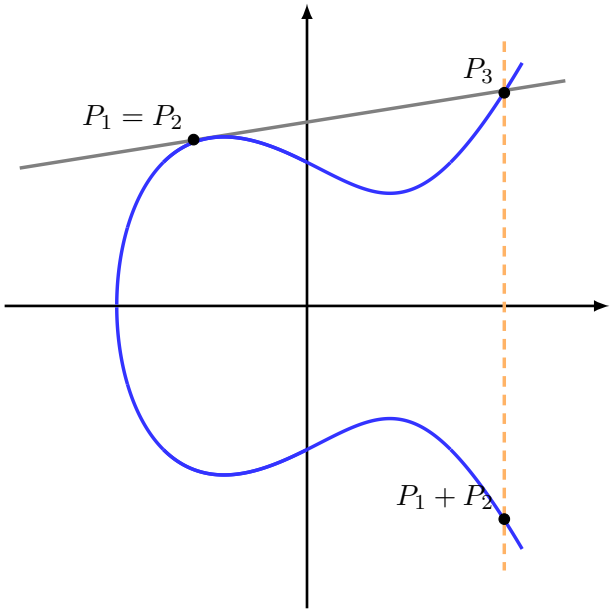


Figura 1.6: Suma de puntos sobre una curva elíptica E con $P_1 = P_2$.

Si $y_1 = 0$ entonces l es una recta vertical y $P_1 + P_2 = \infty$.

Si $y_1 \neq 0$ entonces la ecuación de l es

$$y = m(x - x_1) + y_1. \tag{1.4}$$

Nuevamente obtenemos

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

En este caso x_1 es raíz doble del polinomio cúbico

$$x^3 + Ax + B - (m(x - x_1) + y_1)^2 = 0.$$

Igual que en el proceso para encontrar la expresión (1.3), la raíz buscada es

$$\begin{aligned} x_3 &= m^2 - (x_1 + x_1) \\ &= m^2 - 2x_1. \end{aligned}$$

Y por (1.4) tenemos que

$$y_3 = m(x_3 - x_1) + y_1.$$

Entonces $P_3 = (x_3, y_3)$ es

$$P_3 = (x_3, y_3) = (m^2 - 2x_1, m(x_3 - x_1) + y_1).$$

Por último, realizamos la reflexión de P_3 respecto al eje x y de este modo obtenemos la suma de P_1 y P_2

$$P_1 + P_2 = (x_3, -y_3).$$

En este caso en particular, la expresión de la coordenada x_3 se puede seguir desarrollando de modo que quede expresada en términos de x_1

$$\begin{aligned} x_3 = m^2 - 2x_1 &= \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1 \\ &= \frac{9x_1^4 + 6Ax_1^2 - 8x_1y_1^2 + A^2}{4y_1^2} \\ &= \frac{9x_1^4 + 6Ax_1^2 - 8x_1(x_1^3 + Ax_1 + B) + A^2}{4(4x_1^3 + Ax_1 + B)}, \text{ sustituyendo } y_1 \text{ en } (1.1). \end{aligned}$$

Luego, se obtiene que

$$x_3 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4x_1^3 + 4Ax_1 + 4B}. \tag{1.5}$$

La formula anterior para calcular $2P_1$ es llamada **fórmula de duplicación** para una curva elíptica definida por su ecuación de Weierstrass reducida. Para una curva elíptica definida por su ecuación de Weierstrass generalizada puede ver la deducción en [14].

Si $P_1 = P_2 = \infty$ entonces

$$P_1 + P_2 = \infty.$$

Nota 1. *Por convención* $\infty + \infty = \infty$.

Caso 3 : Si $P_1 \neq P_2$ y $P_2 = \infty$. La recta l que pasa por P_1 y P_2 es vertical e interseca a E en $P_3 = \infty$, la reflexión de P_3 es $P_1 + P_2 = \infty$.

Análogamente, si $P_1 = \infty$ obtenemos que $P_1 + P_2 = \infty$.

Ejemplo 1.2.2. Sea E una curva elíptica sobre $\mathbf{K} = \mathbb{R}$ y definida por su ecuación de Weierstrass

$$y^2 = x^3 + 73.$$

Deseamos calcular la suma de los puntos $P = (2, 9),\ Q = (3, 10)$ en E. El proceso es el siguiente:

Paso 1. Trazamos la recta l secante a la curva que pasa por P y Q (ver figura 1.7).

Paso 2. Encontramos la fórmula de l teniendo en cuenta que $P \neq Q$

$$y = m(x - 2) + 9.$$

Paso 3. Identificamos que la pendiente m se puede calcular por

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} \\ &= \frac{10 - 9}{3 - 2} = 1. \end{aligned}$$

Paso 4. Sustituyendo m, la ecuación de la recta l es

$$y = x + 7.$$

Paso 5. Ahora calculamos la coordenada x_3, que es

$$x_3 = m^2 - x_1 - x_2 = 1^2 - 2 - 3 = -4.$$

Paso 6. Sustituimos la coordenada x_3 en la ecuación de la recta l para encontrar y_3

$$y_3 = x_3 + 7 = -4 + 7 = 3.$$

Entonces el tercer punto $P_3 = (x_3, y_3)$ que interseca a l y la curva E es

$$P_3 = (-4, 3).$$

Paso 7. Por lo tanto, el punto $P + Q$ es la reflexión con respecto al eje x de P_3 el cual es

$$P + Q = (-4, -3).$$

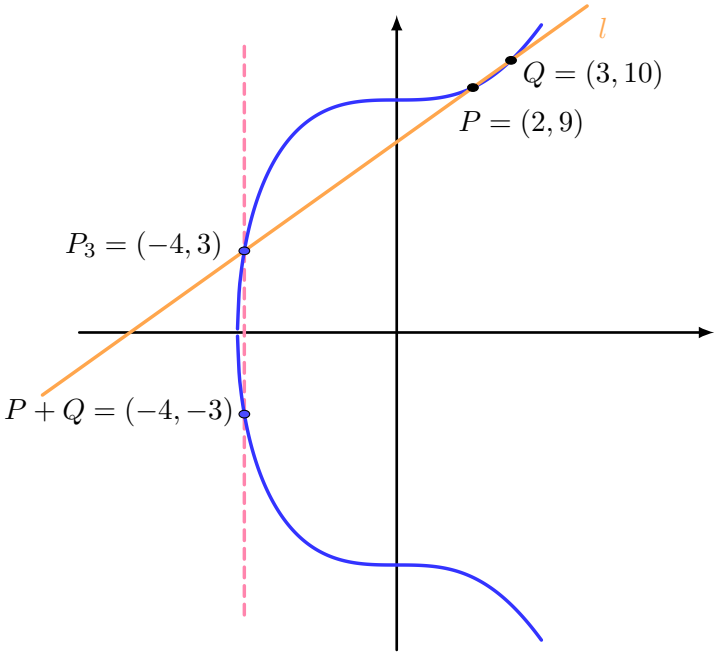


Figura 1.7: Suma de puntos sobre la curva elíptica $E : y^2 = x^3 + 73$.

En el siguiente ejemplo se ilustra el procedimiento para utilizar la fórmula de duplicación en una curva elíptica:

Ejemplo 1.2.3. Con la curva dada en el ejemplo 1.2.2, se quiere calcular $2P = 2(2, 9)$. Identificamos que $x_1 = 2$ y $A = 0$, $B = 73$ en la ecuación de la curva elíptica $y^2 = x^3 + 73$ y se procede a sustituir en (1.5):

$$\begin{aligned} x_3 &= \frac{(2)^4 - 2(0)(2)^2 - 8(73)(2) + (0)^2}{4(2)^3 + 4(0)(2) + 4(73)} \\ &= \frac{16 - 1168}{32 + 292} \\ x_3 &= -\frac{32}{9}. \end{aligned}$$

Luego se calcula la coordenada y_3 por medio de la ecuación

$$y_3 = m(x_3 - x_1) + y_1. \tag{1.6}$$

donde m es la pendiente de la recta que pasa por P y esta es

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{3(2)^2 + 0}{2(9)} = \frac{2}{3}.$$

Ahora sustituimos x_3 y m en (1.6)

$$\begin{aligned} y_3 &= \left(\frac{2}{3}\right) \cdot \left(-\frac{32}{9} - 2\right) + 9 \\ &= \frac{-100}{27} + 9 \\ &= \frac{143}{27}. \end{aligned}$$

Seguidamente obtenemos la reflexión del punto $(x_3, y_3) = (-\frac{32}{9}, \frac{143}{27})$ que es $(x_3, -y_3)$.

Por lo tanto, la suma del punto P es

$$2P = \left(-\frac{32}{9}, -\frac{143}{27}\right).$$

La operación de suma de puntos de una curva elíptica $E(\mathbf{K})$ se resume en el siguiente algoritmo (presentado como pseudocódigo):

Algoritmo 1 Suma de puntos en una curva elíptica E descrita por una ecuación de Weierstrass.

Entrada: $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ puntos en $E(\mathbf{K})$.
Salida: $P_1 + P_2 = (x_3, -y_3)$ en $E(\mathbf{K})$.

Si $P_1 \neq P_2$ y distintos de ∞ **entonces**
  Si $x_1 \neq x_2$ **entonces**
    $x_3 = m^2 - x_1 - x_2,\ \ y_3 = m(x_1 - x_2) + y_1,$ con $m = \frac{y_2 - y_1}{x_2 - x_1}$
  Si $x_1 = x_2$ y $y_1 \neq y_2$ **entonces**
    $P_1 + P_2 = \infty$
Si $P_1 = P_2 = (x_1, y_1)$ **entonces**
  Si $y_1 \neq 0$ **entonces**
    $x_3 = m^2 - 2x_1,\ \ y_3 = m(x_1 - x_2) + y_1,$ con $m = \frac{3x_1^2 + A}{2y_1}$
  Si $y_1 = 0$ **entonces**
    $P_1 + P_2 = \infty$
Si $P_1 \neq \infty$ **entonces**
    $P_1 + \infty = P_1$

En el siguiente resultado se demostrará que la suma de puntos sobre una curva elíptica define una estructura de grupo abeliano. Cabe destacar que se utilizará la definición (1.2.2) de curva elíptica.

Teorema 1.2.1 (Ley de grupo)**.** *La adición de puntos en una curva elíptica E sobre un campo* $\mathbf{K}$ *satisface las siguientes propiedades:*

1. ***Existencia del elemento neutro**: $P + \infty = P$ para todo P en E.*

2. ***Existencia de elementos inversos****: Para todo P en E, existe $-P$ en E que cumple:*

$$P + (-P) = \infty.$$

3. ***Conmutatividad****: $P_1 + P_2 = P_2 + P_1$ para cualesquiera P_1, P_2 en E.*

4. ***Asociatividad****: Para cualesquiera P_1, P_2, P_3 en E*

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3).$$

Demostración. Sea E una curva elíptica sobre un campo $\mathbf{K}$. Se debe demostrar que $E(K)$ es un grupo abeliano con la operación suma definida en (1.2.3).

1. **Existencia del elemento neutro**: El punto ∞ es el elemento neutro de $E(\mathbf{K})$ ya que para todo $P \in E(\mathbf{K})$, la recta l que pasa por ∞ y P es vertical donde P' el tercer punto de intersección de l con E y es el reflejo de P, entonces por definición de suma de puntos en $E(K)$ se tiene que

$$P + \infty = P.$$

2. **Existencia de inversos**: Para todo $P \in E(\mathbf{K})$. El punto $-P$ reflexión de P, es el elemento inverso de P ya que por definición, la recta l que pasa por P y $-P$ es vertical; entonces el tercer punto de intersección de la recta l con E es ∞ y su reflexión es ∞. Por lo tanto

$$P + (-P) = \infty.$$

3. **Conmutatividad**: Sean $P_1, P_2 \in E(\mathbf{K})$. La recta l que pasa por P_1 y P_2 tiene como intersección un tercer punto $P_3' \in E(\mathbf{K})$ y el reflejo de P_3' es P_3 entonces por definición de suma de puntos en $E(\mathbf{K})$ tenemos que

$$P_1 + P_2 = P_3.$$

   La recta que pasa por P_2 y P_1 es l por lo que la intersección con la curva E es P_3' y por definición de suma de puntos

$$P_2 + P_1 = P_3.$$

   De modo que

$$P_1 + P_2 = P_2 + P_1.$$

   Por lo tanto, se cumple la conmutatividad de suma de puntos de $E(\mathbf{K})$.

4. **Asociatividad**.
   La asociatividad no se comprobará en el presente trabajo. Una prueba que hace uso de herramientas de Geometría Algebraica puede consultarse en [3].

■

1.2.2. Curvas elípticas sobre campos finitos

En esta sección se estudiarán resultados y propiedades de curvas elípticas definidas sobre un campo finito $\mathbb{F}_q$ donde q es una potencia de primo, es decir $q = p^s$ con p un número primo y $s > 0$. Además, denotaremos por $\overline{\mathbb{F}}_q$ a una clausura algebraica de $\mathbb{F}_q$.

Número de puntos sobre curvas elípticas

En este apartado estudiaremos las formas de estimar el número de puntos de una curva elíptica E sobre $\mathbb{F}_q$, el cual es uno de los resultados más importante asociados a curvas elípticas, y sirve como punto de partida para muchas aplicaciones tales como la criptografía.

Iniciamos mostrando el siguiente ejemplo, en el cual se ilustran resultados sobre cálculos de puntos sobre una curva elíptica sobre un campo finito.

Ejemplo 1.2.4. $E : y^2 = x^3 + 2$ es una curva elíptica sobre $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. Este campo tiene 7 elementos y podemos hacer una lista de los puntos sobre $E(\mathbb{F}_7)$. El problema es equivalente a encontrar las soluciones de la ecuación $y^2 = x^3 + 2$. Como se muestra a continuación:

x	$x^3 + 2$	y	Puntos
0	2	3,4	(0,3), (0,4)
1	3	No tiene solución	No tiene solución
2	3	No tiene solución	No tiene solución
3	1	1,6	(3,1),(3,6)
4	3	No tiene solución	No tiene solución
5	1	1, 6	(5,1), (5,6)
6	1	1, 6	(6,1), (6,6)

De la tabla anterior podemos notar que los puntos sobre la curva son

$$E(\mathbb{F}_7) = \{\infty, (0,3), (0,4), (3,1), (3.6), (5,1), (5,6), (6,1), (6,6)\},$$

que fueron obtenidos por medio de la resolución de congruencias de la forma $y^2 \equiv a \pmod 7$ y en el caso ∞ se agrega a la lista como elemento neutro del grupo aditivo de $E(\mathbb{F}_7)$. Una forma de comprobar este resultado es considerando la ecuación de la curva elíptica homogeneizada, es decir

$$ZY^2 = X^3 + 2Z^3.$$

Y se comprueba que al sustituir el punto $\infty = [0 : 1 : 0]$ en ambos de la ecuación, la igualdad se cumple. Por lo tanto, el número de puntos de $E(\mathbb{F}_7)$ es 9.

Como podemos observar para este ejemplo en particular, resulta fácil contar el número de puntos en una curva elíptica sobre el campo finito $\mathbb{F}_7$ ya que tiene un número de elementos pequeño. Sin embargo, esto se vuelve una tarea difícil a medida que q aumenta.

Para una curva elíptica E sobre $\mathbb{F}_q$ definida en su forma generalizada de Weierstrass (1.2), una cota superior para el número de puntos es

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

La cantidad $2q$ es porque y puede tomar a lo sumo dos valores en $\mathbb{F}_q$, y el 1 es el punto ∞, es decir el elemento identidad del grupo $E(\mathbb{F}_q)$.

Por otra parte, es posible que la ecuación cuadrática no tenga solución en $\mathbb{F}_q$ (como en el ejemplo 1.2.4 para ciertos x la ecuación no tiene solución). Entonces es razonable pensar en una cota más pequeña para el número de puntos en $E(\mathbb{F}_q)$, es decir que lugar de $2q$ sea q. Esto se debe a que por un lado, el grupo de unidades de $\mathbb{F}_q$ (que denotamos por $\mathbb{F}_q^\times$) es cíclico; en otras palabras $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$, por lo que eligiendo un generador x podemos escribir $\mathbb{F}_q^\times = \{1, x, x^2, \ldots, x^{q-1}\}$ es finito ya que $\mathbb{F}_q$ es un campo $\mathbb{F}_q^\times = \mathbb{F}_q / \{0\}$ es decir $\#\mathbb{F}_q^\times = q - 1$.

En particular, para $\mathbb{F}_p$ con p primo su grupo de unidades $\mathbb{F}_p^\times = \{1, x, x^2, \ldots, x^{p-1}\}$ cumple que $x^k \in \mathbb{F}_p^\times$ es cuadrado si y sólo si k es par y por lo tanto $(p-1)/2$ son cuadrados en $\mathbb{F}_p^\times$ (ver [1]).

El siguiente teorema brinda una cota superior para el orden de $E(\mathbb{F}_q)$. Este resultado fue conjeturado por Artin y demostrado por Hasse en 1930.

Teorema 1.2.2 (Hasse)**.** *Sea E una curva elíptica definida sobre un campo finito $\mathbb{F}_q$. Entonces*

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

La demostración de este teorema utiliza nociones de Geometría Algebraica y conocimiento acerca del grupo de Galois de la extensión $\overline{\mathbb{F}}_q/\mathbb{F}_q$. Véase [14], capítulo V, sección 1.

Ejemplo 1.2.5. Sea E una curva elíptica sobre $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. La cota superior que da el teorema de Hasse 1.2.2 es

$$\begin{aligned} |\#E(\mathbb{F}_7) - 7 - 1| &\leq 2\sqrt{7} \\ |\#E(\mathbb{F}_7) - 8| &\leq 2\sqrt{7} \approx 5. \end{aligned}$$

Entonces el número de puntos de $E(\mathbb{F}_7)$ se encuentra dentro del intervalo

$$3 \leq \#E(\mathbb{F}_7) \leq 13.$$

Y comparando con el ejemplo 1.2.4, notamos que es un resultado válido ya que $E : y^2 = x^3 + 2$ tiene 9 puntos definidos sobre $\mathbb{F}_7$.

Ejemplo 1.2.6. Consideremos una curva elíptica E sobre el campo $\mathbb{F}_{5^6} = \mathbb{F}_5[X]/(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$, por el teorema de Hasse tenemos que

$$\begin{aligned} \left|\#E(\mathbb{F}_{5^6}) - 5^6 - 1\right| &\leq 2\sqrt{5^6} \\ |\#E(\mathbb{F}_{5^6}) - 15626| &\leq 2(125) = 250. \end{aligned}$$

Por lo tanto , la cantidad de elementos del grupo $E(\mathbb{F}_{5^6})$ se encuentra en el intervalo

$$15376 \leq \#E(\mathbb{F}_{5^6}) \leq 15876.$$

Es importante señalar que el teorema 1.2.2 de Hasse, no indica un algoritmo para encontrar la cantidad de puntos en una curva elíptica $E(\mathbb{F}_q)$, sino más bien nos proporciona una estimación del número de puntos sobre $E(\mathbb{F}_q)$ el cual nos dice que es aproximadamente $q + 1$ con un error de $2\sqrt{q}$.

Ejemplo 1.2.7. Un ejemplo de aplicación de curvas elípticas definidas sobre un campo finito $\mathbb{F}_q$, que refleja la importancia de la numeración de puntos, es el problema del logaritmo discreto para curvas elípticas ECDLP, el cual consiste en que dados dos puntos $P, Q \in E(\mathbb{F}_q)$ tales que P pertenece al subgrupo generado por Q y se debe encontrar un entero n que satisface $P = [n]Q$. Sin embargo, para valores grandes de q encontrar dicho n resulta difícil. Como consecuencia, surgen criptosistemas basados en la dificultad de resolver el problema de ECDLP (el lector interesado puede consultar [14] sección XI.4).

1.3. Función zeta de curvas elípticas

En este apartado estudiaremos la función zeta para curvas elípticas definidas sobre un campo finito $\mathbb{F}_q$ como una reiterpretación del teorema de Hasse 1.2.2.

Definición 1.3.1. *Para $n \geq 1$. Decimos que $\mathbb{F}_q$ es la **extensión** de $\mathbb{F}_p$ de grado n y $\#\mathbb{F}_q = q = p^n$.*

Definición 1.3.2. *Para $n \geq 1$. Una **variedad proyectiva** sobre $\mathbb{F}_q$, es el conjunto de soluciones de*

$$f_1(x_0, \ldots, x_N) = \cdots = f_m(x_0, \ldots, x_N) = 0,$$

donde $f_1, \ldots, f_m$ son polinomios homogéneos con coeficientes en $\mathbb{F}_q$. Se denota por $V(\mathbb{F}_{q^n})$ al conjunto de puntos de V con coordenadas en $\mathbb{F}_{q^n}$.

Definición 1.3.3. *La función zeta de $V/\mathbb{F}_q$ es la serie de potencias*

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty}\left(\#V\left(\mathbb{F}_{q^n}\right)\frac{T^n}{n}\right)\right).$$

Además,

$$F(T) = \sum_{n=1}^{\infty} \left(\#V\left(\mathbb{F}_{q^n}\right) \frac{T^n}{n} \right) \in \mathbb{Q}[T],$$

y puede definirse la exponencial como la serie de potencia de la forma

$$Z(V/\mathbb{F}_q; T) = \sum_{k=0}^{\infty} \frac{F(T)^k}{k!}.$$

Si se conoce la función zeta de $V/\mathbb{F}_q$ entonces es posible calcular las cantidades de $V(\mathbb{F}_{q^n})$ para $n \geq 1$.

Proposición 1.3.1. *Sea $Z(V/\mathbb{F}_q; T)$ la función zeta de $V/\mathbb{F}_q$ entonces*

$$\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!} \left(\frac{d^n}{dT^n} \log Z(V/\mathbb{F}_q; T) \right) \Big|_{T=0}, \text{ para todo } n \geq 1.$$

Demostración. Sea $V/\mathbb{F}_q$ una variedad con $Z(V/\mathbb{F}_q; T)$ la función zeta asociada a $V/\mathbb{F}_q$. Se quiere demostrar que las cantidades de puntos del conjunto $V(\mathbb{F}_{q^n})$ para $n \geq 1$ son obtenidos por medio de la igualdad

$$\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!} \left(\frac{d^n}{dT^n} \log Z(V/\mathbb{F}_q; T) \right) \Big|_{T=0}.$$

Al realizar derivadas sucesivas de $\log Z(V/\mathbb{F}_q)$ con respecto a T se obtiene que la n-ésima derivada es de la forma

$$\frac{d^n}{dT^n} \log Z(V/\mathbb{F}_q : T) = (n-1)!\#V(\mathbb{F}_{q^n}) + \underbrace{\sum_{k=n+1}^{\infty} (k-1)!\#V(\mathbb{F}_{q^k}) T^{n-k}}_{f(T)},$$

Aquí $f(T)$ es una función generatriz .

Ahora se demostrará por inducción sobre n que la derivada n-ésima de $\log Z(V/\mathbb{F}_q, T)$ es

$$\frac{d^n}{dT^n} \log Z(V/\mathbb{F}_q : T) = (n-1)!\#V(\mathbb{F}_{q^n}) + f(T).$$

Caso base: Para $n = 1$.
Calculamos la primera derivada de $\log Z(V/\mathbb{F}_q)$ con respecto a T:

$$\begin{aligned} \frac{d}{dT} \log Z(V/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n}) T^{n-1} \\ &= \#V(\mathbb{F}_q) + \sum_{n=2}^{\infty} \#V(\mathbb{F}_{q^n}) T^{n-1} \\ \frac{d}{dT} \log Z(V/\mathbb{F}_q; T) &= 0!\#V(\mathbb{F}_q) + f(T). \end{aligned}$$

Por lo tanto, se cumple el caso base.

Hipótesis inductiva: Supongamos que es cierto para la n-ésima derivada.

$$\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T) = (n-1)!\#V(\mathbb{F}_{q^n}) + f(T),$$

donde

$$f(T) = \sum_{k=n+1}^{\infty}(k-1)!\#V(\mathbb{F}_{q^k})T^{n-k}.$$

Paso inductivo: Se demostrará que para $(n+1)$-ésima derivada también es verdadero. Por la hipótesis inductiva tenemos que

$$\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T) = (n-1)!\#V(\mathbb{F}_{q^n}) + f(T).$$

Derivando con respecto a T nuevamente se obtenemos

$$\begin{aligned}\frac{d^{n+1}}{dT^{n+1}}\log Z(V/\mathbb{F}_q;T) &= 0 + f'(T), \text{ donde } f', \text{ también es una función generatriz.}\\ &= f'(T)\\ &= n!\#V(\mathbb{F}_{q^{n+1}}) + \underbrace{\sum_{k=n+2}^{\infty}(k-1)!\#V(\mathbb{F}_{q^k})T^{n-k}}\\ \frac{d^{n+1}}{dT^{n+1}}\log Z(V/\mathbb{F}_q;T) &= n!\#V(\mathbb{F}_{q^{n+1}}) \; + \qquad\qquad g(T).\end{aligned}$$

Se concluye que el resultado también es cierto para $n+1$.
Ahora, tenemos que para $n \geq 1$ se cumple que la n-ésima derivada es

$$\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T) = (n-1)!\#V(\mathbb{F}_{q^n}) + f(T).$$

Seguidamente evaluamos en $T=0$:

$$\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T)\Big|_{T=0} = (n-1)!\#V(\mathbb{F}_{q^n}) + f(T).$$

Y notemos que $f(T)=0$; de este modo obtenemos el resultado deseado:

$$\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\left(\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T)\right)\Big|_{T=0}, \text{ para todo } n \geq 1.$$

■

Ejemplo 1.3.1. Si $V = \mathbb{P}^N$. Entonces los puntos del conjunto $V(\mathbb{F}_{q^n})$ están dados por las coordenadas homogéneas $[x_0 : x_1 : \cdots : x_N]$ para todo $x_i \in \mathbb{F}_{q^n}$ con al menos un x_i distinta de cero.
Para contabilizar el número de elementos de $V(\mathbb{F}_{q^n})$ notamos que para cada componente de una coordenada homogénea arbitraria $[x_0 : x_1 : \cdots : x_N]$ tenemos q^n formas de elección entonces por las $N+1$ componente se tiene en total

$$\underbrace{q^n \cdots q^n}_{N+1 \text{ veces}} = q^{n(N+1)}.$$

Como es posible tener dos coordenadas homogéneas que difieran por un elemento $\lambda \in \mathbb{F}_{q^n}^{\times}$ entonces tenemos $q^n - 1$ coordenadas repetidas y finalmente se debe restar la coordenada que está compuesta por componentes $x_i = 0$ para $i = 0, \ldots, N$. Por lo tanto, la cantidad puntos sobre $V(\mathbb{F}_{q^n})$ es:

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}.$$

Luego, por definición 1.3.3 se tiene

$$\begin{aligned}
\log Z(V/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} \underbrace{\#V(\mathbb{F}_{q^n})}\, \frac{T^n}{n} \\
&= \sum_{n=1}^{\infty} \left(\sum_{i=0}^{N} q^{ni} \right) \frac{T^n}{n} \\
&= \sum_{n=1}^{\infty} \left(1 + q^n + q^{2n} + \cdots + q^{Nn}\right) \frac{T^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{T^n}{n} + \sum_{n=1}^{\infty} \frac{(qT)^n}{n} + \cdots + \sum_{n=1}^{\infty} \frac{(q^N T)^n}{n}.
\end{aligned}$$

Del cálculo se sabe que la serie de potencias de $-\log(1-x)$ es

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}. \tag{1.7}$$

Entonces, utilizando la igualdad anterior resulta que

$$\begin{aligned}\log Z(V/\mathbb{F}_q;T) &= (-\log(1-T)) + (-\log(1-qT)) + \cdots + (-\log(1-q^NT)) \\ &= -\sum_{i=0}^{N}(\log(1-q^iT)) \\ &= -\log\left(\prod_{i=0}^{N}(1-q^iT)\right), \text{ por propiedad de suma de logaritmo} \\ Z(V/\mathbb{F}_q;T) &= \frac{1}{\prod_{i=0}^{N}(1-q^iT)}.\end{aligned}$$

Por lo tanto, la función zeta asociada a $V/\mathbb{F}_{q^n}$ es

$$Z(V/\mathbb{F}_q;T) = \frac{1}{(1-T)(1-qT)(1-q^2T)\cdots(1-q^NT)} \in \mathbb{Q}[T].$$

Teorema 1.3.1 (Conjeturas de Weil)**.** *Sea $V/\mathbb{F}_q$ una variedad proyectiva lisa de dimensión N.*

1. *Racionalidad:*

$$Z(V/\mathbb{F}_q;T) \in \mathbb{Q}[T].$$

2. *Ecuación funcional: Existe un entero ϵ, llamada la característica de Euler de V, tal que*

$$Z(V/\mathbb{F}_q;1/q^NT) = \pm q^{\frac{N\cdot\epsilon}{2}}T^{\epsilon}Z(V/\mathbb{F}_q;T).$$

3. *Hipótesis de Riemann: La función zeta se factoriza como*

$$Z(V/\mathbb{F}_q;T) = \frac{P_1(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)},$$

donde cada $P_i(T) \in \mathbb{Z}[T]$ con

$$P_0(T) = 1-T \;\; y \;\; P_{2N}(T) = 1-q^NT,$$

y tales que para cada $0 \leq i \leq 2N$, el polinomio $P_i(T)$ factoriza sobre $\mathbb{C}$ como

$$P_i(T) = \prod_{j=1}^{b_i}(1-\alpha_{ij}T) \;\; con \;\; |\alpha_{ij}| = q^{1/2}.$$

Nota 2. *En el caso de una curva elíptica $E/\mathbb{F}_q$, la característica de Euler $\epsilon = 0$ y su dimensión es $N = 1$.*

Las conjeturas de Weil para el caso de curvas y variedades abelianas fueron demostradas por André Weil en 1949. Para el caso general, la racionalidad fue probada por Dword en 1960. Años más tarde, con la teoría desarrollada por matemáticos como M. Artin y Grothendieck dieron otra prueba de la racionalidad y la ecuación funcional. Asimismo, en el año 1973 fue demostrado el análogo de la hipótesis de Riemann por Deligne como se menciona en el capítulo V, sección 2 de [14].

Teorema 1.3.2. *Sea E una curva elíptica sobre $\mathbb{F}_q$. Sea*

$$\begin{aligned} \phi : E &\to E \\ (x, y) &\mapsto (x^q, y^q), \end{aligned}$$

la q-ésima potencia del endomorfismo de Frobenius, y definimos

$$a = q + 1 - \#E(\mathbb{F}_q).$$

a) Sea $\alpha, \beta \in \mathbb{C}$ son raíces del polinomio $T^2 - aT + q$. Entonces α y β son conjugados complejos que satisface $|\alpha| = |\beta| = \sqrt{q}$, y para cada $n \geq 1$,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

b) El endomorfismo de Frobenius satisface que

$$\phi^2 - a\phi + q = 0 \text{ en } End(E).$$

Una demostración para este teorema utiliza resultados relacionados con módulos de Tate. Para mayores detalles sobre la misma puede consultar [14], capítulo V, sección 2.

La importancia del Teorema 1.3.2 es que facilita la comprobación de las conjeturas de Weil para el caso de las curvas elípticas, como se verifica en el siguiente teorema.

Teorema 1.3.3. *Sea $E/\mathbb{F}_q$ una curva elíptica. Entonces existe $a \in \mathbb{Z}$ tal que*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.$$

Además,

$$Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T),$$

y

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T) \text{ con } |\alpha| = |\beta| = \sqrt{q}.$$

Demostración. Sea $E/\mathbb{F}_q$ una curva elíptica. Por definición 1.3.3, la función zeta asociada a $E/\mathbb{F}_q$ es

$$Z(E/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty} \#E\left(\mathbb{F}_{q^n}\right)\frac{T^n}{n}\right).$$

Luego,

$$\begin{aligned}
\log\left(Z(E/\mathbb{F}_q;T)\right) &= \sum_{n=1}^{\infty} \#E\left(\mathbb{F}_{q^n}\right)\frac{T^n}{n} \\
&= \sum_{n=1}^{\infty}(q^n+1-\alpha^n-\beta^n)\frac{T^n}{n}, \text{ por el Teorema 1.3.2 } a). \\
&= \sum_{n=1}^{\infty}\frac{(qT)^n}{n} + \sum_{n=1}^{\infty}\frac{T^n}{n} - \sum_{n=1}^{\infty}\frac{(\alpha T)^n}{n} - \sum_{n=1}^{\infty}\frac{(\beta T)^n}{n} \\
&= -\log(1-qT) - \log(1-T) + \log(1-\alpha T) + \log(1-\beta T), \text{ por } (1.7) \\
&= -\log((1-T)(1-qT)) + \log((1-\alpha T)(1-\beta T)), \text{ por propiedad de logaritmo} \\
\log\left(Z(E/\mathbb{F}_q;T)\right) &= -\log((1-T)(1-qT)) + \log((1-\alpha T)(1-\beta T)) \\
\exp\left(\log\left(Z(E/\mathbb{F}_q;T)\right)\right) &= \exp\left(-\log((1-T)(1-qT)) + \log((1-\alpha T)(1-\beta T))\right) \\
Z(E/\mathbb{F}_q;T) &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.
\end{aligned}$$

Luego se obtiene que

$$Z(E/\mathbb{F}_q;T) = \frac{1-(\alpha+\beta)T+\alpha\beta T^2}{(1-T)(1-qT)}.$$

Tomando $a = \alpha+\beta$, donde $|\alpha| = |\beta| = \sqrt{q} \Rightarrow \alpha\beta = q$, por propiedad de números complejos*

$$a = \alpha+\beta = 2\text{Re}(\alpha) = 2\text{Re}(\beta).$$

Además,

$$\begin{aligned}
a &= q+1-\#E(\mathbb{F}_q) \\
\Rightarrow a &= 2\text{Re}(\alpha) = 2\text{Re}(\beta) \in \mathbb{Z}.
\end{aligned}$$

Por lo tanto,

$$Z(E/\mathbb{F}_q;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)} \in \mathbb{Q}[T].$$

■

*Para todo $z \in \mathbb{C},\ z\overline{z} = |z|^2$.

Ejemplo 1.3.2. Sea $E : y^2 = x^3 + x + 1$ una curva elíptica sobre el campo $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. Su lista de puntos sobre $\mathbb{F}_5$ es:

$$E(\mathbb{F}_5) = \{\infty, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

Entonces la cantidad de puntos es

$$\#E(\mathbb{F}_5) = 9 \Rightarrow a = 1 + 5 - 9 = -3.$$

En el espacio proyectivo esta es la curva descrita por la ecuación $ZY^2 = X^3 + Z^2X + Z^3$. Por el Teorema 1.3.3, la función zeta de $E/\mathbb{F}_5$ es

$$Z(E/\mathbb{F}_5; T) = \frac{1 + 3T + 5T^2}{(1-T)(1-5T)}.$$

Ejemplo 1.3.3. Para la curva elíptica $E : ZY^2 = X^3 + 2Z^3$ sobre $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$, por el ejemplo 1.2.4, sabemos que

$$\begin{aligned} \#E(\mathbb{F}_7) = 9 \Rightarrow a &= 1 + q - \#E(\mathbb{F}_7) = 1 + 7 - 9 = -1 \\ &\Rightarrow a = -1. \end{aligned}$$

Entonces la función zeta asociada a $E(\mathbb{F}_7)$ por el Teorema 1.3.3 es

$$Z(E/\mathbb{F}_7; T) = \frac{1 + T + 7T^2}{(1-T)(1-7T)}.$$

Luego,

$$1 + T + 7T^2 = 0 \Rightarrow (1 - \alpha T)(1 - \beta T) = 0.$$

donde las raíces del polinomio son conjugados complejos:

$$\begin{aligned} \alpha' &= \frac{-1}{14} + \frac{3\sqrt{3}}{14}i, \\ \beta' &= \frac{-1}{14} - \frac{3\sqrt{3}}{14}i. \end{aligned}$$

Por propiedades de números complejos, los coeficientes α y β son

$$\begin{aligned} \alpha &= \frac{\overline{\alpha'}}{|\alpha'|^2} = \frac{-1}{2} - \frac{3\sqrt{3}i}{2}, \\ \beta &= \frac{\overline{\beta'}}{|\beta'|^2} = \frac{-1}{2} + \frac{3\sqrt{3}i}{2}. \end{aligned}$$

Además, se cumple que

$$|\alpha| = |\beta| = \sqrt{7}.$$

Por el Teorema 1.3.2, la cantidad de puntos en $E(\mathbb{F}_{7^n})$ está dada por

$$\#E(\mathbb{F}_{7^n}) = 7^n + 1 - \left(\frac{-1}{2} - \frac{3\sqrt{3}i}{2}\right)^n - \left(\frac{-1}{2} + \frac{3\sqrt{3}i}{2}\right)^n, \text{ con } n \geq 1.$$

Nota 3. *Para una curva elíptica $E/\mathbb{F}_q$ de función zeta 1.3.3 con un cambio de variable $T = q^{-s}$,*

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q; q^{-s}) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}.$$

- $\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1-s)$ *satisface la ecuación funcional, puesto que*

$$\begin{aligned}\zeta_{E/\mathbb{F}_q}(s) &= \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})} \\ &= \frac{q^{1-2s}(q^{2s-1} - aq^{s-1} + 1)}{q^{1-2s}(q^s - 1)(q^{s-1} - 1)} \\ &= \frac{1 - aq^{s-1} + q^{2s-1}}{(q^s - 1)(q^{s-1} - 1)} \\ &= \zeta_{E/\mathbb{F}_q}(1-s).\end{aligned}$$

- *Se comprueba la hipótesis de Riemann: si $\zeta_{E/\mathbb{F}_q}(s) = 0$ entonces $|q^s| = \sqrt{q}$.*

Capítulo 2

Funciones simétricas

2.1. Funciones simétricas homogéneas

En este apartado nos enfocamos en estudiar la definición de función simétrica homogénea, ejemplos y algunos tipos de funciones simétricas tales como: funciones simétricas homogéneas elementales, completas y de potencias. Para un estudio más detallado sobre funciones simétricas, se recomienda ver [17].

Definición 2.1.1. *Sea $x = (x_1, x_2, \ldots, x_k)$ un conjunto de variables y $n \in \mathbb{N}$. Una **función simétrica homogénea** de grado n sobre un anillo conmutativo R (con identidad) es una serie formal de potencias*

$$f(x) = \sum_{\alpha} c_\alpha x^\alpha,$$

donde

(a) $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ *recorre $k-$ uplas de enteros no negativos que suman n.*

(b) *Cada $c_\alpha \in R$.*

(c) x^α *representa el monomio $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}$.*

(d) $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_k)$ *para cada permutación σ de los enteros positivos $1, 2, \ldots, n$.*

El conjunto de las funciones simétricas de grado n sobre un anillo R es denotado por Λ_R^n y recibe la estructura de $R-$módulo con las operaciones de suma y producto por escalar. Esto se plantea en la siguiente proposición, cuya demostración es inmediata.

Proposición 2.1.1. *Sea Λ_R^n el conjunto de funciones simétricas de grado $n \geq 0$ sobre un anillo conmutativo R. Este es un R-módulo respecto a las operaciones de suma y producto por escalar definidas como:*

- *Para todo $f, g \in \Lambda_R^n$ y $x = (x_1, \ldots, x_k)$ un conjunto de k variables, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ una k-upla de enteros positivos que suman n*

$$\begin{aligned} \Lambda_R^n \times \Lambda_R^n &\to \Lambda_R^n \\ (f, g) &\mapsto f + g := \sum_\alpha (a_\alpha + b_\alpha) x^\alpha. \end{aligned}$$

- *Para todo $r \in R$ y $f \in \Lambda_R^n$*

$$\begin{aligned} R \times \Lambda_R^n &\to \Lambda_R^n \\ (r, f) &\mapsto r \cdot f := \sum_\alpha (r \cdot a_\alpha) x^\alpha. \end{aligned}$$

El conjunto de funciones simétricas sobre un anillo conmutativo R es denotado por Λ_R. Es posible definir el conjunto de funciones simétricas como suma directa de funciones simétricas homogéneas de grado $n \geq 0$.

Proposición 2.1.2. *Sea Λ_R el conjunto de funciones simétricas sobre R se tiene la siguiente descomposición en suma directa:*

$$\Lambda_R = \Lambda_R^0 \oplus \Lambda_R^1 \oplus \cdots .$$

En otras palabras,

$$\Lambda_R = \{f = f_0 + f_1 + \cdots : \forall f_n \in \Lambda_R^n,\ f_n = 0, \textit{salvo un número finito de casos}\}.$$

Por otra parte, el conjunto de funciones simétricas Λ_R también cumple con ser una R - álgebra, usualmente conocida como **álgebra de funciones simétricas**.

Proposición 2.1.3. *El conjunto Λ_R de funciones simétricas sobre R recibe la estructura de R- álgebra:*

1. *Λ_R es un anillo con las operaciones definidas como:*

   - *Suma de funciones: $\forall h, f \in \Lambda_R$,*

   $$h + f := \sum_\alpha (a_\alpha + b_\alpha) x^\alpha.$$

   - *Producto de funciones simétricas: Si $h \in \Lambda_R^n$ y $f \in \Lambda_R^m$,*

   $$h \cdot f := \sum_{\alpha+\beta} (a_\alpha b_\beta) x^{\alpha+\beta}.$$

2. *Λ_R posee un homomorfismo definido por:*

$$\begin{aligned} \omega : R &\to \Lambda_R \\ r &\mapsto r \cdot \sum_\alpha c_\alpha x^\alpha. \end{aligned}$$

Este homomorfismo otorga a Λ_R una multiplicación escalar que coincide con la proposición 2.1.1.

Ejemplo 2.1.1. Si $R = \mathbb{Q}$, el conjunto de funciones simétricas sobre $\mathbb{Q}$ es un $\mathbb{Q}$ espacio vectorial.

Nota 4. *Para efectos del presente trabajo, será suficiente considerar funciones simétricas sobre $R = \mathbb{Q}$ y $R = \mathbb{Z}$.*

Ya definimos el conjunto de funciones simétricas y su estructura. Ahora nos enfocaremos en estudiar tipos de funciones simétricas homogéneas, por lo que iniciamos con la definición de función simétrica elemental.

Definición 2.1.2. *Para cada entero positivo k, definimos la* ***función simétrica homogénea elemental***

$$e_k = \sum_{i_1<\cdots<i_k} x_{i_1}\cdots x_{i_k},\ k \geq 1,\ \textit{con}\ e_0 = 1.$$

En otras palabras, e_k es la suma de todos los productos de k variables distintas.

Ejemplo 2.1.2. En este ejemplo se muestran funciones simétricas elementales, donde n representa el número de variables

$n = 2$	$n = 3$	$n = 4$
$e_0 = 1$	$e_0 = 1$	$e_0 = 1$
$e_1 = x_1 + x_2$	$e_1 = x_1 + x_2 + x_3$	$e_1 = x_1 + x_2 + x_3 + x_4$
$e_2 = x_1x_2$	$e_2 = x_1x_2 + x_1x_3 + x_2x_3$	$e_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$
$e_3 = 0$	$e_3 = x_1x_2x_3$	$e_3 = x_1x_2x_3 + x_1x_2x_4 + x_2x_3x_4 + x_1x_3x_4$
	$e_4 = 0$	$e_4 = x_1x_2x_3x_4$
		$e_5 = 0$

Definición 2.1.3. *Para cada entero positivo k, definimos la* ***función simétrica homogénea completa***

$$h_k = \sum_{i_1\leq\cdots\leq i_k} x_{i_1}\cdots x_{i_k},\ k \geq 1\ \textit{con}\ h_0 = 1.$$

h_k, es la suma de todos los productos de k variables no necesariamente distintas.

Ejemplo 2.1.3. En este ejemplo se muestran funciones simétricas completas donde n representa el número de variables y k el grado:

$n=2$	$n=3$
$h_0 = 1$	$h_0 = 1$
$h_1 = x_1 + x_2$	$h_1 = x_1 + x_2 + x_3$
$h_2 = x_1x_2 + x_1^2 + x_2^2$	$h_2 = x_1x_2 + x_1x_3 + x_2x_3 + x_1^2 + x_2^2 + x_3^2$
$h_3 = x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^3$	$h_3 = x_1x_2x_3 + x_1^2x_2 + x_1^2x_3 + x_2^2x_3 + x_1x_2^2 + x_1x_3^2$
$h_4 = x_1^3x_2 + x_1x_2^3 + x_1^2x_2^2 + x_1^4 + x_2^4$	$+x_2x_3^2 + x_1^3 + x_2^3 + x_3^3$

$n = 4$

$$h_0 = 1$$
$$h_1 = x_1 + x_2 + x_3 + x_4$$
$$h_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_1^2 + x_2^2 + x_3^2 + x_4^2$$
$$h_3 = x_1x_2x_3 + x_2x_3x_4 + x_1^2x_2 + x_1^2x_3 + x_1^2x_4 + x_2^2x_3 + x_2^2x_4 + x_1x_2^2 + x_3^2x_1 + x_3^2x_2 + x_3^2x_4 + x_4^2x_1 + x_4^2x_2 + x_4^2x_3 + x_1^3 + x_2^3 + x_3^3 + x_4^3$$
$$h_4 = x_1x_2x_3x_4 + x_1^2x_2x_3 + x_1^2x_2x_4 + x_1^2x_3x_4 + x_2^2x_1x_3 + x_2^2x_1x_4 + x_2^2x_3x_4 + x_3^2x_1x_2 + x_3^2x_1x_4 + x_4^2x_1x_2 + x_4^2x_1x_3 + x_1^2x_2^2 + x_1^2x_3^2 + x_1^2x_4^2 + x_2^2x_3^2 + x_1^2x_4^2 + x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2 + x_1^4 + x_2^4 + x_3^4 + x_4^4.$$

Proposición 2.1.4. *Las funciones simétricas elementales e_k y completas h_k en n variables cumplen las siguientes propiedades al evaluar $x_1 = x_2 = \cdots = x_n = 1$:*

(a)

$$e_k(1, \ldots, 1) = \sum_{i_1 < \cdots < i_k} 1 = \binom{n}{k}.$$

(b)

$$h_k(1, \ldots, 1) = \sum_{i_1 \leq \cdots \leq i_k} 1 = \binom{n+k-1}{k}.$$

Demostración. Consideremos una función simétrica elemental e_k y la completa h_k con n variables $x_1, x_2, \ldots, x_n$.

(a) Por hipótesis se tiene que

$$e_k(1, \ldots, 1) = \sum_{i_1 < \cdots < i_k} 1 = \binom{n}{k}.$$

Por definición de función simétrica elemental, sabemos que e_k es la suma de monomios de k variables distintas; entonces el resultado de evaluar $x_1 = x_2 = \cdots = x_n = 1$ se entiende como la cantidad de monomios de e_k.

Luego el problema es equivalente a encontrar la cantidad de configuraciones distintas con k variables.

En total tenemos n variables entonces el número de formas de escoger k variables distintas es por definición el número combinatorio:

$$\binom{n}{k}.$$

Por lo tanto,

$$e_k(1,\ldots,1) = \binom{n}{k}.$$

(b) Por definición de función simétrica homogénea completa tenemos que h_k es de la forma

$$h_k = \sum_{i_1 <\cdots< i_k} x_{i_1}\cdots x_{i_k}.$$

Evaluando $x_1 = x_2 = \cdots = x_n = 1$ se obtiene que

$$h_k(\underbrace{1,\ldots,1}_{n \text{ veces}}) = \sum_{i_1 <\cdots< i_k} 1.$$

Ahora notemos que el resultado del sumatorio se puede interpretar como el número de monomios de h_k. Por lo que procedemos a demostrar el resultado por medio de un conteo, en el cual se permite la repetición de variables por definición de h_k.

Tenemos n variables distintas entre si, con la restricción que para cada término de h_k, la suma de los exponentes sea k. Luego, por el método de separadores consideramos las n variables como objetos del mismo tipo y elegimos $n-1$ separadores es decir:

En total tendremos, $n-1+k$ espacios disponibles y finalmente se eligen los k objetos. Entonces el total de configuraciones es igual al número combinatorio.

$$\binom{n+k-1}{k}.$$

Por lo tanto,

$$h_k(1,\ldots,1) = \binom{n+k-1}{k}.$$

■

Finalmente, definimos otro tipo de funciones simétricas homogéneas.

Definición 2.1.4. *Para cada entero positivo k, definimos la* ***función simétrica homogénea de potencias***

$$p_k = \sum_i x_i^k,\ k \geq 1 \text{ con } p_0 = 1.$$

Ejemplo 2.1.4. A continuación se muestran ejemplos de funciones simétricas de potencias para $n = 2, 3, 4$ y k distintos:

$n = 2$	$n = 3$	$n = 4$
$p_0 = 1$	$p_0 = 1$	$p_0 = 1$
$p_1 = x_1 + x_2$	$p_1 = x_1 + x_2 + x_3$	$p_1 = x_1 + x_2 + x_3 + x_4$
$p_2 = x_1^2 + x_2^2$	$p_2 = x_1^2 + x_2^2 + x_3^2$	$p_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$
$p_3 = x_1^3 + x_2^3$	$p_3 = x_1^3 + x_2^3 + x_3^3$	$p_3 = x_1^3 + x_2^3 + x_3^3 + x_4^3$
$p_4 = x_1^4 + x_2^4$	$p_4 = x_1^4 + x_2^4 + x_3^4$	$p_4 = x_1^4 + x_2^4 + x_3^4 + x_4^4$
$p_5 = x_1^5 + x_2^5$	$p_5 = x_1^5 + x_2^5 + x_3^5$	$p_5 = x_1^5 + x_2^5 + x_3^5 + x_4^5$

De los ejemplos anteriores sobre funciones simétricas elementales, completas y de potencias, notamos que para ciertos grados y número de variables, algunas de las funciones simétricas resultan ser la misma. Verificamos esta relación en los siguientes ejemplos.

Ejemplo 2.1.5. En este ejemplo, mostramos casos específicos de cómo las funciones simétricas elementales, completas y de potencias están relacionadas:

- La función simétrica de potencias de grado $k = 2$, $n = 2$ variables y $R = \mathbb{Z}$:

$$p_2 = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = e_1^2 - 2e_2.$$

- La función simétrica de completa de grado $k = 3$, $n = 2$ variables y $R = \mathbb{Z}$:

$$\begin{aligned} h_3 &= x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^3 \\ &= (x_1 + x_2)^3 - 2x_1x_2(x_1 + x_2) \\ h_3 &= e_1^3 - 2e_2e_1. \end{aligned}$$

- La función simétrica elemental de grado $k = 2$, $n = 2$ variables y $R = \mathbb{Q}$:

$$e_2 = x_1x_2 = \frac{(x_1 + x_2)^2 - (x_1^2 + x_2^2)}{2} = \frac{1}{2}p_1^2 + \left(-\frac{1}{2}p_2\right).$$

Por otra parte, a pesar de que existen muchas bases para las funciones simétricas podemos destacar tres tipos de bases que son de importancia; dichas bases son claramente las que involucran los tres tipos especiales de funciones simétricas estudiadas en este apartado, como se establece en la siguiente proposición.

Proposición 2.1.5. *Una partición λ de un entero positivo n, es una k-upla $(\lambda_1, \ldots, \lambda_k)$ donde $\sum_{i=1}^{k} \lambda_i = n$. Sea Par $:= \bigcup_{n\geq 0}$ Par(n), es el conjunto de todas las particiones de enteros positivos. Entonces*

$$\{h_\lambda = h_{\lambda_1} \cdots h_{\lambda_k}\}, \{e_\lambda = e_{\lambda_1} \cdots e_{\lambda_k}\}, \{p_\lambda = p_{\lambda_1} \cdots p_{\lambda_k}\},\ \textit{con}\ \lambda = (\lambda_1, \ldots, \lambda_k) \in \textit{Par}$$

son bases para Λ_R.

Una demostración de este resultado utilizando matrices de cambio de base y funciones simétricas monomiales (las cuales no serán definidas en este trabajo), puede revisarse en [17].

Ejemplo 2.1.6. En concreto, si tomamos a $n = 3$ de modo que

$$\text{Par} := \bigcup_{n=0}^{3} \text{Par}(n).$$

La base formada por funciones simétricas elementales para

$$\Lambda_R = \Lambda_R^0 \oplus \Lambda_R^1 \oplus \Lambda_R^2 \oplus \Lambda_R^3,$$

está conformada por

$$B = \{e_0, e_1, e_2, e_{11}, e_3, e_{21}, e_{111}\},$$

con particiones hasta $n = 3$ los elementos de B son de la forma:

$$\begin{aligned}
e_0 &= 1 \\
e_1 &= x_1 + x_2 + x_3 \\
e_2 &= x_1x_2 + x_1x_3 + x_2x_3 \\
e_{11} &= e_1 \cdot e_1 = x_1^2 + 2x_1x_2 + 2x_3x_1 + 2x_2x_3 + x_2^2 + x_3^2 \\
e_3 &= x_1x_2x_3 \\
e_{21} &= e_2 \cdot e_1 = (x_1x_2 + x_1x_3 + x_2x_3)(x_1 + x_2 + x_3) \\
e_{111} &= e_1 \cdot e_1 \cdot e_1 = (x_1 + x_2 + x_3)^3.
\end{aligned}$$

Por ejemplo la función simétrica

$$f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1x_3 + 3x_1x_2x_3.$$

En la base B es

$$f(x_1, x_2, x_3) = e_2 + 3e_3.$$

Ejemplo 2.1.7. Otro ejemplo tomando a $R = \mathbb{Q}$ y la función simétrica $f(x_1, x_2) = x_1 + x_2 + 3x_1x_2 + 2$. Siempre consideremos que $\text{Par} = \bigcup_{n=0}^{3} \text{Par}(n)$ y las bases son de la forma

$$\begin{aligned} B_e &= \{e_0, e_1, e_2, e_{11}, e_3, e_{21}, e_{111}\}, \\ B_h &= \{h_0, h_1, h_2, h_{11}, h_3, h_{21}, h_{111}\}, \\ B_p &= \{p_0, p_1, p_2, p_{11}, p_3, p_{21}, p_{111}\}. \end{aligned}$$

Podemos escribir de manera explícita los elementos de las bases recurriendo a la definición de función simétrica homogénea correspondiente.

Para el caso de B_e los elementos son de la forma

$$\begin{aligned} e_0 &= 1, \\ e_1 &= x_1 + x_2, \\ e_2 &= x_1x_2, \\ e_{11} &= e_1 \cdot e_1 = (x_1 + x_2) \cdot (x_1 + x_2) = (x_1 + x_2)^2, \\ e_3 &= 0, \\ e_{21} &= e_2 \cdot e_1 = (x_1x_2)(x_1 + x_2) = x_1^2x_2 + x_1x_2^2, \\ e_{111} &= e_1 \cdot e_1 \cdot e_1 = (x_1 + x_2)^3. \end{aligned}$$

Los elementos de B_h por definición de función simétrica homogénea completa son

$$\begin{aligned} h_0 &= 1, \\ h_1 &= x_1 + x_2, \\ h_2 &= x_1x_2 + x_1^2 + x_2^2, \\ h_{11} &= (x_1 + x_2) \cdot (x_1 + x_2) = (x_1 + x_2)^2, \\ h_3 &= x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^3, \\ h_{21} &= (x_1x_2 + x_1^2 + x_2^2)(x_1 + x_2), \\ h_{111} &= (x_1 + x_2)(x_1 + x_2)(x_1 + x_2) = (x_1 + x_2)^3. \end{aligned}$$

Por último, los elementos de B_p son de la forma

$$\begin{aligned} p_0 &= 1, \\ p_1 &= x_1 + x_2, \\ p_2 &= x_1^2 + x_2^2, \\ p_{11} &= p_1 \cdot p_1 = (x_1 + x_2) \cdot (x_1 + x_2) = (x_1 + x_2)^2, \\ p_3 &= x_1^3 + x_2^3, \\ p_{21} &= p_2 \cdot p_1 = (x_1^2 + x_2^2)(x_1 + x_2), \\ p_{111} &= (x_1 + x_2)(x_1 + x_2)(x_1 + x_2) = (x_1 + x_2)^3. \end{aligned}$$

Luego, con ayuda de la información anterior obtenemos que f escrito en términos de las bases es

$$\begin{aligned} f(x_1, x_2) &= 2e_0 + 3e_2 + e_1, \text{ en la base } B_e, \\ f(x_1, x_2) &= 2h_0 + h_1 - 3h_2 + 3h_{11}, \text{ en la base } B_h, \\ f(x_1, x_2) &= 2p_0 + p_1 - \frac{3}{2}p_2 + \frac{3}{2}p_{11}, \text{ en la base } B_p. \end{aligned}$$

2.2. Pletismo

En este apartado, estudiamos un resultado sobre funciones simétricas llamado pletismo, que se puede entender como una sustitución de funciones, pues en algunos contextos es parecido a la composición de funciones. Para desarrollar este tema se ha tomado como referencia a [17] y [8].

Definición 2.2.1. *Sea $f \in \Lambda_R$ expresado como una suma de monomios, es decir $f = \sum_{i\geq 0} x^{\alpha_i}$. Dado $g \in \Lambda_R$, definimos el **pletismo** $g[f]$ (a veces denotado como $f \circ g$) por*

$$g[f] = g(x^{\alpha_1}, x^{\alpha_2}, \dots).$$

Conviene tener en cuenta que, para cualesquiera $f, g \in \Lambda_R$ el pletismo $g[f]$ es definido cuando el número de monomios en f es igual al número de variables en g.

Ejemplo 2.2.1. Consideremos la función simétrica elemental

$$e_2 = x_1x_2 + x_1x_3 + x_2x_3$$

y la función simétrica de potencias

$$p_2 = x_1^2 + x_2^2 + x_3^2.$$

El pletismo de e_2 y p_2 es

$$\begin{aligned} e_2[p_2] &= e_2(x_1^2, x_2^2, x_3^2) \\ &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2. \end{aligned}$$

Un ejemplo más general es el que se muestra a continuación.

Ejemplo 2.2.2. Sea $f \in \Lambda_R$ una función simétrica expresada como

$$f = \sum_{i\geq 0} x^{\alpha_i},$$

y sea p_k una función simétrica de potencias de grado k. El pletismo $f[p_k]$ es

$$\begin{aligned} f[p_k] &= f(x_1^k, x_2^k, \dots, x_n^k) \\ &= \sum_{i\geq 0} x^{\alpha_i k} = p_k[f]. \end{aligned}$$

Por lo tanto,

$$f[p_k] = p_k[f].$$

Del ejemplo anterior, notamos que la operación definida por el pletismo está relacionada con las funciones simétricas homogéneas de potencias. Más adelante veremos una definición de pletismo que verifica dicha afirmación.

Ahora, estudiemos algunas propiedades sobre el pletismo de funciones simétricas:

Proposición 2.2.1. *Sean $f, g, h \in \Lambda_R$ y para todo $a, b \in R$. Se cumplen las siguientes propiedades*

(a) $(af + bg)[h] = af[h] + bg[h]$.

(b) $(fg)[h] = f[h] \cdot g[h]$.

Demostración. Sean $f, g, h \in \Lambda_R$ y $a, b \in R$ y además consideremos que h es de la forma

$$h = \sum_{i \geq 0} x^{\alpha_i}.$$

- $(af + bg)[h] = af[h] + bg[h]$.

  Partiendo del lado izquierdo de la igualdad:

  $$\begin{aligned}(af + bg)[h] &= (af + bg)(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ por definición de pletismo,}\\ &= (af)(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}) + (bg)(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ por definición de suma}\\ &\qquad\qquad \text{ya que } af, bg \in \Lambda_R,\\ &= af(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}) + bg(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ porque } a, b \in R.\\ &= af[h] + bg[h], \text{ por definición de pletismo.}\end{aligned}$$

  Ahora partimos del lado derecho de la igualdad,

  $$\begin{aligned}af[h] + bg[h] &= af(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}) + bg(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ por definición de pletismo,}\\ &= (af + bg)(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ por definición de suma de } f, g \in \Lambda_R,\\ &= (af + bg)[h], \text{ por definición de pletismo.}\end{aligned}$$

- $(fg)[h] = f[h] \cdot g[h]$.
  Partimos del lado izquierdo de la igualdad :

  $$\begin{aligned}(fg)[h] &= (fg)(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ por definición de pletismo,}\\ &= f(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n})g(x_1^{\alpha_1}, x_2^{\alpha_2}, \ldots, x_n^{\alpha_n}), \text{ ya que } f, g \in \Lambda_R,\\ &= f[h]g[h], \text{por definición de pletismo.}\end{aligned}$$

Por lo tanto, el enunciado es verdadero. ■

Es posible definir el pletismo para cualquier función simétrica, tomando la base de las funciones simétricas de potencias.

Definición 2.2.2. *Sean $f, g \in \Lambda_R$, tal que*

$$g = \sum_{\lambda} c_\lambda p_\lambda, \quad \textit{con } \lambda \in \textit{Par}, \ \textit{y } c_\lambda \ \textit{ escalar.}$$

Entonces,

$$g[f] = \sum_{\lambda} c_\lambda p_\lambda[f] = \sum_{\lambda} c_\lambda \prod_{i=1}^{\ell(\lambda)} f(x_1^{\lambda_i}, x_2^{\lambda_i}, \ldots, x_n^{\lambda_i}),$$

donde $\ell(\lambda)$ es la longitud de la partición λ.

Para comprender de manera más precisa la definición, revisemos ejemplos de cómo utilizarla.

Ejemplo 2.2.3. Vamos a calcular el pletismo, dadas dos funciones simétricas

$$f(x_1, x_2) = x_1^2 - 2x_1x_2 + x_2^2$$

y con las particiones de $n = 2$, construimos una función simétrica de la forma

$$g(x_1, x_2) = c_1 p_{11} + c_2 p_2,$$

con $p_{11} = p_1 \cdot p_1$ y $c_1, c_2 \in \mathbb{Z}$. Por la definición 2.2.2, calculamos el pletismo de g

$$\begin{aligned} g[f] &= c_1 f(x_1^1, x_2^1) f(x_1^1, x_2^1) + c_2 f(x_1^2, x_2^2) \\ &= c_1(x_1^2 - 2x_1x_2 + x_2^2)^2 + c_2(x_1^4 - 2x_1^2x_2^2 + x_2^4) \\ &= (c_1 + c_2)x_1^4 + (c_1 + c_2)x_2^4 + (6c_1 - 2c_2)x_1^2x_2^2 - 4c_1x_1^3x_2 - 4c_1x_1x_2^3. \end{aligned}$$

Por lo tanto,

$$g[f] = (c_1 + c_2)x_1^4 + (c_1 + c_2)x_2^4 + (6c_1 - 2c_2)x_1^2x_2^2 - 4c_1x_1^3x_2 - 4c_1x_1x_2^3.$$

Ejemplo 2.2.4. Ahora consideremos un ejemplo de pletismo con funciones simétricas sobre $R = \mathbb{Q}$. Por el ejemplo 2.1.7, sabemos que

$$f(x_1, x_2) = 2p_0 + p_1 - \frac{3}{2}p_2 + \frac{3}{2}p_{11},$$

en la base formada por las funciones simétricas de potencias. Para este caso, vamos a calcular el pletismo de f y h_3, por la definición 2.2.2:

$$\begin{aligned}
f[h_3] &= 2p_0[h_3] + p_1[h_3] - \frac{3}{2}p_2[h_3] + \frac{3}{2}p_{11}[h_3], \\
&= 2h_3(x_1^0, x_2^0) + h_3(x_1^1, x_2^1) - \frac{3}{2}h_3(x_1^2, x_2^2) + \frac{3}{2}h_3(x_1^1, x_2^1) \cdot h_3(x_1^1, x_2^1), \text{ por definición de pletismo,} \\
&= 2(4) + \left(x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^3\right) - \frac{3}{2}\left(x_1^4x_2^2 + x_1^2x_2^4 + x_1^6 + x_2^6\right) \\
&+ \frac{3}{2}\left(x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^2\right)^2.
\end{aligned}$$

Por lo tanto, el pletismo de f y h_3 es

$$f[h_3] = 8 + \left(x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^3\right) - \frac{3}{2}\left(x_1^4x_2^2 + x_1^2x_2^4 + x_1^6 + x_2^6\right) + \frac{3}{2}\left(x_1^2x_2 + x_1x_2^2 + x_1^3 + x_2^2\right)^2.$$

Capítulo 3

Propiedades de los coeficientes N_k de la función $Z(E/\mathbb{F}_q;T)$

En este capítulo, se abordarán diversos resultados que relacionan los coeficientes N_k de la función $Z(E/\mathbb{F}_q;T)$ de una curva elíptica E sobre un campo finito $\mathbb{F}_q$ con los números de Fibonacci, Lucas y teoría de Grafos correspondientes al artículo [12] secciones 2 y 3.

Notación:[*] $\lambda = \langle 1^{d_1} 2^{d_2} \cdots k^{d_r} \rangle$ es una partición de $k \in \mathbb{N}$.

3.1. N_k como una suma alternante

Las conjeturas de Weil son resultados útiles para estudiar las curvas elípticas. En este apartado, se presentan propiedades que se derivan de la racionalidad de la función zeta de una curva C de género $g \geq 1$.

$$Z(C/\mathbb{F}_q;T) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_{2g}T)}{(1-T)(1-qT)}. \tag{3.1}$$

para todo $\alpha_i \in \mathbb{C}$.
En particular, la función zeta para curvas elípticas queda expresada de la forma

$$Z(E/\mathbb{F}_q;T) = \frac{1-(\alpha_1+\alpha_2)T+\alpha_1\alpha_2 T^2}{(1-T)(1-qT)},$$

puesto que el género de la curva es $g = 1$.

Un resultado interesante que surge a raíz de la racionalidad de una función zeta asociada a una curva C, es el que permite calcular los coeficientes N_k en término de q y las raíces del polinomio del numerador en la expresión (3.1).

[*] Salvo que se indique lo contrario utilizaremos esta notación para particiones de $k \in \mathbb{N}$.

Proposición 3.1.1 ([12]). *Sea C una curva sobre un campo finito $\mathbb{F}_q$ de género $g \geq 1$. Los coeficientes N_k, satisfacen la siguiente relación:*

$$N_k = 1 + q^k - \alpha_1^k - \alpha_2^k - \cdots - \alpha_{2g}^k.$$

Demostración. Consideremos la función zeta de una curva C sobre un campo finito $\mathbb{F}_q$ definida por

$$Z(C/\mathbb{F}_q; T) = \exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right).$$

Por la racionalidad de la función $Z(C/\mathbb{F}_q; T)$ tenemos

$$\exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_{2g}T)}{(1-T)(1-qT)}$$

aplicando logaritmo a ambos lados de la ecuación

$$\sum_{k\geq 1} N_k \frac{T^k}{k} = \log\left(\frac{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_{2g}T)}{(1-T)(1-qT)}\right),$$

$$\sum_{k\geq 1} N_k \frac{T^k}{k} = \log((1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_{2g}T)) - \log((1-T)(1-qT))$$

$$\sum_{k\geq 1} N_k \frac{T^k}{k} = \log(1-\alpha_1 T) + \log(1-\alpha_2 T) + \cdots + \log(1-\alpha_{2g}T) - \log(1-T) - \log(1-qT)$$

$$\sum_{k\geq 1} N_k \frac{T^k}{k} = \sum_{i=1}^{2g} \log(1-\alpha_i T) - \log(1-T) - \log(1-qT).$$

Derivando con respecto a T

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{i=1}^{2g} \frac{-\alpha_i}{1-\alpha_i T} + \frac{1}{1-T} + \frac{q}{1-qT}$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{i=1}^{2g} (-\alpha_i) \underbrace{\left(\frac{1}{1-\alpha_i T}\right)} + \frac{1}{1-T} + q\left(\frac{1}{1-qT}\right)$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{i=1}^{2g} (-\alpha_i) \left(\sum_{k\geq 1} (\alpha_i T)^{k-1}\right) + \sum_{k\geq 1} T^{k-1} + q\left(\sum_{k\geq 1} (qT)^{k-1}\right)$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{i=1}^{2g} (-\alpha_i) \left(\sum_{k\geq 1} \alpha_i^{k-1} T^{k-1}\right) + \sum_{k\geq 1} T^{k-1} + q\left(\sum_{k\geq 1} q^{k-1} T^{k-1}\right)$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{i=1}^{2g} \left(\sum_{k\geq 1} \left(-\alpha^k\right) T^{k-1}\right) + \sum_{k\geq 1} T^{k-1} + \sum_{k\geq 1} q^k T^{k-1}$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{k\geq 1} (\sum_{i=1}^{2g} \left(-\alpha_i^k\right) T^{k-1} + \sum_{k\geq 1} \left(1+q^k\right) T^{k-1}$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{k\geq 1} \left(\sum_{i=1}^{2g} \left(-\alpha_i^k\right) + 1 + q^k\right) T^{k-1}$$

$$\sum_{k\geq 1} N_k T^{k-1} = \sum_{k\geq 1} \left(1 + q^k - \alpha_1^k - \alpha_2^k - \cdots - \alpha_{2g}^k\right) T^{k-1}.$$

Por igualdad componente a componente

$$N_k = 1 + q^k - \alpha_1^k - \alpha_2^k - \cdots - \alpha_{2g}^k.$$

■

Para el caso de una curva elíptica E, los coeficientes N_k quedan determinados por

$$N_k = 1 + q^k - \alpha_1^k - \alpha_2^k.$$

Los coeficientes N_k, satisfacen una relación de recurrencia tal como lo indica Silverman en [14], ejercicio propuesto 5.13, Capítulo V.

Proposición 3.1.2. *Sea E una curva elíptica en $\mathbb{F}_q$, para cada $k \geq 1$ se satisface que*

$$1 + q^{k+1} - N_{k+1} = (1 + q - N_1)(1 + q^k - N_k) - q(1 + q^{k-1} - N_{k-1}).$$

Demostración. Sea E una curva elíptica en $\mathbb{F}_q$ y N_k los coeficientes de su función $Z(E/\mathbb{F}_q; T)$ asociada, se quiere demostrar que

$$\alpha_1^k + \alpha_2^k = 1 + q^k - N_k,$$

de forma equivalente se mostrará que se satisface la recurrencia

$$\alpha_1^{k+1} + \alpha_2^{k+1} = (\alpha_1 + \alpha_2)\left(\alpha_1^k + \alpha_2^k\right) - q\left(\alpha_1^{k-1} + \alpha_2^{k-1}\right)$$

para $k \geq 2$ y condiciones iniciales $\alpha_1 + \alpha_2 = 1 + q - N_1$ y $\alpha_1^0 + \alpha_2^0 = 2$.
Casos base:

- Si $k = 2$ tenemos que

$$\begin{aligned}(\alpha_1 + \alpha_2)\left(\alpha_1^1 + \alpha_2^1\right) - q\left(\alpha_1^0 + \alpha_2^0\right) &= \alpha_1\alpha_1 + \alpha_1\alpha_2 + \alpha_2\alpha_1 + \alpha_2\alpha_2 - 2q, \\ &= \alpha_1^2 + 2q + \alpha_2^2 - 2q, \\ (\alpha_1 + \alpha_2)\left(\alpha_1^1 + \alpha_2^1\right) - q\left(\alpha_1^0 + \alpha_2^0\right) &= \alpha_1^2 + \alpha_2^2.\end{aligned}$$

- Si $k = 3$.

$$\begin{aligned}(\alpha_1 + \alpha_2)\left(\alpha_1^2 + \alpha_2^2\right) - q\left(\alpha_1 + \alpha_2\right) &= \alpha_1\alpha_1^2 + \alpha_1\alpha_2^2 + \alpha_2\alpha_1^2 + \alpha_2\alpha_2^2 - q\alpha_1 - q\alpha_2 \\ &= \alpha_1^3 + q\alpha_2 + q\alpha_1 + \alpha_2^3 - q\alpha_1 - q\alpha_2 \\ &= \alpha_1^3 + \alpha_2^3.\end{aligned}$$

  Por lo tanto, se cumplen los casos bases.

Hipótesis inductiva: Supongamos que la proposición es cierta para $1 \leq i \leq k$.

$$\alpha_1^k + \alpha_2^k = (\alpha_1 + \alpha_2)\left(\alpha_1^{k-1} + \alpha_2^{k-1}\right) - q\left(\alpha_1^{k-2} + \alpha_2^{k-2}\right).$$

Paso inductivo: Ahora se mostrará que es verdadero para $k + 1$.

$$\begin{aligned}(\alpha_1 + \alpha_2)\left(\alpha_1^k + \alpha_2^k\right) - q\left(\alpha_1^{k-1} + \alpha_2^{k-1}\right) &= \alpha_1\left(\alpha_1^k + \alpha_2^k\right) + \alpha_2\left(\alpha_1^k + \alpha_2^k\right) - q\alpha_1^{k-1} - q\alpha_2^{k-1}, \\ &= \alpha_1\alpha_1^k + \alpha_1\alpha_2^k + \alpha_2\alpha_1^k + \alpha_2\alpha_2^k - q\alpha_1^{k-1} - q\alpha_2^{k-1}, \\ &= \alpha_1^{k+1} + q\alpha_2^{k-1} + q\alpha_1^{k-1} + \alpha_2^{k+1} - q\alpha_1^{k-1} - q\alpha_2^{k-1}, \\ &= \alpha_1^{k+1} + \alpha_2^{k+1}.\end{aligned}$$

■

Mas aún, los coeficientes N_k se pueden calcular a partir del coeficiente N_1 de acuerdo con el siguiente teorema.

Teorema 3.1.1. [**]

$$N_k = \sum_{i=1}^{k} (-1)^{i-1} P_{i,k}(q) N_1^i$$

donde los $P_{i,k}$ son polinomios con coeficientes enteros positivos y $P_{k,k} = 1$.

[**]Se agrega al Teorema 3.1.1 el hecho de que $P_{k,k}(q) = 1$, la versión original de este resultado es debido a Garsia (ver [12], sección 2)

Demostración. Por inducción fuerte sobre k:
Sea E una curva elíptica sobre un campo $\mathbb{F}_q$.
Caso base.

- Si $k = 2$. Por definición sabemos que

$$N_2 = 1 + q^2 - \alpha_1^2 - \alpha_2^2,$$

donde α_1 y α_2 son conjugados complejos y $\alpha_1\alpha_2 = q$. Teniendo en cuenta estos resultados podemos reescribir a N_2 de modo que

$$\begin{aligned}
N_2 &= 1 + q^2 - \left(\alpha_1^2 + \alpha_2^2\right) \\
&= 1 + q^2 - \left((\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2\right) \\
&= 1 + q^2 - \left((1 + q - N_1)^2 - 2q\right) \\
&= 1 + q^2 - \left[1 + 2q + q^2 - (2N_1 + 2qN_1) + N_1^2\right] + 2q \\
&= 1 + q^2 - 1 - 2q - q^2 + (2N_1 + 2qN_1) - N_1^2 + 2q \\
N_2 &= (2 + 2q)N_1 - N_1^2.
\end{aligned}$$

- Si $k = 3$.
En este caso también conocemos una expresión para N_3 la cual está dada por

$$N_3 = 1 + q^3 - \alpha_1^3 - \alpha_2^3.$$

De forma similar al razonamiento realizado para N_2 obtenemos una expresión para N_3, es decir

$$\begin{aligned}
N_3 &= 1 + q^3 - \left(\alpha_1^3 + \alpha_2^3\right) \\
&= 1 + q^3 - (\alpha_1 + \alpha_2)\left(\alpha_1^2 + \alpha_2^2\right) + q(\alpha_1 + \alpha_2) \\
&= 1 + q^3 - (1 + q - N_1)\left(1 + q^2 - N_2\right) + q(1 + q - N_1) \\
&= 1 + q^3 - 1 - q + N_1 - (1 + q - N_1)q^2 + (1 + q - N_1)N_2 + q + q^2 - qN_1 \\
&= 1 + q^3 - 1 - q + N_1 - q^2 - q^3 + q^2N_1 + (1 + q - N_1)N_2 + q + q^2 - qN_1 \\
&= N_1 + q^2N_1 + (1 + q - N_1)N_2 - qN_1 \\
&= N_1 + q^2N_1 + (1 + q - N_1)\left((2 + 2q)N_1 - N_1^2\right) - qN_1 \\
&= N_1 + q^2N_1 + (1 + q - N_1)(2 + 2q)N_1 - (1 + q - N_1)N_1^2 - qN_1 \\
&= N_1 + q^2N_1 + (2 + 2q)N_1 + q(2 + 2q)N_1 - (2 + 2q)N_1^2 - N_1^2 - qN_1^2 + N_1^3 - qN_1 \\
&= \left(1 + q^2 + 2 + 2q + 2q + 2q^2 - q\right)N_1 - (2 + 2q + 1 + q)N_1^2 + N_1^3 \\
N_3 &= \left(3 + 3q + 3q^2\right)N_1 - (3 + 3q)N_1^2 + N_1^3.
\end{aligned}$$

Por lo tanto, los casos bases se satisfacen ya que tanto N_2 como N_3 se pueden escribir en términos de q y N_1.

Hipótesis inductiva: Supongamos que el resultado es cierto para $1 \leq i \leq k$

$$N_k = \sum_{i=1}^{k} (-1)^{i-1} P_{i,k}(q) N_1^i.$$

Paso inductivo: Se demostrará que el enunciado es cierto para $k+1$.

$$\begin{aligned}
N_{k+1} &= 1 + q^{k+1} - (\alpha_1^{k+1} + \alpha_2^{k+1}) \\
&= 1 + q^{k+1} - (\alpha_1 + \alpha_2)(\alpha_1^k + \alpha_2^k) + q(\alpha_1^{k-1} + \alpha_2^{k-1}) \\
&= 1 + q^{k+1} - (1 + q - N_1)(1 + q^k - N_k) + q(1 + q^{k-1} - N_{k-1}), \text{ por la recurrencia 3.1.2,} \\
&= (1 + q^k)N_1 + (1 + q - N_1)N_k - qN_{k-1}, \\
&= (1 + q^k)N_1 + (1 + q - N_1)\left(\sum_{i=1}^{k} (-1)^{i-1} P_{i,k}(q) N_1^i\right) - q\left(\sum_{i=1}^{k-1} (-1)^{i-1} P_{i,k-1}(q) N_1^i\right), \\
&= (1 + q^k)N_1 + P_{1,k}N_1 + \sum_{i=2}^{k} (-1)^{i-1}(P_{i-1,k}(q) + P_{i,k}(q))N_1^i + \sum_{i=1}^{k-1} (-1)^{i-1} q(P_{i,k}(q) \\
&\quad - P_{i,k-1}(q))N_1^i + (-1)^{k-1} q P_{k,k} N_1^k + (-1)^k P_{k,k} N_1^{k+1}, \\
&= \left((1 + q^k) + (1 + q)P_{1,k}(q) - qP_{1,k-1}\right) N_1 + (-1)^{k-1} \left(P_{k-1,k}(q) + (1 + q)\right) N_1^k \\
&\quad + (-1)^k P_{k,k}(q) N_1^{k+1} + \sum_{i=2}^{k-1} (-1)^{i-1} \left((1 + q)P_{i,k}(q) + P_{i-1,k}(q) - qP_{i,k-1}\right) N_1^i \\
N_{k+1} &= \sum_{i=1}^{k+1} (-1)^{i-1} \left((1 + q)P_{i,k}(q) + P_{i-1,k}(q) - qP_{i,k-1}\right) N_1^i
\end{aligned}$$

donde

$$P_{0,k}(q) = 1 + q^k, \;\; P_{k,k}(q) = 1 \;\text{ y }\; P_{i,k} = 0 \text{ cuando } i > k.$$

Por lo tanto, los coeficientes N_{k+1} quedan determinados por N_1 y los polinomios $P_{i,k} \in \mathbb{Z}[q]$. ■

Nota 5. *Es importante señalar que en la demostración anterior solamente se ha comprobado la existencia de los polinomios $P_{i,k}(q)$, queda pendiente la positividad de los polinomios $P_{i,k}(q)$. Este aspecto será retomado en secciones posteriores, por el momento utilizaremos el hecho de que $P_{i,k}(q) \in \mathbb{Z}_{\geq 0}[q]$ sin demostración.*

El siguiente listado muestra los primeros coeficientes N_k en términos de N_1 y q obteni-

dos de [12].

$$\begin{aligned}
N_2 &= (2+2q)N_1 - N_1^2 \\
N_3 &= (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
N_4 &= (4+4q+4q^2+4q^3)N_1 - (6+8q+6q^2)N_1^2 + (4+4q)N_1^3 - N_1^4 \\
N_5 &= (5+5q+5q^2+5q^3+5q^4)N_1 - (10+15q+15q^2+10q^3)N_1^2 \\
&\quad + (10+15q+10q^2)N_1^3 - (5+5q)N_1^4 + N_1^5.
\end{aligned}$$

A partir de la demostración del Teorema 3.1.1, se observó que los coeficientes $P_{i,k}(q)$ satisfacen una relación de recurrencia.

Proposición 3.1.3 (2024)**.** *El polinomio $P_{i,k}(q) \in \mathbb{Z}_{\geq 0}[q]$ con $1 \leq i \leq k$, satisface la siguiente relación de recurrencia*

$$P_{i,k+1}(q) = (1+q)P_{i,k}(q) + P_{i-1,k}(q) - qP_{i,k-1}(q)$$

con condiciones iniciales $P_{0,k}(q) = 1+q^k$, $P_{i,0}(q) = 0$ y $P_{0,0}(q) = 1$ donde $i = 0, 1$, y $k = 0, 1$.

Demostración. Se procede por inducción fuerte sobre $l = k + i$, con $1 \leq i \leq k$.
Caso base:

- Si $l = 2 \Rightarrow i = 1,\ k = 1$ porque $1 \leq i \leq k$.

$$(1+q)P_{1,0}(q) + P_{0,0}(q) - qP_{1,-1}(q) = 1 = P_{1,1}(q).$$

- Si $l = 3 \Rightarrow i = 1,\ k = 2$.

$$(1+q)P_{1,1}(q) + P_{0,1}(q) - qP_{1,0}(q) = 2(1+q) = P_{1,2}(q).$$

Hipótesis inductiva: Supongamos que el enunciado es cierto para $1 \leq j \leq l$.

$$P_{i,k}(q) = (1+q)P_{i,k-1}(q) + P_{i-1,k-1}(q) - qP_{i,k-2}(q).$$

Paso inductivo: Ahora se demostrará que también se cumple para $l + 1$.

$$l + 1 = k + i + 1 = \begin{cases} (k+1) + i \\ k + (i+1). \end{cases}$$

- $l + 1 = (k + 1) + i$.
  Por el Teorema 3.1.1, se tiene que

$$N_{k+1} = \sum_{i=1}^{k+1} (-1)^{i-1} P_{i,k+1}(q) N_1^i.$$

Realizando un cambio de variables de tal forma que $r = k + 1$, se tiene que

$$= \sum_{i=1}^{r} (-1)^{i-1} P_{i,r}(q) N_1^i$$

Comparando los coeficientes a ambos lados de la igualdad se obtiene que

$$P_{i,k}(q) + (1+q)P_{i-1,k}(q) - qP_{i,k-1}(q) = P_{i,k+1}.$$

Por lo tanto, para este caso la recurrencia de los polinomios es cierta.

- $l + 1 = k + (i + 1)$.
  Por el Teorema 3.1.1, los coeficientes N_k se pueden expresar de la forma

$$N_k = \sum_{i=0}^{k} (-1)^i P_{i+1,k}(q) N^{i+1}. \tag{3.2}$$

Ahora realizamos un cambio de variables de tal forma que $j = i + 1$

$$\sum_{i=0}^{k} (-1)^i P_{i+1,k}(q) N^{i+1} = \sum_{j=1}^{k} (-1)^{j-1} P_{j,k}(q) N^j.$$

Por la hipótesis inductiva, se cumple que

$$\begin{aligned}\sum_{j=1}^{k} (-1)^{j-1} P_{j,k}(q) N^j &= \sum_{i=0}^{k} (-1)^j \left[P_{j,k}(q) + (1+q)P_{j,k}(q) - qP_{j,k}(q)\right] N^j \\ &= \sum_{j=1}^{k} (-1)^{j-1} \left[P_{j,k-1}(q) + (1+q)P_{j-1,k-1}(q) - qP_{j,k-2}(q)\right] N^j.\end{aligned}$$

Recordamos que $j = i + 1$ y realizamos nuevamente el cambio de variable

$$\begin{aligned}&\sum_{j=1}^{k} (-1)^{j-1} \left[P_{j,k-1}(q) + (1+q)P_{j-1,k-1}(q) - qP_{j,k-2}(q)\right] N^j \\ &\quad = \sum_{i=0}^{k} (-1)^i [P_{i+1,k-1}(q) + (1+q)P_{i,k-1}(q) - qP_{i+1,k-2}(q)] N^{i+1}. \end{aligned} \tag{3.3}$$

Finalmente, comparamos los coeficientes de N^{i+1} de la expresión 3.2 y 3.3.

$$P_{i+1,k}(q) = P_{i+1,k-1}(q) + (1+q)P_{i,k-1}(q) - qP_{i+1,k-2}(q).$$

Con la igualdad anterior, se concluye que la proposición es cierta para este caso.

Por lo tanto, para ambos casos se cumple la recurrencia de la familia de polinomios $P_{i,k}(q)$ por lo que la proposición es verdadera para $l+1$. ■

Con esta relación de recurrencia, es posible encontrar fórmulas explícitas para ciertos polinomios $P_{i,k}(q)$.

Ejemplo 3.1.1. A continuación se presentan fórmulas para polinomios $P_{i,k}(q)$ particulares.

- $P_{1,k}(q) = k\sum_{j=0}^{k-1} q^j$.
- $P_{k,k+1}(q) = (k+1)(1+q)$.
- $P_{k,k}(q) = 1$.

Con el listado de coeficientes N_k, también podemos identificar otras propiedades por medio de la observación de patrones de los polinomios $P_{i,k}(q)$. Por ejemplo, consideremos el cálculo del grado de un polinomio para elementos específicos de la familia de polinomios $P_{i,k}(q) \in \mathbb{Z}_{\geq 0}[q]$.

Ejemplo 3.1.2. Para $1 \leq i \leq k$ y k se tienen los siguientes ejemplos del cálculo del grado:

(a) $\deg P_{1,2}(q) = \deg(2+2q) = 1$.

(b) $\deg P_{2,5}(q) = \deg(10+15q+15q^2+10q^3) = 3$.

(c) $\deg P_{1,k}(q) = \deg\left(k\sum_{j=0}^{k-1} q^j\right) = k-1$.

A partir de estos resultados, podemos conjeturar que el grado de los polinomios $P_{i,k}(q)$ depende directamente de la resta de los subíndices $k-i$.
En la siguiente proposición, enunciamos de forma general la afirmación realizada con respecto al grado de la familia de polinomios $P_{i,k}(q)$. Para el desarrollo de la demostración, utilizaremos principalmente la recurrencia dada en la Proposición 3.1.3.

Proposición 3.1.4 (2024)**.** *El grado del polinomio $P_{i,k}$ con coeficientes enteros positivos satisface la siguiente propiedad para $0 \leq i \leq k$:*

$$\deg(P_{i,k}(q)) = k-i.$$

Demostración. (Inducción fuerte sobre $S = k+i$)
Caso base:

- $S = 1 \Rightarrow \begin{cases} k=1, \ \ i=0 \\ k=0, \ \ i=1, \text{ este caso no sucede porque } 0 \leq i \leq k. \end{cases}$

  - Si $k=1, \ \ i=0$ entonces

$$\deg(P_{0,1}(q)) = \deg(1+q) = 1 = k-i.$$

- $S = 2 \Rightarrow \begin{cases} k = 1, \ \ i = 1 \\ k = 2, \ \ i = 0 \\ k = 0, \ \ i = 2, \text{ este caso no sucede porque } 0 \leq i \leq k. \end{cases}$

  - Si $k = 1, \ \ i = 1$ entonces

$$\deg(P_{1,1}(q)) = \deg(1) = 0 = k - i.$$

  - Si $k = 2, \ \ i = 0$ entonces

$$\deg(P_{0,2}(q)) = \deg(1 + q^2) = 2 = k - i.$$

En todos los casos posibles se satisface la propiedad.
Hipótesis inductiva: Supongamos que la propiedad es cierta para $1 \leq j \leq S$.

$$\deg(P_{i,k}(q)) = k - i.$$

Paso inductivo: Ahora se demostrará que la identidad es cierta para $S + 1$.

$$\Rightarrow S + 1 = (k + i) + 1 = \begin{cases} (k + 1) + i \\ k + (i + 1). \end{cases}$$

- Utilizando $S + 1 = (k + 1) + i$.

$$\begin{aligned} \deg(P_{i,k+1}(q)) &= \deg((1 + q)P_{i,k}(q) + P_{i-1,k}(q) - qP_{i,k-1}) \\ &\leq \text{máx}\{\deg(1 + q)P_{i,k}(q), \deg P_{i-1,k}(q), \deg qP_{i,k-1}\}. \end{aligned}$$

  - $\deg(1 + q)P_{i,k}(q)$.

$$\begin{aligned} \deg(1 + q)P_{i,k}(q) &= 1 + \deg P_{i,k}(q) \\ &= 1 + (k - i), \text{ por la hipótesis inductiva} \\ &= (k + 1) - i. \end{aligned}$$

    Por lo tanto,

$$\deg(1 + q)P_{i,k}(q) = (k + 1) - i. \tag{3.4}$$

  - $\deg P_{i-1,k}(q)$.

$$\deg P_{i-1,k}(q) = k - (i - 1) = (k + 1) - i. \tag{3.5}$$

  - $\deg qP_{i,k-1}(q)$.

$$\begin{aligned} \deg qP_{i,k-1}(q) &= 1 + \deg P_{i,k-1}(q) \\ &= 1 + (k - 1) - i = k - i, \text{por la hipótesis inductiva.} \end{aligned}$$

    Por lo tanto,

$$\deg(1 + q)P_{i,k}(q) = k - i. \tag{3.6}$$

Utilizando los resultados 3.4, 3.5 y 3.6 se obtiene

$$\deg(P_{i,k+1}(q)) \leq \text{máx}\{(k+1)-i, (k+1)-i, k-i\}$$
$$\deg(P_{i,k+1}(q)) \leq (k+1)-i.$$

Ahora analizamos los grados de cada término que conforman el polinomio $P_{i,k+1}(q)$.

De los resultados 3.4 y 3.5 tenemos que

$$\deg(1+q)P_{i,k}(q) = \deg P_{i-1,k}(q).$$

Como los polinomios tienen coeficientes positivos, consideremos la resta de $P_{i-1,k}(q) - qP_{i,k-1}$, comparando los grados se observa que

$$\deg qP_{i,k-1}(q) \leq \deg P_{i-1,k}(q).$$

De forma similar se tiene que

$$\deg qP_{i,k-1}(q) \leq \deg P_{i,k}(q).$$

Así, en ambos casos al realizar la resta de los polinomios no afectaría en el grado por lo que

$$\deg(P_{i,k+1}(q)) = (k+1)-i.$$

- $S+1 = k+(i+1)$, para este caso se cumple para $i \leq k-1$ entonces

$$\deg(P_{i+1,k}(q)) = \deg(P_{i+1,k-1}(q) + P_{i,k-1}(q) - P_{i+1,k-2}(q)).$$

Ahora consideremos los siguientes casos para i:

- Si $i = k-1$.

$$\begin{aligned}\deg(P_{i+1,k}(q)) &= \deg((1+q)P_{i+1,k-1}(q) + P_{i,k-1}(q) - P_{i+1,k-2}(q)) \\ &= \deg(P_{k-1,k-1}(q)) \\ &= \deg(1) = 0 = k-(i+1) = k-(k-1+1).\end{aligned}$$

  Por lo tanto, la propiedad se cumple.

- Si $i < k-1$.

$$\deg(P_{i+1,k}(q)) = \deg((1+q)P_{i+1,k-1}(q) + P_{i,k-1}(q) - P_{i+1,k-2}(q))$$

  Si $i+1 \geq k-1$ entonces

$$\begin{aligned}\deg(P_{i+1,k}(q)) &= \deg((1+q)P_{i+1,k-1}(q) + P_{i,k-1}(q) - P_{i+1,k-2}(q)) \\ &= \deg(P_{i,k-1}(q)) \\ &= (k-1)-i, \text{ por la hipótesis inductiva,} \\ \deg(P_{i+1,k}(q)) &= k-(i+1).\end{aligned}$$

Para este caso, también se cumple la propiedad del grado del polinomio $P_{i+1,k}(q)$.

Si $i+1 < k-1$ entonces

$$\begin{aligned}\deg(P_{i+1,k}(q)) &= \deg((1+q)P_{i+1,k-1}(q) + P_{i,k-1}(q) - P_{i+1,k-2}(q)) \\ &\leq \text{máx}\{\deg(1+q)P_{i+1,k-1}(q), \deg P_{i,k-1}(q), \deg P_{i+1,k-2}(q)\}.\end{aligned}$$

Seguidamente, se obtienen los grados de cada polinomio

(a)

$$\deg(1+q)P_{i+1,k-1}(q) = 1 + \deg P_{i+1,k-1}(q) = k-(i+1).$$

(b)

$$\deg P_{i,k-1}(q) = (k-1) - i = k-(i+1), \text{por la hipótesis inductiva.}$$

(c)

$$\begin{aligned}\deg P_{i+1,k-2}(q) &= (k-2)-(i+1), \text{por la hipótesis inductiva} \\ &= k-(i+3).\end{aligned}$$

De (a) y (b) obtenemos:

$$\deg(1+q)P_{i+1,k-1}(q) = \deg P_{i,k-1}(q).$$

Luego, por los casos (a), (b) y (c) se tiene que

$$\deg(P_{i+1,k}(q)) \leq k-(i+1).$$

Realizando el mismo análisis que en el caso de $S+1 = (k+1)+i$ se tiene que

$$\deg(P_{i+1,k}(q)) = k-(i+1).$$

Por lo tanto, la propiedad es cierta para $S+1$. ■

La proposición anterior, nos da una nueva propiedad para la familia de polinomios $P_{i,k}(q)$, que indica la importancia del estudio de este tipo de polinomios. En conformidad con [12], las recurrencias encontradas dan pistas de que se puede llegar a establecer conexiones con identidades combinatorias interesantes gracias a las características de esta familia de polinomios como se estudiará más adelante.

3.2. Los coeficientes N_k y $(q,t)-$ analogías

En esta sección, estudiamos más a fondo la familia de polinomios $P_{i,k}(q)$ desde un punto de vista combinatorio que dan lugar a identidades con curvas elípticas.

Para comenzar, se abordarán ciertos polinomios bivariados del artículo de [12] con el fin de explorar identidades combinatorias con los coeficientes N_k. Cabe destacar que estos polinomios son $(q,t)-$ analogías de los números de Fibonacci y Lucas, por lo cual existen diversos modelos de polinomios. Por ejemplo, el modelo combinatorio que se utiliza en [7], Capítulo 32 y 33, son $(q,t)-$ analogías. Es válido aclarar que para el desarrollo esta sección, no se profundizará en la teoría de $q-$ análogos. Para los lectores interesados en este tema se recomienda leer [16], Capítulo 1, Sección 1.10.

3.2.1. Los números de Lucas y $(q,t)-$ analogías

En este apartado iniciamos definiendo $(q,t)-$ analogías de los números de Lucas para estudiar posibles conexiones con la enumeración de puntos sobre curvas elípticas.

Definición 3.2.1. *Sea $S^{(1)}$ una variación circular del conjunto $S \subseteq \{1,2,\ldots,n\}$ módulo n, es decir cada elemento $x \in S^{(1)}$ si y sólo si $x-1(\mod n) \in S$. Definimos los $(q,t)-$* ***polinomios de Lucas*** *como la sucesión de polinomios en las variables q y t*

$$L_n(q,t) = \sum_{S\subseteq\{1,2,\ldots,n\}:S\cap S_1^{(n)}=\emptyset} q^{\#\text{ elementos pares en } S} t^{\left\lfloor \frac{n}{2} \right\rfloor - \#S}.$$

Utilizando la Definición 3.2.1, vamos a calcular casos particulares de los $(q,t)-$ polinomios de Lucas.

Ejemplo 3.2.1. Consideremos los siguientes casos:

1. Si $n=2$ y $\{1,2\}$.
   Los subconjuntos de $\{1,2\}$ son:

$$\begin{aligned} S_1 &= \emptyset \\ S_2 &= \{1\} \\ S_3 &= \{2\} \\ S_4 &= \{1,2\}. \end{aligned}$$

   Los subconjuntos de $\{1,2\}$ sin elementos circularmente consecutivos son:

$$S_1,\ S_2,\ S_3.$$

Luego, el polinomio de Lucas en las variables q y t es:

$$\begin{aligned} L_2(q,t) &= q^{\#\text{ elementos pares en } S_1} t^{\lfloor \frac{n}{2} \rfloor} - \#S_1 + q^{\#\text{ elementos pares en } S_2} t^{\lfloor \frac{n}{2} \rfloor} - \#S_2 \\ &\quad + q^{\#\text{ elementos pares en } S_3} t^{\lfloor \frac{n}{2} \rfloor} - \#S_3 \\ &= q^0 t^1 + q^0 t^0 + q^1 t^0 \\ L_2(q,t) &= t + 1 + q = 1 + t + q. \end{aligned}$$

2. Si $n = 3$ entonces se tendrá el conjunto $\{1, 2, 3\}$.

   Los subconjuntos de $\{1, 2, 3\}$ son:

$$\begin{array}{lll} S_0 = \emptyset & S_3 = \{3\} & S_6 = \{1, 3\} \\ S_1 = \{1\} & S_4 = \{1, 2\} & S_7 = \{1, 2, 3\}. \\ S_2 = \{2\} & S_5 = \{2, 3\} & \end{array}$$

   A continuación, se identificarán los subconjuntos que no tiene elementos circularmente consecutivos:

$$S_0,\ S_1,\ S_2,\ S_3.$$

   Así, el polinomio de Lucas está dado por

$$L_3(q,t) = q^0 t^1 + q^0 t^0 + q^1 t^0 + q^0 t^0 = t + 1 + q + 1 = 2 + t + q.$$

La siguiente tabla muestra el cálculo de los primeros $(q,t)-$ polinomios de Lucas obtenidos mediante la Definición 3.2.1.

k	$L_k(q,t)$
2	$1 + t + q$
3	$2 + t + q$
4	$1 + q^2 + (2 + 2q)t + t^2$

Cuadro 3.1: Primeros $(q,t)-$ polinomios de Lucas.

El polinomio de Lucas $L_n(q,t)$ tiene una interpretación combinatoria que consiste en elegir subconjuntos $S \subseteq \{1, 2, \ldots, n\}$ sin elementos consecutivos y que no contengan a los elementos 1 y n.

Otra interpretación combinatoria, es considerar a $L_n(q,t)$ como una función generadora de collares con cuentas color negras y blancas de modo que no hayan dos cuentas negras

consecutivas.

Existe otro tipo de polinomios en las variables (q,t), los cuales surgen a partir de los $L_n(q,t)$ como se mostrará más adelante. Además, son una $(q,t)-$ analogía de los número de Lucas y se definen a continuación.

Definición 3.2.2. *Para $k \geq 1$ definimos el conjunto de polinomios $\{\tilde{L}_{2k}(q,t)\}$*

$$\tilde{L}_{2k}(q,t) = \sum_{S\subseteq\{1,2,\ldots,2k\}:S\cap S_1^{2k}=\emptyset} q^{\#\textit{elementos pares en } S} t^{\#S}.$$

La interpretación combinatoria para los polinomios definidos anteriormente es igual a la de los $(q,t)-$ polinomios definidos en 3.2.1, es decir que consideramos a un elemento de la familia $\{\tilde{L}_{2k}\}_{k\geq 1}$ como una función generadora de collares con cuentas de color negro y blanco sin dos color negro consecutivas. La diferencia con los polinomios $L_k(q,t)$ es que el exponente de t es el número de elementos de cada subconjunto $S \subseteq \{1,2,\ldots,2k\}$. Otra observación, es que los términos de estos polinomios se generan a partir de subconjuntos S de conjuntos de longitud par.

Para comprender mejor estas afirmaciones se presentamos ejemplos concretos.

Ejemplo 3.2.2. Consideremos el siguiente caso particular.
Si $k = 1$ entonces el conjunto es $\{1,2\}$. Los subconjuntos son:

$$\begin{aligned} S_0 &= \emptyset, \\ S_1 &= \{1\}, \\ S_2 &= \{2\}, \\ S_3 &= \{1,2\}. \end{aligned}$$

Luego, identificamos cuáles son los subconjuntos de $\{1,2\}$ que no tienen elementos consecutivos ni a 1 y 2 que serán los términos del polinomio $\tilde{L}_{2k}$. Así, nuestro polinomio es:

$$\begin{aligned} \tilde{L}_2(q,t) &= q^0t^0 + q^0t^1 + q^1t^1, \\ \tilde{L}_2(q,t) &= 1 + t + qt. \end{aligned}$$

3.2.2. Los números de Fibonacci y $(q,t)-$ analogías

Definición 3.2.3. *Los $(q,t)-$ **polinomios de Fibonacci**, denotados como $\tilde{F}_n(q,t)$, son definidos como*

$$\tilde{F}_k(q,t) = \sum_{S\subseteq\{1,2,\ldots,k-1\}:S\cap(S_1^{(k-1)}-\{1\})=\emptyset} q^{\#\textit{elementos pares en } S} t^{\#S}.$$

Cada uno de los términos que conforman el polinomio $\tilde{F}_k(q,t)$ son subconjuntos de $\{1,2,\ldots,k-1\}$ tales que no hay dos elementos linealmente consecutivos. También se pueden interpretar como cadenas con cuentas de longitud $k-1$ blancas o negras de modo que no ocurra el caso de dos cuentas negras consecutivas.

Ejemplo 3.2.3. A continuación se presentan ejemplos del cálculo con los primeros $(q,t)-$ polinomios de Fibonacci.

- Si $k=2$ entonces tenemos el conjunto $\{1\}$ que consta de los subconjuntos $\emptyset$ y $\{1\}$.

$$\tilde{F}_2(q,t) = 1+t.$$

- Si $k=3$ entonces tenemos el conjunto $\{1,2\}$ y los subconjuntos son:

$$\begin{aligned} S_0 &= \emptyset, \\ S_1 &= \{1\}, \\ S_2 &= \{2\}, \\ S_3 &= \{1,2\}. \end{aligned}$$

  Los subconjuntos que cumplen con la definición son: $S_0,\ S_1,\ S_2$ y son términos del polinomio.

$$\tilde{F}_3(q,t) = 1+t+qt.$$

- Si $k=4$ entonces tenemos el conjunto $\{1,2,3,4\}$ y los subconjuntos que no tienen elementos linealmente consecutivos son:

$$\begin{aligned} S_0 &= \emptyset \\ S_1 &= \{1\} \\ S_2 &= \{2\} \\ S_3 &= \{3\} \\ S_4 &= \{1,3\}. \end{aligned}$$

  Estos subconjuntos conforman los términos del polinomio $\tilde{F}_4(q,t)$. Así obtenemos que

$$\tilde{F}_4(q,t) = 1+t+qt+t+t^2 = 1+2t+qt+t^2.$$

Lema 3.2.1. *El número de pares de collares que no pueden ser combinados para formar un collar más largo es*

$$2qt^2\tilde{F}_{2k-2}(q,t).$$

Demostración. Para la demostración se pueden considerar dos casos tomando en cuenta la interpretación de $(2k+2)-$ collares con cuentas coloreadas de blanco o negro.

- **Caso 1:** Si 1 y $2k+2$ son negras (ver Figura 3.1).
  Este caso implica que las cuentas etiquetadas como 2, $2k+1$ y $2k$ deben ser blancas. Así, la cantidad de posibilidades es qt^2 por las combinaciones de $(2k-3)-$ cadenas que no contienen dos cuentas negras consecutivas que por definición es $\tilde{F}_{2k-2}(q,t)$. Para este caso tendremos

$$qt^2\tilde{F}_{2k-2}(q,t).$$

- **Caso 2:** Si $2k$ y $2k+1$ son negras (ver Figura 3.2).
  Para este caso, las cuentas etiquetas por $1, 2k+2, 2k-1$ deben de ser blancas. De forma similar, la cantidad de combinaciones posibles es

$$qt^2\tilde{F}_{2k-2}(q,t).$$

  Por lo tanto, el número de pares que no pueden ser combinados para formar un collar más largo es

$$2qt^2\tilde{F}_{2k-2}(q,t).$$

■

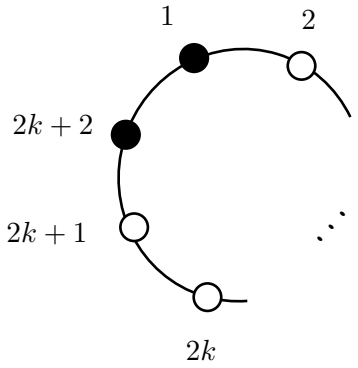


Figura 3.1: Caso 1

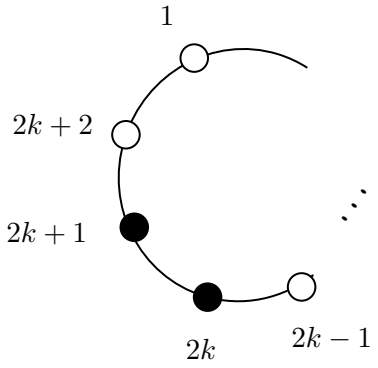


Figura 3.2: Caso 2

Lema 3.2.2. *El número de $(2k+2)-$ collares que no se pueden transformar a un $2-$collar y un $2k-$collar es $qt^2\tilde{F}_{2k-3}(q,t)$.*

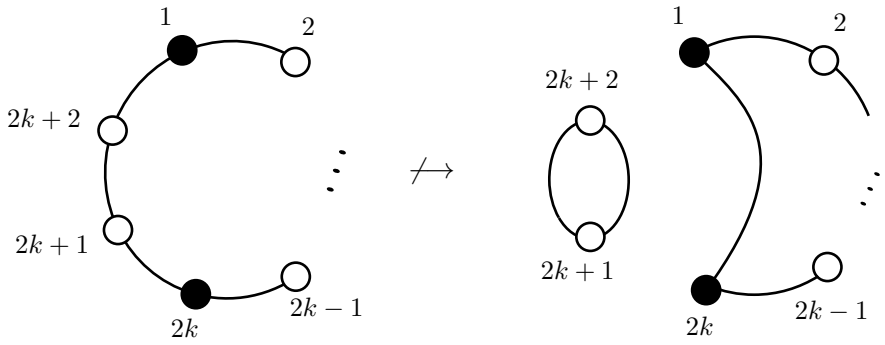


Figura 3.3: $(2k+2)-$ collar que no se puede cortar en dos.

Demostración. Consideremos $(2k+2)-$ collares con cuentas de color blanco o negro. Podemos notar que el único caso que no puede ser transformado en uno de longitud 2 y de $2k$ es cuando 1 y $2k$ son negros implica que 2 y $2k-1$ son blancas.

Analizando las cadenas de longitud $2k-4$ enumeradas a partir de 3 hasta $2k-2$, tendremos que la cantidad de collares que no tienen 2 cuentas negras consecutivas es $\tilde{F}_{2k-3}(q,t)$. Por lo tanto, la cantidad de collares que no se pueden descomponer en uno de longitud 2 y uno de $2k$ es

$$qt^2\tilde{F}_{2k-3}(q,t).$$

■

Lema 3.2.3. *La diferencia entre las cantidades del Lema 3.2.2 y el Lema 3.2.1 es exactamente* $qt^2\tilde{L}_{2k-2}(q,t)$.

Demostración. Se debe mostrar que

$$2qt^2\tilde{F}_{2k-2}(q,t) - qt^2\tilde{F}_{2k-3}(q,t) = qt^2\tilde{L}_{2k-2}(q,t).$$

Por la identidad

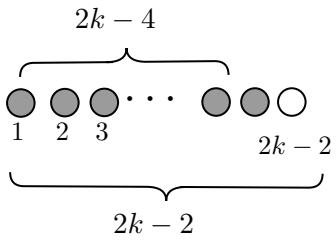
$$\tilde{F}_{2k-2}(q,t) = qt\tilde{F}_{2k-4}(q,t) + \tilde{F}_{2k-3}(q,t). \tag{3.7}$$

Esta recurrencia quiere decir que la cuenta $2k-2$ puede ser de color blanco o negro. Consideremos cadenas de longitud $2k-2$ etiquetadas del 1 al $2k-2$ y se analizan los casos:

- Si la cuenta $2k-2$ es blanca entonces la cuenta $2k-3$ puede ser blanca o negra. Así la cantidad de formas de que $2k-2$ sea blanca es:

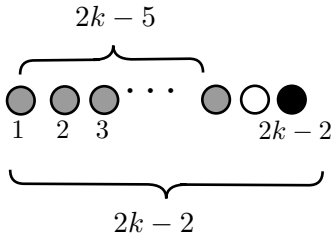
$$\tilde{F}_{2k-3}(q,t),$$

son las cadenas de longitud $2k-4$ que no tienen dos cuentas negras consecutivas. A continuación se presenta gráficamente este caso.



- Si la cuenta $2k-2$ es negra entonces la cuenta $2k-3$ es blanca y la cuenta $2k-4$ puede ser blanca o negra por lo que la cantidad de formas que sucede este caso es qt. Finalmente analizamos las cadenas de longitud $2k-5$. Por lo tanto, el número total de combinaciones es

$$qt\tilde{F}_{2k-4}(q,t),$$



Con esta identidad basta con demostrar que

$$qt^2\tilde{L}_{2k-2}(q,t) = qt^2\tilde{F}_{2k-2}(q,t) + q^2t^3\tilde{F}_{2k-4}(q,t).$$

Ahora dividimos por qt^2 y obtenemos que

$$\tilde{L}_{2k-2}(q,t) = \tilde{F}_{2k-2}(q,t) + qt\tilde{F}_{2k-4}(q,t).$$

Luego, se analizan los casos en los que la cuenta 1 es blanca o negra.

- Si la cuenta 1 es blanca entonces la cuenta $2k-2$ puede ser blanca o negra y analizamos las cadenas de longitud $2k-3$. Por lo tanto, el número de formas de que la cuenta $2k-2$ sea blanca es

$$\tilde{F}_{2k-3}(q,t).$$

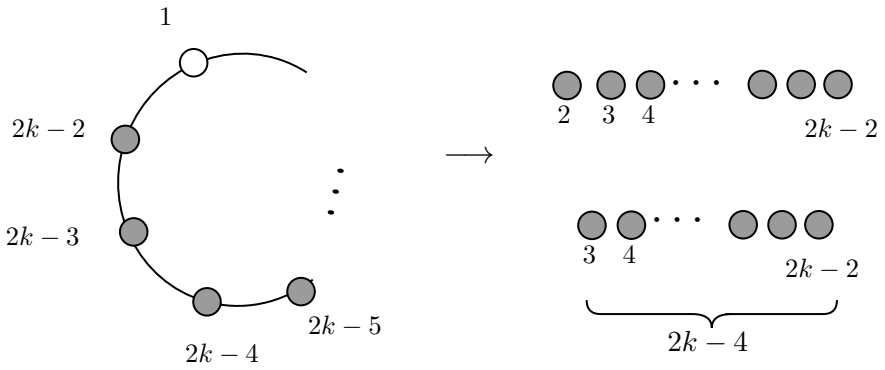


Figura 3.4: Cuenta 1 color blanco.

- Si la cuenta 1 es negra entonces 2 y $2k-2$ deben ser blancas entonces hay qt formas que ocurra este caso. Luego se analizan las cadenas de longitud $2k-5$ que no van a tener dos cuentas negras consecutivas que por definición es el polinomio de Fibonacci

$$\tilde{F}_{2k-4}(q,t).$$

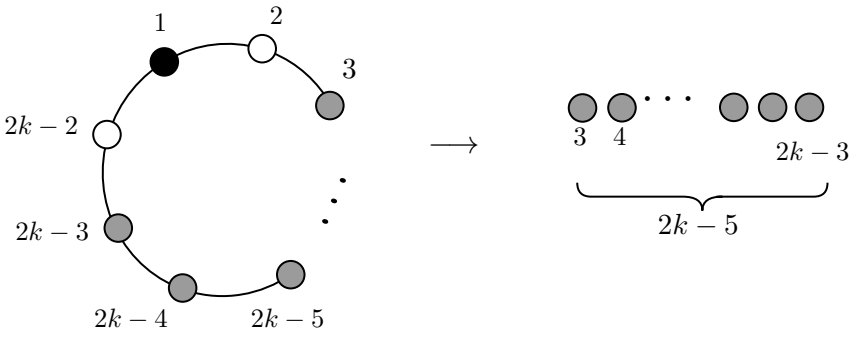


Figura 3.5: Cuenta 1 color negro.

Por lo tanto, la cantidad de formas que se pueden construir collares de longitud $2k-2$ es

$$\tilde{L}_{2k-2}(q,t) = \tilde{F}_{2k-2}(q,t) + qt\tilde{F}_{2k-4}(q,t).$$

Ahora multiplicamos por qt^2

$$qt^2\tilde{L}_{2k-2}(q,t) = qt^2\tilde{F}_{2k-2}(q,t) + q^2t^3\tilde{F}_{2k-4}(q,t).$$

Por lo tanto,

$$qt^2\tilde{L}_{2k-2}(q,t) = 2qt^2\tilde{F}_{2k-2}(q,t) - qt^2\tilde{F}_{2k-3}(q,t).$$

■

Proposición 3.2.1. *Los $(q,t)-$polinomios de Lucas $L_k(q,t)$ definidos en 3.2.1 cumplen la identidad*

$$L_{2k+2}(q,t) = (1+q+t)L_{2k}(q,t) - qL_{2k-2}(q,t), \text{ con } k \geq 1.$$

Demostración. Para demostrar el resultado consideramos un conjunto de polinomios auxiliares $\{\tilde{L}_{2k}\}_{k\geq 1}$ definidos en la Proposición 3.2.2 de modo que

$$L_{2k}(q,t) = t^k\tilde{L}_{2k}(q,t^{-1}). \tag{3.8}$$

Transformando la identidad en términos de los polinomios auxiliares obtenemos que la identidad es equivalente a mostrar que se satisface

$$\tilde{L}_{2k+2}(q,t) = (1+t+qt)\tilde{L}_{2k}(q,t) - qt^2\tilde{L}_{2k-2}(q,t).$$

Para la demostración, consideremos que tenemos una función generadora de collares de longitud $2k+2$ etiquetados de 1 hasta $2k+2$. De modo que son construidos con collares de longitud $2k$ con cuentas de 1 hasta $2k$ y de longitud 2 con cuentas etiquetadas por $2k+1$ y $2k+2$.
Por lo tanto, el número de formas que se pueden construir dichos collares de longitud $2k+2$ es

$\tilde{L}_2(q,t)\tilde{L}_{2k-2}(q,t) = (1+t+qt)\tilde{L}_{2k-2}(q,t),$ por definición de los polinomios de Lucas.

Ahora consideremos que no todos los collares de longitud $2k+2$ pueden ser separados en dos nuevos collares de longitud $2k$ y 2. También se cumple que no siempre se pueden formar collares a partir de uno de longitud $2k$ y otro de longitud 2. Por el Lema 3.2.1, el número de combinaciones de dos collares que no se pueden transformar a uno nuevo de longitud $2k+2$ es

$$2qt^2\tilde{F}_{2k-2}(q,t).$$

Por el Lema 3.2.2, obtenemos la cantidad de casos de collares que no se pueden separar a uno de longitud 2 y $2k$ es

$$qt^2\tilde{F}_{2k-3}.$$

Por el Lema 3.2.3 tenemos que

$$2qt^2\tilde{F}_{2k-2}(q,t) - qt^2\tilde{F}_{2k-3}(q,t) = qt^2\tilde{L}_{2k-2}(q,t),$$

es el tercer término de la recurrencia, por lo que

$$\tilde{L}_{2k+2}(q,t) = (1+t+qt)\tilde{L}_{2k-2}(q,t) - qt^2\tilde{L}_{2k-2}(q,t).$$

Ahora, evaluamos en (q,t^{-1}) los polinomios con el fin de obtener la expresión equivalente.

$$\begin{aligned}
\tilde{L}_{2(k+1)}(q,t^{-1}) &= (1+t^{-1}+qt^{-1})\tilde{L}_{2k-2}(q,t^{-1}) - q(t^{-1})^2\tilde{L}_{2k-2}(q,t^{-1}) \\
t^{-(k+1)}L_{2(k+1)}(q,t) &= (1+t^{-1}+qt^{-1})t^{-(k-1)}L_{2k-2}(q,t) - q(t^{-1})^2t^{-(k-1)}L_{2k-2}(q,t) \\
L_{2(k+1)}(q,t) &= (t+1+q)L_{2k-2}(q,t) - qL_{2k-2}(q,t).
\end{aligned}$$

Por lo tanto,

$$L_{2k+2}(q,t) = (t+1+q)L_{2k-2}(q,t) - qL_{2k-2}(q,t).$$

■

Teorema 3.2.1.

$$1 + q^k - N_k = L_{2k}(q,-N_1)$$

para todo $k \geq 1$.

Demostración. Para demostrar este resultado vamos a comprobar que ambos lados son iguales y que satisfacen la misma relación de recurrencia, es decir

$$G_{k+1} = (1+q-N_1)G_k - qG_{k-1}$$

donde $G_k = 1 + q^k - N_k$ para $k \geq 2$ con condiciones iniciales

$$G_0 = 2 \text{ y } G_1 = 1 + q - N_1.$$

Primero comprobamos las condiciones iniciales en ambos lados de la igualdad, es decir para $k \in \{1,2\}$. Para comprobar el lado izquierdo de la igualdad tenemos que por la Proposición 3.1.2 se cumple que

$$\begin{aligned}
1 + q - N_1 &= G_1, \\
1 + q^2 - N_2 &= (\alpha_1+\alpha_2)(\alpha_1+\alpha_2) - 2q = (1+q-N_1)G_1 - qG_0.
\end{aligned}$$

Ahora verificamos las condiciones iniciales para el lado derecho de la igualdad recordando la definición de los $(q,t)-$ polinomios de Lucas (3.2.1). Por el ejemplo 3.2.1 y evaluando en $(q,-N_1)$ para $k \in \{1,2\}$ se tiene que:

- Si $k = 1$ el polinomio de Lucas es

$$\begin{aligned}
L_2(q,t) &= 1 + q + t, \\
L_2(q,-N_1) &= 1 + q - N_1 = G_1.
\end{aligned}$$

- Si $k=2$ el polinomio de Lucas es

$$\begin{aligned} L_4(q,t) &= 1+q^2+(2+2q)t+t^2, \\ L_4(q,-N_1) &= 1+q^2+(2+2q)(-N_1)+(-N_1)^2 \\ &= 1+q^2-(2+2q)N_1+N_1^2, \\ &= 1+q^2-\underbrace{[(2+2q)N_1-N_1^2]}, \\ L_4(q,-N_1) &= 1+q^2-N_2=(1+q-N_1)G_1-qG_0. \end{aligned}$$

Ahora comprobamos la recurrencia para $k \geq 2$.

Partimos del lado izquierdo, observando que se cumple inmediatamente la recurrencia por la Proposición 3.1.2, es decir

$$\begin{aligned} 1+q^k-N_k &= (1+q-N_1)(1+q^{k-1}-N_{k-1})-q(1+q^{k-2}-N_{k-2}) \\ &= (1+q-N_1)G_{k-1}-qG_{k-2}. \end{aligned}$$

Para el lado derecho de la igualdad por la proposición 3.2.1 se cumple que

$$L_{2k+2}(q,t)=(1+q+t)L_{2k}(q,t)-qL_{2k-2}(q,t).$$

Seguidamente, evaluamos en $(q,-N_1)$:

$$L_{2k+2}(q,-N_1)=(1+q-N_1)L_{2k}(q,-N_1)-qL_{2k-2}(q,-N_1).$$

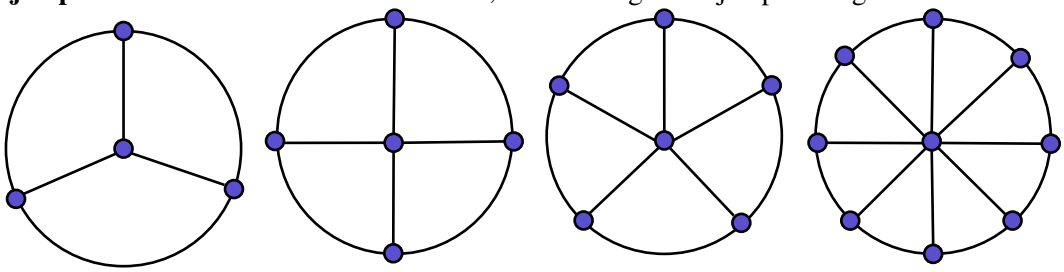
Por lo tanto, ambos lados de la igualdad satisfacen la misma recurrencia de tres términos. ■

3.2.3. $(q,t)-$ polinomios de ruedas

Los números de Fibonacci y Lucas por su naturaleza lineal y circular respectivamente, permiten establecer fórmulas con las que se pueden calcular los coeficientes N_k como las estudiadas en la sección anterior. Ahora bien, centrándonos en ciertas interpretaciones de los números de Lucas y Fibonacci, exploraremos la posibilidad de encontrar identidades para calcular de forma explícita los coeficientes N_k desde la teoría de grafos.
Un problema ampliamente estudiado en teoría de grafos, es el conteo de los árboles generadores de un grafo G. Bajo este enfoque, el conteo de los árboles generadores de los grafos de rueda están determinados por la sucesión de números de Lucas $\{L_{2n}-2\}$ de acuerdo con [7] y [15]. Por lo cual, será necesario definir qué es un grafo de rueda y luego pasaremos a resultados sobre el conteo de árboles generadores.

Definición 3.2.4. *Para $n \geq 1$ el **grafo de rueda** W_n tiene $n+1$ vértices, que consta de un ciclo de n vértices exteriores denominados $w_1, w_2, \ldots, w_n$ y un vértice central denominado w_0 que es adyacente a todos los vértices exteriores.*

Ejemplo 3.2.4. De acuerdo a la definición, tenemos algunos ejemplos de grafos de rueda.



W_3 W_4 W_5 W_6

En [12] profundiza en una interpretación combinatoria de los árboles generadores de un grafo de rueda W_n, como se describirá a continuación.
Sea T un árbol generador de W_n el cual consta de radios y arcos disconexos en el borde del grafo, donde cada radio conecta a un único arco. Además diremos que un arco tiene longitud k si pasa por k vértices (ver Figura 3.6).

Definición 3.2.5. *(Cola de un arco) definimos la* ***cola de un arco*** *de un árbol generador T del grafo de rueda W_k como el vértice que es sumidero de un arco eligiendo una dirección horaria de los arcos de T.*

Definición 3.2.6. *($q-$ peso del arco) El $q-$* ***peso de un arco*** *es el número de aristas entre un radio y la cola de un arco.*

Notemos que por definición para el caso de un vértice que solamente tenga como arista al radio, es decir una arista de de w_0 a w_i con $1 \leq i \leq n$, el $q-$ peso del arco es igual a cero.

Definición 3.2.7. *($q-$ peso del árbol) Definimos el $q-$* ***peso del árbol generador*** *T como el producto de los pesos de q para todos los arcos del árbol generador.*

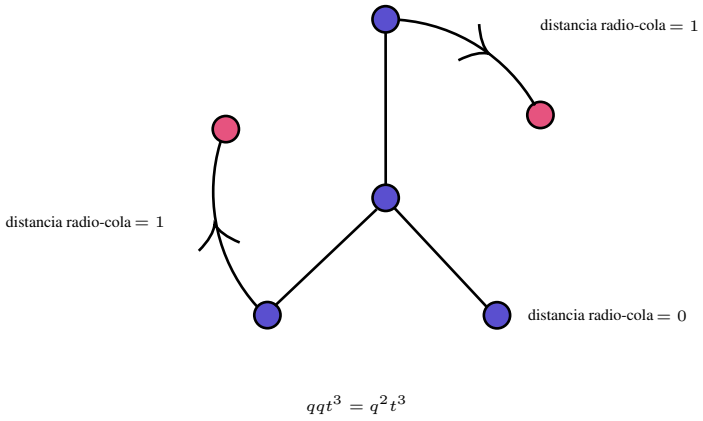


Figura 3.6: Árbol generador T de W_5.

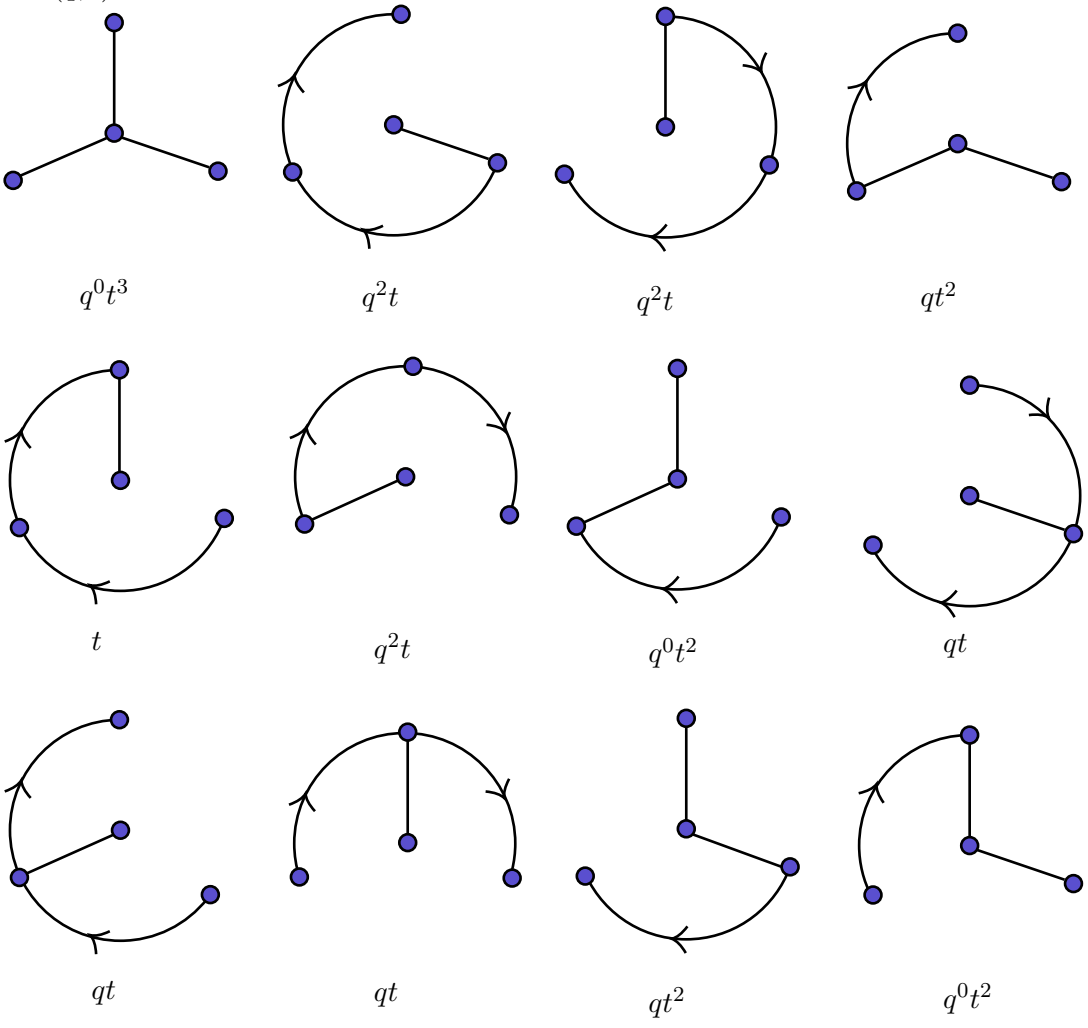
Con la interpretación combinatoria realizada, es posible definir un $(q,t)-$ polinomio relacionado con la enumeración de los árboles generadores de un grafo W_n.

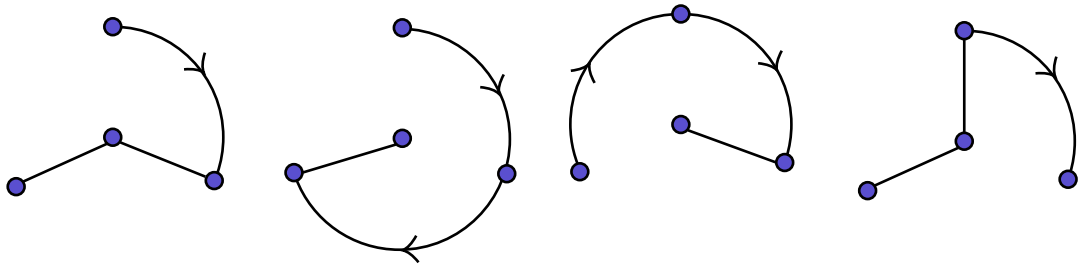
Definición 3.2.8. *Sea W_n un grafo de rueda con $n+1$ vértices, definimos el $(q,t)-$* ***polinomio de rueda*** *como:*

$$\mathcal{W}_n(q,t) = \sum_{T \text{ es un árbol generador de } W_n} q^{\text{suma de las distancias cola-radio en } T} t^{\#\text{radios en } T}.$$

A continuación se muestra el cálculo de un caso particular de los polinomios $\mathcal{W}_n(q,t)$.

Ejemplo 3.2.5. En este ejemplo vamos a considerar el grafo W_3 y construiremos el polinomio $\mathcal{W}_3(q,t)$.





q^0t^2 q^0t q^0t qt^2

Luego, el polinomio resultante es

$$\mathcal{W}_3(q,t) = t^3 + (3+3q+3q^2)t + (3+3q)t^2.$$

Observemos que el resultado de evaluar $(q,-N_1)$ en el polinomio $\mathcal{W}_3(q,t)$ es el coeficiente $-N_3$.

$$\begin{aligned} -\mathcal{W}_3(q,-N_1) &= N_1^3 + (3+3q+3q^2)N_1 - (3+3q)N_1^2, \\ &= N_3. \end{aligned}$$

Nuevamente, los coeficientes N_k depende de N_1.

Este resultado, indica que existe una relación entre el conteo de árboles generadores de un grafo de rueda W_k y los coeficientes N_k que se fundamenta en una interpretación de los números de Lucas con la sucesión $\{L_{2k}-2\}$.

Teorema 3.2.2. *Sea W_k un grafo de rueda con $k \geq 1$, entonces*

$$N_k = -\mathcal{W}_k(q,-N_1)$$

donde

$$P_{i,k}(q) = \sum_{T \text{ es un árbol generador de } W_k} q^{\text{suma radio - cola en } T}.$$

Es posible realizar la demostración del Teorema 3.2.2 con herramientas de teoría de grafos directamente (ver [12] para más detalles). Otra demostración del Teorema 3.2.2, utiliza funciones generatrices de los divisores de una curva de género $g = 1$.
Sea C una curva sobre $\mathbb{F}_q$, la función zeta puede ser escrita en términos de los divisores positivos de C como

$$Z(C/\mathbb{F}_q;T) = 1 + \sum_{k\geq 1} H_k T^k. \tag{3.9}$$

Trabajando con curvas de género $g = 1$, los valores H_k se pueden reescribir en términos de N_1 y q como se muestra a continuación.

Proposición 3.2.2. *Sea C una curva de género $g = 1$ sobre un campo finito $\mathbb{F}_q$ el número de divisores positivos H_k de grado k, satisfacen la propiedad:*

$$H_k = N_1(1 + q + q^2 + \cdots + q^{k-1}),\ k \geq 1\ y\ \ H_0 = 1 \tag{3.10}$$

Demostración. Sea C una curva de género $g = 1$. Sabemos que para el casos de una curva C de género $g = 1$, la función zeta asociada a dicha curva se puede expresar de la forma

$$\begin{aligned} Z(C/\mathbb{F}_q;T) &= \frac{1-(1+q-N_1)T+qT^2}{(1-T)(1-qT)} \\ &= 1 + \frac{N_1T}{(1-T)(1-qT)} \\ Z(C/\mathbb{F}_q;T) &= 1 + \frac{N_1T}{(1-T)(1-qT)}. \end{aligned} \tag{3.11}$$

Igualamos las expresiones (3.9) y (3.11) de la función zeta $Z(C/\mathbb{F}_q;T)$.

$$\begin{aligned} 1 + \frac{N_1T}{(1-T)(1-qT)} &= 1 + \sum_{k\geq 1} H_kT^k \\ \frac{N_1T}{(1-T)(1-qT)} &= \sum_{k\geq 1} H_kT^k \\ N_1\left(\sum_{k\geq 1} T^k\right)\left(\sum_{k\geq 1} q^kT^k\right) &= \sum_{k\geq 1} H_kT^k. \end{aligned}$$

Comparando los coeficientes de T^k con $k \geq$ de ambos lados de la igualdad

$$[T^k]N_1\left(\sum_{k\geq 1} T^k\right)\left(\sum_{k\geq 1} q^kT^k\right) = [T^k]\left(\sum_{k\geq 1} H_kT^k\right). \tag{3.12}$$

Sabemos que el coeficientes de T^k del producto de las funciones generatrices es[***]

$$[T^k]N_1\left(\sum_{k\geq 1} T^k\right)\left(\sum_{k\geq 1} q^kT^k\right) = N_1\sum_{j=0}^{k-1} 1\cdot q^j = N_1(1 + q + q^2 + \cdots + q^{k-1}).$$

Sustituyendo en la expresión (3.12), se tiene

$$\begin{aligned} [T^k]N_1\left(\sum_{k\geq 1} T^k\right)\left(\sum_{k\geq 1} q^kT^k\right) &= [T^k]\left(\sum_{k\geq 1} H_kT^k\right). \\ N_1(1 + q + q^2 + \cdots + q^{k-1}) &= H_k. \end{aligned}$$

[***] Propiedad 5.54 de [5] para funciones generatrices.

Por lo tanto,

$$H_k = N_1(1 + q + q^2 + \cdots + q^{k-1}), \text{ con } k \geq 1.$$

■

Observación 1. *La deducción de H_k no se realizará puesto que los objetos que enumera son los divisores positivos de grado k de una curva C, tema que no será profundizado porque utiliza herramientas técnicas de geometría algebraica (para más detalles leer [14], capítulo II).*

A continuación, se presentan dos proposiciones que sirven como herramientas para la demostración del Teorema 3.2.2.

Proposición 3.2.3. *Sea $k \geq 1$*

$$N_k = \sum_{\lambda \vdash k} (-1)^{\ell(\lambda)-1} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, \ldots, d_k} \prod_{j=1}^{\ell(\lambda)} H_{\lambda_j}.$$

Demostración. Sea E una curva elíptica sobre $\mathbb{F}_q$. Sabemos que la función zeta es

$$Z(E/\mathbb{F}_q; T) = \exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right). \tag{3.13}$$

Aplicamos logaritmo a la expresión (3.13).

$$\log(Z(E/\mathbb{F}_q; T)) = \log\left(\exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right)\right). \tag{3.14}$$

Ahora, aplicamos logaritmo a la función zeta de E expresada de la forma (3.9) y se comparan los coeficientes de T^k:

$$[T^k]\log(Z(E/\mathbb{F}_q; T)) = \log(1 + \sum_{m\geq 1} H_m T^m)$$
$$\frac{N_k}{k} = [T^k]\log(1 + \sum_{m\geq 1} H_m T^m), \text{ por (3.14)}.$$

Aplicamos identidades de la serie geométrica $\log(1+x)$

$$[T^k]\frac{N_k}{k} = [T^k]\sum_{n\geq 1}(-1)^{n-1}\left(\sum_{m=1}^{k} H_m T^m\right)^n$$
$$\Rightarrow \frac{N_k}{k} = (-1)^{n-1}\left(\sum_{m=1}^{k} H_m T^m\right)^n$$
$$\frac{N_k}{k} = (-1)^{n-1}\left(H_1 T + H_2 T^2 + \cdots + H_k T^k\right)^n. \tag{3.15}$$

Luego, seleccionamos una partición de $\lambda \vdash k$ de modo que la longitud $\ell(\lambda) = n$. Por definición del multicombinatorio, se tiene que 3.15 es

$$\begin{aligned}\frac{N_k}{k} &= \left(H_1T + H_2T^2 + \cdots + H_kT^k\right)^n \\ &= \sum_{\lambda\vdash k} \frac{(-1)^{n-1}}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, d_2, \cdots, d_k} \prod_{i=1}^{\ell(\lambda)} H_{\lambda_i} \\ &= \sum_{\lambda\vdash k} \frac{(-1)^{\ell(\lambda)-1}}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, d_2, \cdots, d_k} \prod_{i=1}^{\ell(\lambda)} H_{\lambda_i}.\end{aligned}$$

Por lo tanto, se cumple que

$$N_k = \sum_{\lambda\vdash k} (-1)^{\ell(\lambda)-1} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, d_2, \cdots, d_k} \prod_{i=1}^{\ell(\lambda)} H_{\lambda_i}.$$

■

La siguiente proposición, es una consecuencia de la Proposición 3.2.3.

Proposición 3.2.4. *Las fórmulas para los polinomios N_k en términos de q y N_1 se definen como*

$$N_k = \sum_{\lambda\vdash k} (-1)^{\ell(\lambda)-1} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, \ldots, d_k} \left(\prod_{j=1}^{\ell(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_j - 1}) \right) N_1^{\ell(\lambda)}.$$

Demostración. Sea C una curva de género $g = 1$ y N_k con $k \geq 1$, son los coeficientes de la función $Z(C,T)$. Para la demostración, recordemos que existe una identidad entre N_1 y las cantidades H_k entonces basta con sustituir la igualdad (3.10) en

$$N_k = \sum_{\lambda\vdash k} (-1)^{\ell(\lambda)-1} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, d_2, \cdots, d_k} \prod_{i=1}^{\ell(\lambda)} H_{\lambda_i}$$

obtenida en la Proposición 3.2.3. Así,

$$N_k = \sum_{\lambda\vdash k} (-1)^{\ell(\lambda)-1} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, d_2, \cdots, d_k} \prod_{i=1}^{\ell(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_i - 1}) N_1^{\ell(\lambda)}.$$

■

Proposición 3.2.5. *Sea $k \geq 1$*

$$\mathcal{W}_k(q,t) = \sum_{\substack{\lambda\vdash k \\ \ell(\lambda)=i}} \frac{k}{i} \binom{i}{d_1, \ldots, d_k} \left(\prod_{j=1}^{i} (1 + q + q^2 + \cdots + q^{\lambda_j - 1}) \right) t^{\ell(\lambda)}.$$

Demostración. Sea W_k un grafo de rueda, para la demostración consideremos un árbol generador T y se contará el total de formas que puede ser construido. Elegimos una partición de $k \geq 1$, digamos $\lambda = \langle 1^{d_1} 2^{d_2} \cdots k^{d_k} \rangle$, representa la cantidad de arcos de cada longitud que conforman el árbol generador T, es decir d_1 arcos de longitud 1, d_2 arcos de longitud 2 hasta d_k arcos de longitud k. Por lo que, el total de arcos de T serán $\ell(\lambda) = i$ que es la longitud de la partición $\lambda \vdash k$. Además, por la definición de árbol generador T, el total de radios es igual al número de arcos

$$\ell(\lambda) = i.$$

Seguidamente, se eligen como estarán distribuidos los arcos $\ell(\lambda)$ y el vértice exterior con el que se van a iniciar a colocar en este caso son k opciones. De tal forma que el total de arreglos es

$$\frac{k}{\ell(\lambda)} \binom{i}{d_1, \ldots, d_k}.$$

Finalmente, elegimos dónde se unen los arcos con los radios que son $\ell(\lambda)$.

$$\frac{k}{\ell(\lambda)} \binom{i}{d_1, \ldots, d_k} \left(\prod_{j=1}^{\ell(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_j - 1}) \right) t^{\ell(\lambda)}.$$

Por lo tanto,

$$\sum_{\substack{\lambda \vdash k \\ \ell(\lambda) = i}} \frac{k}{\ell(\lambda)} \binom{i}{d_1, \ldots, d_k} \left(\prod_{j=1}^{\ell(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_j - 1}) \right) t^{\ell(\lambda)}.$$

■

∗ **Demostración del Teorema 3.2.2**

Demostración. Sea W_k un grafo de rueda con $k+1$ vértices, se debe demostrar que

$$N_k = -\mathcal{W}_k(q, -N_1).$$

Por la Proposición 3.2.4 se tiene que

$$N_k = \sum_{\lambda \vdash k} (-1)^{\ell(\lambda)-1} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, d_2, \cdots, d_k} \prod_{i=1}^{\ell(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_i - 1}) N_1^{\ell(\lambda)}.$$

Seguidamente, utilizamos la identidad demostrada en la Proposición 3.2.5 y evaluamos en $(q, -N_1)$.

$$\mathcal{W}_k(q, -N_1) = \sum_{\lambda \vdash k} (-1)^{\ell(\lambda)} \frac{k}{\ell(\lambda)} \binom{\ell(\lambda)}{d_1, \ldots, d_k} \left(\prod_{i=1}^{\ell(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_i - 1}) \right) N_1^{\ell(\lambda)}.$$

Por lo tanto,

$$N_k = -\mathcal{W}_k(q, -N_1).$$

■

3.3. Dualidad combinatoria

3.3.1. Dualidad entre la función completa h_k y elemental e_k

Definición 3.3.1. *Definimos los $(q,t)-$* ***polinomios de Fibonacci*** *como una sucesión de polinomios en las variables q y t dado por*

$$F_k(q,t) = \sum_{S\subseteq\{1,2,3,\ldots,k-1\}:S\cap\left(S_1^{(k-1)}-\{1\}\right)=\emptyset} q^{\#\textit{elemento pares en } S} t^{\lceil \frac{k}{2}\rceil - \#S}.$$

Ejemplo 3.3.1. Primeros polinomios de Fibonacci

k	$F_k(q,t)$
1	t
2	$1+t$
3	$t^2+(1+q)t$
4	$t^2+(2+q)t+1$
5	$\left(1+q+q^2\right)t+2(1+q)t^2+t^3$

Cuadro 3.2: Primeros $(q,t)-$ polinomios de Fibonacci.

Proposición 3.3.1. $F_{2n+1}(q,t) = (1+q+t)F_{2n-1}(q,t) - qF_{2n-3}(q,t)$ *para* $n \geq 2$.

Demostración. Por definición de los $(q,t)-$ polinomios de Fibonacci, el lado izquierdo de la igualdad, es la cantidad de cadenas de longitud $2n$ sin dos cuentas negras consecutivas. Ahora analizamos el lado derecho, considerando que ahora vamos a unir dos cadenas:

- El término $(1+q+t)F_{2n-1}(q,t)$ indica la unión de una collar de longitud 2 con una cadena de longitud $2n-2$, puesto que

  $$(1+q+t)F_{2n-1}(q,t) = L_2(q,t)F_{2n-1}(q,t).$$

- Ahora descontamos los casos en los que la cuenta $2n-2$ y $2n-1$ son ambas color negro.Por lo que en total son

  $$qF_{2n-3}(q,t).$$

  Entonces la cuenta $2n-3$ y la cuenta $2n$ debe ser blanca.

En consecuencia, el total de formas de construir cadenas de longitud $2n$ a partir de una de longitud 2 y otra de longitud $2n-2$ es

$$(1+q+t)F_{2n-1}(q,t) - qF_{2n-3}(q,t).$$

Por lo tanto, la proposición es verdadera puesto que se ha encontrado dos formas de contar cadenas de longitud $2n$. ■

Teorema 3.3.1. *Sea C una curva de género $g=1$ y $E_n = e_n[1+q-\alpha_1-\alpha_2]$ entonces para $n \geq 1$, $E_{-n}=0$, $E_0=1$ y*

$$E_n = (-1)^n F_{2n-1}(q,-N_1).$$

La demostración del Teorema 3.3.1, se realizará comprobando ambos lados de la igualdad cumplen con la misma recurrencia.

Observación 2. *Los objetos que contabiliza E_k son los divisores con signo de una curva C de género $g=1$. La teoría de divisores es un tema muy profundo en geometría algebraica y se extiende sobre los objetivos del capítulo, por tal razón solamente se abordará el enfoque combinatorio. Para el lector interesado en profundizar sobre teoría de divisores puede leer en [14], Capítulo II, sección 3 y [11] capítulo 2.*

Proposición 3.3.2. $(-1)^{n+1}E_{n+1} = (1+q-N_1)(-1)^n E_n - q(-1)^{n-1}E_{n-1}$ *para $n \geq 2$.*

Demostración. La demostración se desarrollará utilizando propiedades de la operación del pletismo de las funciones simétricas (ver [17], capítulo 7 para más detalles).
Consideremos que

$$f = \alpha_1 + \alpha_2$$
$$g = 1 + q - \alpha_1 - \alpha_2$$

En consecuencia, de las identidades del pletismo de funciones simétricas y la definición de los E_n se tiene que

$$e_n[A+B] = \sum_{i=0}^{n} e_i[A]e_{n-i}[B].$$

Seguidamente, se realizan los cálculos

$$\begin{aligned}
e_{n+1}[f+g] &= \sum_{i=0}^{n+1} e_i[\alpha_1+\alpha_2]e_{n+1-i}[1+q-\alpha_1-\alpha_2] \\
&= e_0[\alpha_1+\alpha_2]e_{n+1}[1+q-\alpha_1-\alpha_2] + e_1[\alpha_1+\alpha_2]e_n[1+q-\alpha_1-\alpha_2]+ \\
&\quad e_2[\alpha_1+\alpha_2]e_{n-1}[1+q-\alpha_1-\alpha_2] + e_3[\alpha_1+\alpha_2]e_{n-2}[1+q-\alpha_1-\alpha_2] \\
&\quad + \cdots + e_n[\alpha_1+\alpha_2]e_1[1+q-\alpha_1-\alpha_2] + e_{n+1}[\alpha_1+\alpha_2]e_0[1+q-\alpha_1-\alpha_2] \\
&= e_{n+1}[1+q-\alpha_1-\alpha_2] + (\alpha_1+\alpha_2)e_n[1+q-\alpha_1-\alpha_2] \\
&\quad + \alpha_1\alpha_2 e_{n-1}[1+q-\alpha_1-\alpha_2] \\
e_{n+1}[1+q] &= e_{n+1}[1+q-\alpha_1-\alpha_2] + (1+q-N_1)e_n[1+q-\alpha_1-\alpha_2] \\
&\quad + qe_{n-1}[1+q-\alpha_1-\alpha_2] \\
0 &= e_{n+1}[1+q-\alpha_1-\alpha_2] + (1+q-N_1)e_n[1+q-\alpha_1-\alpha_2] \\
&\quad + qe_{n-1}[1+q-\alpha_1-\alpha_2] \\
-e_{n+1}[1+q-\alpha_1-\alpha_2] &= (1+q-N_1)e_n[1+q-\alpha_1-\alpha_2] + qe_{n-1}[1+q-\alpha_1-\alpha_2] \\
e_{n+1}[1+q-\alpha_1-\alpha_2] &= -(1+q-N_1)e_n[1+q-\alpha_1-\alpha_2] - qe_{n-1}[1+q-\alpha_1-\alpha_2]. \\
E_{n+1} &= -(1+q-N_1)E_n - qE_{n-1}.
\end{aligned}$$

Si $n \geq 2$ implica que

$$e_{n+1}[1+q] = 0.$$

Así, obtenemos que

$$e_{n+1}[1+q-\alpha_1-\alpha_2] = -(1+q-N_1)e_n[1+q-\alpha_1-\alpha_2] - qe_{n-1}[1+q-\alpha_1-\alpha_2].$$

Luego, multiplicando por $(-1)^{n+1}$ a ambos lados de la igualdad resulta la identidad

$$\begin{aligned}
(-1)^{n+1}e_{n+1}[1+q-\alpha_1-\alpha_2] &= (1+q-N_1)(-1)^n e_n[1+q-\alpha_1-\alpha_2] \\
&\quad -q(-1)^{n-1}e_{n-1}[1+q-\alpha_1-\alpha_2].
\end{aligned}$$

Por lo tanto, por definición de los E_n

$$(-1)^{n+1}E_{n+1} = (1+q-N_1)(-1)^n E_n - q(-1)^{n-1}E_{n-1}.$$

■

Con el resultado anterior, retomaremos la demostración del Teorema 3.3.1.

∗ **Demostración del Teorema 3.3.1**.

Demostración. Sea C una curva sobre $\mathbb{F}_q$ de género $g = 1$, se debe demostrar que para $n \geq 1$

$$E_n = (-1)^n F_{2n-1}(q, -N_1),\ E_{-n} = 0,\ \text{y}\ E_0 = 1.$$

Demostrando que ambos lados de la igualdad satisfacen la misma relación de recurrencia. Primero comprobamos que las condiciones iniciales son iguales:

- Si $k = 1$

$$E_1 = e_1[1 + q - \alpha_1 - \alpha_2] = 1 + q - \alpha_1 - \alpha_2 = N_1 = -F_1(q, -N_1).$$

- Si $k = 2$

$$\begin{aligned}
E_2 &= e_2[1 + q - \alpha_1 - \alpha_2] \\
&= e_2(1, q, \alpha_1, \alpha_2) \\
&= \frac{1}{2}(1 + q - \alpha_1 - \alpha_2)^2 - \frac{1}{2}(1 + q^2 - \alpha_1^2 - \alpha_2^2) \\
&= \frac{1}{2}N_1^2 - \frac{1}{2}N_2 \\
&= \frac{1}{2}\left(N_1^2 - N_2\right) \\
&= \frac{1}{2}(N_1^2 - (2 + 2q)N_1 + N_1^2) \\
&= \frac{1}{2}(2N_1^2 - 2(1 + q)N_1) \\
&= \frac{2}{2}\left(N_1^2 - (1 + q)N_1\right) \\
E_2 &= N_1^2 - (1 + q)N_1 = F_3(q, -N_1).
\end{aligned}$$

Con los dos casos anteriores muestran que las condiciones iniciales son iguales.

Por la Proposición 3.3.2 y la Proposición 3.3.1 ambos lados de la igualdad cumplen la misma relación de recurrencia.

Por lo tanto,

$$E_n = (-1)^n F_{2n-1}(q, -N_1).$$

■

Lema 3.3.1.

$$h_k[\alpha_1 + \alpha_2] = (-1)^k E_{k+1}/N_1$$

donde α_1 y α_2 son raíces del polinomios $T^2 - (1 + q - N_1)T + q$.

Demostración. Inducción sobre k.

Caso base.
$k = 1$

$$\begin{aligned}
h_1[\alpha_1 + \alpha_2] &= \alpha_1 + \alpha_2 = 1 + q - N_1 \\
E_2 = e_2[1 + q - \alpha_1 - \alpha_2] &= -(1 + q)N_1 + N_1^2 \\
\frac{E_2}{N_1} = \frac{e_2[1 + q - \alpha_1 - \alpha_2]}{N_1} &= -[1 + q - N_1] = -h_1[\alpha_1 + \alpha_2].
\end{aligned}$$

$k = 2$

$$\begin{aligned} h_2[\alpha_1 + \alpha_2] &= \alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2 \\ &= \left(\alpha_1^2 + \alpha_2^2\right) + q \\ &= (1 + q - N_1)^2 - 2q + q \\ &= (1+q)^2 - 2(1+q)N_1 + N_1^2 - q \\ &= 1 + 2q + q^2 - 2(1+q)N_1 + N_1^2 - q \\ h_2[\alpha_1 + \alpha_2] &= 1 + q + q^2 - 2(1+q)N_1 + N_1^2. \end{aligned}$$

$$\begin{aligned} E_3 &= (-1)^2 F_5(q, -N_1), \text{ por el Teorema 3.3.1} \\ &= \left(1 + q + q^2\right) N_1 - (2 + 2q)N_1^2 + N_1^3 \\ \frac{E_3}{N_1} &= \left(1 + q + q^2\right) - 2(1+q)N_1 + N_1^2 = h_2[\alpha_1 + \alpha_2]. \end{aligned}$$

Hipótesis inductiva. Supongamos que para $2 \leq k$ se satisface que

$$h_k[\alpha_1 + \alpha_2] = (-1)^k E_{k+1}/N_1.$$

Paso inductivo. Se demostrará que la propiedad es cierto para $k+1$, es decir

$$h_{k+1}[\alpha_1 + \alpha_2] = (-1)^{k+1} E_{k+2}/N_1.$$

Partimos del lado derecho de la igualdad y utilizamos la identidad de los E_k de la Proposición 3.3.4

$$(-1)^{k+2} E_{k+2} = (1 + q - N_1)(-1)^{k+1} E_{k+1} - q(-1)^k E_k.$$

Dividimos entre N_1:

$$\begin{aligned} (-1)^{k+2} E_{k+2}/N_1 &= (1 + q - N_1)(-1)^{k+1} E_{k+1}/N_1 - q(-1)^k E_k/N_1 \\ -(-1)^{k+1} E_{k+2}/N_1 &= -(1 + q - N_1)(-1)^k E_{k+1}/N_1 + q(-1)^{k-1} E_k/N_1 \\ -(-1)^{k+1} E_{k+2}/N_1 &= -(1+q)(-1)^k E_{k+1}/N_1 + N_1(-1)^k E_{k+1}/N_1 \\ &\quad + q(-1)^{k-1} E_k/N_1 \\ (-1)^{k+1} E_{k+1} &= (-1)^{k+1} E_{k+2}/N_1 + (1+q)(-1)^{k+1} E_{k+1}/N_1 \quad + q(-1)^{k-1} E_k/N_1 \\ E_{k+1} &= E_{k+2}/N_1 + (1+q)E_{k+1}/N_1 + qE_k/N_1. \end{aligned} \tag{3.16}$$

Aplicando una identidad del pletismo se obtiene,

$$\begin{aligned}
E_{k+1} &= e_{k+1}[1+q-\alpha_1-\alpha_2] \\
&= \sum_{i=0}^{k+1}(-1)^{k+1-i}e_i[1+q]h_{k+1-i}[\alpha_1+\alpha_2] \\
&= (-1)^{k+1}e_0[1+q]h_{k+1}[\alpha_1+\alpha_2] + (-1)^k e_1[1+q]h_k[\alpha_1+\alpha_2] \\
&+ \ (-1)^{k-1}e_2[1+q]h_{k-1}[\alpha_1+\alpha_2] + \cdots + e_{k+1}[1+q]h_0[\alpha_1+\alpha_2] \\
&= (-1)^{k+1}(1)h_{k+1}[\alpha_1+\alpha_2] + (-1)^k(1+q)h_k[\alpha_1+\alpha_2] \\
&+ (-1)^{k-1}qh_{k-1}[\alpha_1+\alpha_2] \\
&= (-1)^{k+1}h_{k+1}[\alpha_1+\alpha_2] + (-1)^k(1+q)h_k[\alpha_1+\alpha_2] \\
&\qquad + (-1)^{k-1}qh_{k-1}[\alpha_1+\alpha_2] \\
&= (-1)^{k+1}h_{k+1}[\alpha_1+\alpha_2] + (1+q)E_{k+1}/N_1 + qE_k/N_1, \text{ por la hipótesis inductiva.}
\end{aligned}$$

De esta forma, se obtiene una expresión para E_{k+1} en términos de los anteriores.

$$E_{k+1} = (-1)^{k+1}h_{k+1}[\alpha_1+\alpha_2] + (1+q)E_{k+1}/N_1 + qE_k/N_1. \tag{3.17}$$

Igualando las expresiones (3.16) y (3.17) para E_{k+1}

$$\begin{aligned}
E_{k+2}/N_1 + (1+q)E_{k+1}/N_1 + qE_k/N_1 &= (-1)^{k+1}h_{k+1}[\alpha_1+\alpha_2] + (1+q)E_{k+1}/N_1 + qE_k/N_1 \\
E_{k+2}/N_1 &= (-1)^{k+1}h_{k+1}[\alpha_1+\alpha_2] \\
(-1)^{k+1}E_{k+2}/N_1 &= h_{k+1}[\alpha_1+\alpha_2].
\end{aligned}$$

Por lo tanto,

$$h_{k+1}[\alpha_1+\alpha_2] = (-1)^{k+1}E_{k+2}/N_1.$$

■

Lema 3.3.2. *Sea E una curva elíptica y definimos la función generatriz del número de árboles de un grafo de rueda como la función exponencial*

$$W(q,N_1,T) = \exp\left(\sum_{k\geq 1}\mathcal{W}_k(q,N_1)\frac{T^k}{k}\right) = 1 + \sum_{k\geq 1}F_{2k-1}(q,N_1)T^k.$$

Demostración. Por el Teorema 3.2.2.

$$-\mathcal{W}_k(q,-N_1) = N_k.$$

Evaluando en $N_1 = -N_1$ en la función generatriz se obtiene que

$$\begin{aligned}
W(q, N_1, T) &= \exp\left(\sum_{k\geq 1} \mathcal{W}_k(q, N_1)\frac{T^k}{k}\right) \\
&= \exp\left(\sum_{k\geq 1} \mathcal{W}_k(q, -N_1)\frac{T^k}{k}\right) \\
&= \exp\left(\sum_{k\geq 1} (-N_k)\frac{T^k}{k}\right) \\
&= \exp\left(-\left(\sum_{k\geq 1} N_k\frac{T^k}{k}\right)\right) \\
&= \frac{1}{\exp\left(\sum_{k\geq 1} N_k\frac{T^k}{k}\right)} \\
&= \frac{1}{Z(E/\mathbb{F}_q; T)} \\
&= \frac{1}{\frac{1-(1+q-N_1)T+qT^2}{(1-T)(1-qT)}} \\
&= \frac{(1-T)(1-qT)}{1-(1+q-N_1)T+qT^2} \\
&= \sum_{k\geq 0} (-1)^k E_k T^k \\
W(q, N_1, T) &= 1 + \sum_{k\geq 1} (-1)^k F_{2k-1}(q, -N_1)T^k.
\end{aligned}$$

Por lo tanto,

$$W(q, t, T) = 1 + \sum_{k\geq 1} (-1)^k F_{2k-1}(q, t)T^k.$$

■

3.3.2. Dualidad entre los números de Lucas y Fibonacci

Lema 3.3.3. *Para $1 \leq i \leq k$ y $0 \leq j \leq k - i$, el número de subconjuntos S_1 de $\{1, 2, \ldots, 2k\}$ denotado por $c_{i,j}$ con $k - i - j$ elementos impares, j elementos pares, y con elementos no circularmente consecutivos es igual a*

$$c_{i,j} = \frac{k}{i} b_{i,j}$$

donde

$$b_{i,j} = \#(\textit{subconjuntos } S_2 \textit{ de } \{1, 2, \ldots, 2k-2\} \textit{ , con } k-i-j \textit{ elementos impares } j \textit{ elementos pares sin dos elementos consecutivos }).$$

Una demostración sobre este resultado, hace uso de la biyección que existe entre los subconjuntos enumerados por los números de Lucas y los enumerados por los números de Fibonacci en ([12], Sección 3, pág. 16).

Ejemplo 3.3.2. Si $k = 2 \rightarrow 1 \leq i \leq 2$ y $0 \leq j \leq k - i$.

Los subconjuntos del conjunto $\{1, 2, 3, 4\}$ sin elementos circularmente consecutivos:

$$\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 3\}, \{2, 4\}.$$

Los subconjuntos del conjunto $\{1, 2\}$ sin elementos consecutivos: $\emptyset,\ \{1\}, \{2\}$.

(I) $i = 1\ \rightarrow j = 0, 1.$

- $j = 0.$
  - Elementos impares:

  $$k - i - j = 2 - 1 - 0 = 1.$$

  - Elementos pares: $j = 0$ entonces el total de subconjuntos es

  $$b_{1,0} = 1.$$

  Representa la cantidad de subconjuntos de $\{1, 2\}$ sin elementos consecutivos con 0 elementos pares y 1 elemento impar es decir $\{1\}$.
  El número de subconjuntos de $\{1, 2, 3, 4\}$ sin elementos circularmente consecutivos con 1 elementos impar y cero pares es

  $$c_{1,0} = 2 = \frac{2}{1} b_{1,0}.$$

  Este valor hace referencia a los subconjuntos $\{1\}$ y $\{3\}$.
- $j = 1.$
  - Elementos impares:

  $$k - i - j = 2 - 1 - 1 = 0.$$

  - Elementos pares: $j = 1.$

  $$b_{1,1} = 1.$$

  Indica la cantidad de subconjuntos de $\{1, 2\}$ sin 2 elementos consecutivos con 1 elemento par y 0 elementos impares, corresponde al subconjunto $\{2\}$.

El número de subconjuntos de $\{1,2,3,4\}$ sin elementos circularmente consecutivos con un 1 par es

$$c_{1,1} = 2 = \frac{2}{1} b_{1,1}.$$

Los subconjuntos son: $\{2\},\ \{4\}$.

(II) $i = 2 \to j = 0$.

- Elementos impares:

$$k - i - j = 2 - 2 - 0 = 0.$$

- Elementos pares: $j = 0$. El número de subconjuntos de $\{1,2\}$ sin elementos consecutivos con cero elementos pares e impares es

$$b_{2,0} = 1$$

corresponde al subconjunto $\emptyset$. Luego, el número de subconjuntos sin elementos circularmente consecutivos con cero elementos pares e impares es

$$c_{2,0} = \frac{2}{2} b_{2,0} = 1.$$

corresponde al subconjunto $\emptyset$ de $\{1,2,3,4\}$.

La siguiente proposición nos muestra una identidad que permite calcular los polinomios $P_{i,k}(q)$ de forma explícita utilizando coeficientes binomiales. Esta identidad, surge como consecuencia del Lema 3.3.3.

Proposición 3.3.3. *Para $k \geq 1$ y $1 \leq i \leq k$, tenemos que*

$$P_{i,k}(q) = \sum_{j=0}^{k-i} \frac{k}{i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j.$$

Demostración. Sea $k \geq 1$ y $1 \leq i \leq k$, se debe demostrar que se cumple la identidad

$$P_{i,k}(q) = \sum_{j=0}^{k-i} \frac{k}{i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j.$$

Partimos del lado izquierdo de la igualdad y recordamos la interpretación combinatoria de los $(q,t)-$ polinomios de Fibonacci.

$$\begin{aligned} \Rightarrow \frac{k}{i} P_{i,k}(q) &= [N_1^i] F_{2k-1}(q, N_1) \\ &= \sum_{j=0}^{k-i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j. \end{aligned}$$

Por lo tanto,

$$P_{i,k}(q) = \sum_{j=0}^{k-i} \frac{k}{i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j.$$

■

Nota 6. *Con el resultado anterior comprobamos que los polinomios comprobamos la positividad de los coeficientes que establece el Teorema 3.1.1, es decir $P_{i,k} \in \mathbb{Z}[q]_{>0}$.*

Proposición 3.3.4. *Sea $k \geq 1$*

$$E_k = \sum_{i=1}^{k} \frac{(-1)^{k+i} \cdot i}{k} P_{i,k}(q) N_1^i.$$

Demostración. Sea E una curva elíptica. Por definición de E_k se tiene que

$$E_k = e_k[1 + q - \alpha_1 - \alpha_2].$$

Además la función generatriz es

$$\begin{aligned}
\sum_{k\geq 0}(-1)^k E_k T^k &= 1 + \sum_{k\geq 1}(-1)^k E_k T^k \\
\sum_{k\geq 1}(-1)^k E_k T^k &= \sum_{k\geq 0}(-1)^k E_k T^k - 1 \\
&= \frac{1}{Z(E,T)} - 1 \\
&= \frac{1}{1 + \frac{N_1 T}{(1-T)(1-qT)}} - 1 \\
&= \sum_{k\geq 0}(-1)^k \left(\frac{N_1 T}{(1-T)(1-qT)}\right)^k - 1 \\
&= \sum_{k\geq 1}(-1)^k \left(\frac{N_1 T}{(1-T)(1-qT)}\right)^k \\
&= -N_1 \frac{d}{dN_1}\left(\sum_{k\geq 1} \frac{(-1)^{k-1}}{k} \left(\frac{N_1 T}{(1-T)(1-qT)}\right)^k\right) \\
&= -N_1 \frac{d}{dN_1}\left(\log\left(1 + \frac{N_1 T}{(1-T)(1-qT)}\right)\right) \\
&= -N_1 \frac{d}{dN_1}(\log(Z(E,T))
\end{aligned}$$

$$
\begin{aligned}
&= -N_1 \frac{d}{dN_1}\left(\log\left(\exp\left(\sum_{k\geq 1}\frac{N_k}{k}T^k\right)\right)\right)\\
&= -N_1 \frac{d}{dN_1}\left(\sum_{k\geq 1}\frac{N_k}{k}T^k\right)\\
&= -N_1 \frac{d}{dN_1}\left(\sum_{k\geq 1}\frac{1}{k}\sum_{i=1}^{k}(-1)^{i-1}P_{i,k}(q)N_1^i T^k\right)\\
\sum_{k\geq 1}(-1)^k E_k T^k &= \sum_{k\geq 1}\sum_{i=1}^{k}(-1)^i \frac{i}{k}P_{i,k}(q)N_1^i T^k.
\end{aligned}
$$

Comparando el coeficiente de T^k se obtiene que

$$(-1)^k E_k T^k = \sum_{i=1}^{k}(-1)^i \frac{i}{k}P_{i,k}(q)N_1^i T^k.$$

■

Corolario 3.3.1.

$$N_k(q,N_1) = \sum_{i=1}^{k}\sum_{j=0}^{k-i}\frac{(-1)^{i+1}\cdot k}{i}\binom{k-1-j}{i-1}\binom{i+j-1}{j}N_1^i q^j$$

y

$$E_k = \sum_{i=1}^{k}\sum_{j=0}^{k-i}(-1)^{k+i}\binom{k-1-j}{i-1}\binom{i+j-1}{j}N_1^i q^j.$$

Demostración. Por el Teorema 3.1.1

$$
\begin{aligned}
N_k(q,N_1) &= \sum_{i=1}^{k}(-1)^{i-1}P_{i,k}(q)N_1^i\\
&= \sum_{i=1}^{k}(-1)^{i-1}\sum_{j=0}^{k-i}\frac{k}{i}\binom{k-1-j}{i-1}\binom{i+j-1}{j}q^j N_1^i\\
&= \sum_{i=1}^{k}\sum_{j=0}^{k-i}\frac{(-1)^{i-1}\cdot k}{i}\binom{k-1-j}{i-1}\binom{i+j-1}{j}q^j N_1^i, \text{ por la Proposición 3.3.3.}\\
N_k(q,N_1) &= \sum_{i=1}^{k}\sum_{j=0}^{k-i}\frac{(-1)^{i-1}\cdot k}{i}\binom{k-1-j}{i-1}\binom{i+j-1}{j}q^j N_1^i.
\end{aligned}
$$

Ahora se demostrará la identidad

$$E_k = \sum_{i=1}^{k} \sum_{j=0}^{k-i} (-1)^{k+i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} N_1^i q^j.$$

Por la Proposición 3.3.4

$$\begin{aligned} E_k &= \sum_{i=1}^{k} \frac{(-1)^{k+i} \cdot i}{k} P_{i,k}(q) N_1^i \\ &= \sum_{i=1}^{k} \frac{(-1)^{k+i} \cdot i}{k} \sum_{j=0}^{k-i} \frac{k}{i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j N_1^i, \text{ por la Proposición 3.3.3} \\ &= \sum_{i=1}^{k} \sum_{j=0}^{k-i} (-1)^{k+i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j N_1^i. \end{aligned}$$

■

Capítulo 4

Identidades combinatorias

Este capítulo es motivado por las propiedades de los coeficientes N_k estudiadas anteriormente; los cuales reflejan una importante conexión entre el álgebra y combinatoria. Mediante la exploración de los temas del Capítulo 3, presentamos una serie de resultados referentes a los coeficientes N_k de la función zeta asociada a una curva elíptica. Por lo cual se aclara que salvo se indique lo contrario al citar a otros autores, todo el trabajo del presente capítulo es debido a la autora.

4.1. Propiedades de la familia de polinomios $\{P_{i,k}(q)\}$

Iniciamos esta sección con el cálculo explícito de polinomios correspondientes a la familia $\{P_{i,k}(q)\}$, a partir de identidades que surgen a raíz de interpretaciones combinatorias de los números de Fibonacci y Lucas.
De acuerdo con la Proposición 3.3.3, los polinomios $\{P_{i,k}(q)\}$ están dados por la expresión:

$$P_{i,k}(q) = \sum_{j=0}^{k-i} \frac{k}{i} \binom{k-1-j}{i-1} \binom{i+j-1}{j} q^j \tag{4.1}$$

para $k \geq 1$ y $1 \leq i \leq k$. Aplicando este resultado, consideremos los siguientes casos particulares.

Ejemplo 4.1.1. En este ejemplo, nos enfocamos en el cálculo explícito de polinomios $\{P_{i,k}(q)\}$ utilizando la identidad 4.1.

- Para $i = 2$ y $k \geq 1$.

$$\begin{aligned}
P_{2,k}(q) &= \sum_{j=0}^{k-2} \frac{k}{2} \binom{k-1-j}{1} \binom{2+j-1}{j} q^j \\
&= \sum_{j=0}^{k-2} \frac{k}{2}(k-1-j) \binom{j+1}{j} q^j \\
&= \sum_{j=0}^{k-2} \frac{k}{2}(k-1-j)(j+1) q^j \\
P_{2,k}(q) &= \sum_{j=0}^{k-2} \frac{k}{2}(k-1-j)(j+1) q^j.
\end{aligned}$$

- Para $i = k-1$ y $k \geq 1$.

$$\begin{aligned}
P_{k-1,k}(q) &= \sum_{j=0}^{1} \frac{k}{k-1} \binom{k-1-j}{k-1-1} \binom{k-1+j-1}{j} q^j \\
&= \sum_{j=0}^{1} \frac{k}{k-1} \binom{k-1-j}{k-2} \binom{k+j-2}{j} q^j \\
&= \frac{k}{k-1} \binom{k-1}{k-2} \binom{k-2}{0} + \frac{k}{k-1} \binom{k-2}{k-2} \binom{k-1}{1} q \\
&= k + kq = k(1+q) \\
P_{k-1,k}(q) &= k(1+q).
\end{aligned}$$

- Para $i = k$.

$$\begin{aligned}
P_{k,k}(q) &= \sum_{j=0}^{k-k} \frac{k}{k} \binom{k-1-j}{k-1} \binom{k+j-1}{j} q^j \\
&= \binom{k-1}{k-1} \binom{k-1}{0} \\
P_{k,k}(q) &= 1.
\end{aligned}$$

- $i = 1$ y $k \geq 1$.

$$\begin{aligned} P_{1,k}(q) &= \sum_{j=0}^{k-1} k \binom{k-1-j}{0} \binom{j}{j} q^j, \\ &= \sum_{j=0}^{k-1} k q^j \\ P_{1,k}(q) &= \sum_{j=0}^{k-1} k q^j. \end{aligned}$$

En resumen, tenemos las siguientes fórmulas para los polinomios $\{P_{i,k}\}$.

$$P_{2,k}(q) = \sum_{j=0}^{k-2} \frac{k}{2}(k-1-j)(j+1)q^j \tag{4.2}$$

$$P_{1,k}(q) = \sum_{j=0}^{k-1} k q^j \tag{4.3}$$

$$P_{k-1,k}(q) = k(1+q) \tag{4.4}$$

$$P_{k,k}(q) = 1. \tag{4.5}$$

Con estos resultados, notemos que el polinomio 4.5 es constante cuando $i = k$, así comprobamos la observación hecha en el Teorema 3.1.1, ya que $P_{k,k}(q) = 1$ para $k \geq 1$.

Además, observemos que el polinomio 4.4 cuando los subíndices son enteros consecutivos el polinomio es el producto del $\max\{i, k\}$ con el polinomio $1+q$. Para este polinomio y el caso del polinomio (4.3), ya fueron trabajados en el Ejemplo 3.1.2, con la recurrencia de la familia de polinomios $\{P_{i,k}\}$ de la Proposición 3.1.3.
A continuación se presentan ejemplos de polinomios pertenecientes a la familia $\{P_{i,k}\}$.

Ejemplo 4.1.2.

- $i = 2$ y $k = 5$

$$\begin{aligned} P_{2,5}(q) &= \sum_{j=0}^{5-2} \frac{5}{2}(5-1-j)(j+1)q^j, \text{ por (4.2)} \\ &= \sum_{j=0}^{3} \frac{5}{2}(4-j)(j+1)q^j \\ &= \frac{5}{2}(4)(1) + \frac{5}{2}(4-1)(2)q + \frac{5}{2}(4-2)(3)q^2 + \frac{5}{2}(4-3)(4)q^3 \\ P_{2,5}(q) &= 10 + 15q + 15q^2 + 10q^3. \end{aligned}$$

- $i = 2$ y $k = 4$

$$\begin{aligned} P_{2,4}(q) &= \sum_{j=0}^{4-2} \frac{4}{2}(4-1-j)(j+1)q^j, \text{ por } (4.2) \\ &= \sum_{j=0}^{2} 2(3-j)(j+1)q^j \\ &= 2(3) + 2(2)(2)q + 2(1)(3)q^2 \\ P_{2,4}(q) &= 6 + 8q + 6q^2. \end{aligned}$$

- $i = 2$ y $k = 3$

$$\begin{aligned} P_{2,3}(q) &= 3(1+q), \text{ por } (4.4) \\ P_{2,4}(q) &= 3 + 3q. \end{aligned}$$

- $i = 1$ y $k = 2$

$$P_{1,2}(q) = 2(1+q) = 2 + 2q, \text{ por } (4.5).$$

En todos los casos, se verifica que coinciden con la tabla proporcionada en la Sección 3.1.

Otra identidad para calcular los polinomios de la familia $\{P_{i,k}\}$ proviene del conteo de árboles generadores de un grafo de rueda W_k con $k+1$ vértices, tal como establece la Proposición 3.2.5 y la Proposición 3.2.4. Es decir, por medio de la expresión

$$P_{i,k}(q) = \frac{k}{i} \sum_{\substack{\lambda \vdash k \\ \ell(\lambda)=i}} \binom{i}{d_1, \cdots, d_k} \prod_{j=1}^{i} (1 + q + \cdots + q^{\lambda_j - 1}). \tag{4.6}$$

Nuevamente, veremos algunas fórmulas explícitas utilizando los resultados que relacionan la teoría de grafos con dichos polinomios y luego realizaremos una comparación con las fórmulas encontradas por medio de la identidad 4.1.

Ejemplo 4.1.3. Consideremos los siguientes casos:

- Si $i = k$ y $k \geq 1$.

$$\begin{aligned} P_{k,k}(q) &= \binom{k}{k} \prod_{j=1}^{k} \left(1 + q + \cdots + q^{\lambda_j - 1}\right) \qquad (4.7) \\ &= \left(q^{1-1}\right) \cdots \left(q^{1-1}\right) \\ P_{k,k}(q) &= 1. \end{aligned}$$

- Si $i = 1$ y $k \geq 1$.

$$P_{1,k}(q) = \frac{k}{1} \sum_{\substack{\lambda \vdash k \\ \ell(\lambda)=1}} \binom{1}{0, \cdots, 1} \left(1 + q + \cdots + q^{\lambda_j - 1}\right) \tag{4.8}$$

$$P_{1,k}(q) = k \left(1 + q + \cdots + q^{k-1}\right).$$

- Si $i = 2$ y $k \geq 1$.

$$\begin{aligned} P_{2,k}(q) &= \frac{k}{2} \sum_{\substack{\lambda \vdash k \\ \ell(\lambda)=2}} \binom{2}{1,\ 1} \prod_{j=1}^{2} \left(1 + q + q^2 + \cdots + q^{\lambda_j - 1}\right) \\ &= k \sum_{\substack{\lambda \vdash k \\ \ell(\lambda)=2}} \prod_{j=1}^{2} \left(1 + q + q^2 + \cdots + q^{\lambda_j - 1}\right) \\ P_{2,k}(q) &= k \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} \left(1 + q + q^2 + \cdots + q^{i-1}\right) \left(1 + q + q^2 + \cdots + q^{(k-i)-1}\right). \end{aligned} \tag{4.9}$$

A partir de los ejemplos anteriores, podemos comprobar que al aplicar la identidad 4.6, para el caso de 4.7 y 4.8 se producen la mismas fórmulas como en el caso de utilizar la identidad 4.1.

Ahora bien, no sucede lo mismo con la deducción de la fórmula para el polinomio $P_{2,k}(q)$ y de hecho tenemos contraejemplos que verifican que no se cumple para cualquier valor de k.

Ejemplo 4.1.4. Consideremos los siguientes ejemplos aplicando (4.9).

- Si $k = 3$.

$$P_{2,3}(q) = 3(1)(1 + q) = 3 + 3q.$$

- Si $k = 4$

$$P_{2,4}(q) \neq 8 + 12q + 8q^2.$$

El cual no coincide con el polinomio mencionado, puesto que $P_{2,4}(q) = 6 + 8q + 6q^2$.

Sin embargo, cuando k es par vemos que la fórmula anterior no es válida, porque si k es par tenemos una partición $\lambda \vdash k$ de la forma $\frac{k}{2} + \frac{k}{2}$ entonces el multicombinatorio de la identidad es de la forma

$$\binom{2}{d_1, \cdots, 2, \cdots, d_k}, \text{ con } d_r = 0 \text{ cuando } r \neq \frac{k}{2}.$$

Quiere decir que para calcular el polinomio debemos saber la paridad de k. Así, los polinomios $P_{2,k}(q)$ quedan determinados por la siguiente expresión

$$P_{2,k}(q)=\begin{cases}\sum_{j=1}^{\lfloor \frac{k}{2}\rfloor} k\left(1+q+q^2+\cdots+q^{j-1}\right)\left(1+q+q^2+\cdots+q^{(k-j)-1}\right) & \text{, si } k \text{ es impar.}\\ \sum_{j=1}^{\frac{k}{2}-1} k\left(1+q+q^2+\cdots+q^{j-1}\right)\left(1+q+q^2+\cdots+q^{(k-j)-1}\right)^2 & \text{, si } k \text{ es par.}\\ +\frac{k}{2}\left(1+q+\cdots+q^{\frac{k}{2}-1}\right)^2 & \end{cases}$$

Ejemplo 4.1.5. Si $k=4$

$$\begin{aligned}P_{2,4}(q)=4(1)\left(1+q+q^2\right)+2(1+q)^2&=4+4q+4q^2+2\left(1+2q+q^2\right)\\&=6+8q+6q^2.\end{aligned}$$

De este modo, comprobamos que la identidad con particiones brinda expresiones complicadas de los polinomios $P_{i,k}$. En particular para los polinomios $P_{2,k}(q)$ con $k\geq 1$, se obtuvo una expresión que depende si k es par ó impar.

Otro aspecto de interés en combinatoria, es evaluar las funciones para responder un problema de conteo en concreto. En particular, vamos a comparar los términos constantes de las identidades 4.1 y 4.6, evaluando en $q=0$.

Observación 3. *La evaluación en* 0*, es un caso particular de " especialización " según lo explica Stanley en [17], Sección 7.8.*

Primero encontramos el término constante del polinomio $P_{i,k}(q)$ expresado por medio de la identidad 4.1.

$$\begin{aligned}P_{i,k}(0)&=\sum_{j=0}^{k-i}\frac{k}{i}\binom{k-1-j}{i-1}\binom{i+j-1}{j}(0)^j\\&=\frac{k}{i}\binom{k-1}{i-1}\binom{i-1}{0}\\P_{i,k}(0)&=\frac{k}{i}\binom{k-1}{i-1}.\end{aligned}\tag{4.10}$$

Nota 7. *En las operaciones realizadas con anterioridad, tomamos a* $0^0=1$.

Luego, evaluamos en $q=0$ el polinomio $P_{i,k}(q)$ dado por la Identidad 4.6

$$P_{i,k}(0)=\frac{k}{i}\sum_{\substack{\lambda\vdash k\\ \ell(\lambda)=i}}\binom{i}{d_1,\cdots,d_k}.\tag{4.11}$$

Igualando ambos términos constantes (expresiones 4.10 y 4.11) se obtiene la siguiente identidad combinatoria

$$\frac{k}{i}\sum_{\substack{\lambda\vdash k\\ \ell(\lambda)=i}}\binom{i}{d_1,\cdots,d_k}=\frac{k}{i}\binom{k-1}{i-1}\Leftrightarrow\sum_{\substack{\lambda\vdash k\\ \ell(\lambda)=i}}\binom{i}{d_1,\cdots,d_k}=\binom{k-1}{i-1}.$$

Proposición 4.1.1 (2024)**.** *Para todo $k \geq 1$ y $1 \leq i \leq k$, se satisface la identidad*

$$\sum_{\substack{\lambda \vdash k \\ \ell(\lambda)=i}} \binom{i}{d_1, \ldots, d_k} = \binom{k-1}{i-1}.$$

La identidad puede ser demostrada por medio de argumentos combinatorios o algebraicos. En nuestro caso optamos por una prueba usando una técnica de conteo clásica en combinatoria.

Demostración. Consideremos que tenemos tableros conformados por ladrillos tales que d_1 son de 1×1, d_2 de 2×1, $\cdots$, d_k de $k \times 1$, con a lo sumo k celdas de tamaño 1×1 y el total de celdas sea i. Se debe contar el total de configuraciones posibles de tableros de altura i, compuestos por ladrillos de diversos tamaños.

- **Conteo 1:** Consideremos las tablas de Young de la forma $\lambda = \langle 1^{d_1} 2^{d_2} 3^{d_3} \cdots k^{d_k} \rangle$ de modo que

$$\begin{aligned} d_1 \text{ de } & 1 \times 1 \\ d_2 \text{ de } & 2 \times 1 \\ d_3 \text{ de } & 3 \times 1 \\ & \vdots \\ d_k \text{ de } & k \times 1. \end{aligned}$$

  Además

$$d_1 + d_2 + \cdots + d_k = \ell(\lambda) = i$$

  donde $\lambda \vdash k$. En total, son i ladrillos que se pueden distribuir en el tablero según su tamaño (ver Figura 4.1). El número de formas es $i!$, como tenemos k tipos de ladrillos. Se obtiene que

$$\frac{i!}{d_1! d_2! \cdots d_k!} = \binom{i}{d_1, d_2, \ldots, d_k}.$$

  Como $\lambda \vdash k$ entonces el total de configuraciones posibles es

$$\sum_{\substack{\lambda \vdash k \\ \ell(\lambda)=i}} \binom{i}{d_1, d_2, \ldots, d_k}.$$

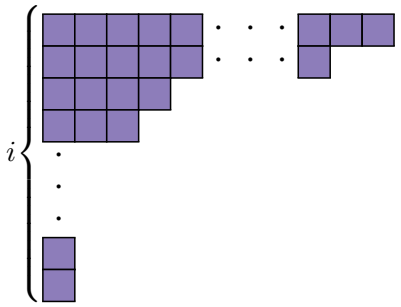


Figura 4.1: Ilustración del conteo 1

- **Conteo 2:** Ahora contemos el número de configuraciones posibles de ladrillos en un tablero de altura i.
  Como el total de celdas de cada ladrillo del tablero es k, nos aseguramos que cada ladrillo tenga al menos una celda, entonces en total son i celdas (ver Figura 4.2). Sabemos que, el número de celdas de cada ladrillo es a lo sumo k, entonces para calcular el número de configuraciones posibles de los ladrillos se contarán la distribución de las celdas restantes como un tablero que tenga a lo sumo $k-1$ celdas.

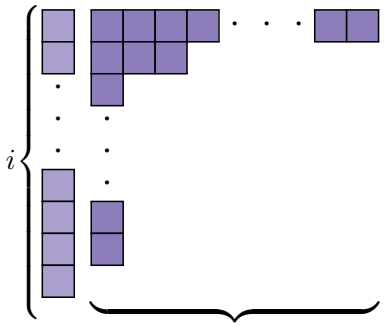


Figura 4.2: Ilustración del conteo 2

En total, son $k-i$ celdas posibles del tablero y por la restricción de que todos los ladrillos deben ser por lo menos de tamaño 1×1, tenemos $i-1$ espacios disponibles. Así, el número de configuraciones posibles del tablero de i ladrillos es

$$\binom{(k-i)+i-1}{i-1} = \binom{k-1}{i-1}.$$

■

4.2. Identidades de Newton

En esta sección, se presentan ejemplos utilizando identidades de Newton y las propiedades de los coeficientes N_k de la función zeta $Z(E/\mathbb{F}_q;T)$ asociada a una curva elíptica $E/\mathbb{F}_q$. Estas identidades de Newton ofrecen una relación entre las funciones simétricas completas, elemental y de potencias, para los lectores interesados en conocer más detalles se recomienda leer [9] y [13].

Proposición 4.2.1. *Para* $k \geq 1$

$$kh_k = \sum_{i=1}^{k} p_i h_{k-i}, \tag{4.12}$$

$$ke_k = \sum_{i=1}^{k} (-1)^{i-1} p_i e_{k-i}. \tag{4.13}$$

Ejemplo 4.2.1. Apliquemos la identidad (4.13) y la sustitución pletística de las funciones simétricas.

- $k = 2$

$$\begin{aligned}
2e_2[1+q-\alpha_1-\alpha_2] &= e_1[1+q-\alpha_1-\alpha_2]p_1[1+q-\alpha_1-\alpha_2] \\
&\quad - e_0[1+q-\alpha_1-\alpha_2]p_2[1+q-\alpha_1-\alpha_2] \\
&= (1+q-\alpha_1-\alpha_2)(1+q-\alpha_1-\alpha_2) - (1+q^2-\alpha_1^2-\alpha_2^2) \\
&= N_1^2 - N_2 \\
&= N_1^2 - \left((2+2q)N_1 - N_1^2\right) \\
2e_2[1+q-\alpha_1-\alpha_2] &= 2N_1^2 - 2(1+q)N_1.
\end{aligned}$$

- $k = 3$

$$\begin{aligned}
3e_3[1+q-\alpha_1-\alpha_2] &= e_2[1+q-\alpha_1-\alpha_2]p_1[1+q-\alpha_1-\alpha_2] \\
&\quad - e_1[1+q-\alpha_1-\alpha_2]p_2[1+q-\alpha_1-\alpha_2] \\
&\quad + e_0[1+q-\alpha_1-\alpha_2]p_3[1+q-\alpha_1-\alpha_2] \\
&= \left(\frac{1}{2}(p_1)^2 - \frac{1}{2}p_2\right) p_1[1+q-\alpha_1-\alpha_2] \\
&\quad - (1+q-\alpha_1-\alpha_2)p_2[1+q-\alpha_1-\alpha_2] + p_3[1+q-\alpha_1-\alpha_2] \\
&= \left(\frac{1}{2}N_1^2 - \frac{1}{2}(1+q^2-\alpha_1^2-\alpha_2^2)\right) N_1 - N_1(1+q^2-\alpha_1^2-\alpha_2^2) \\
&= \left(\frac{1}{2}N_1^2 - \frac{1}{2}N_2\right) N_1 - N_1N_2 + N_3 \\
&= \frac{1}{2}N_1^3 - \frac{1}{2}N_2N_1 - N_1N_2 + N_3
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2}N_1^3 - \frac{1}{2}((2+2q)N_1 - N_1^2)N_1 - N_1((2+2q)N_1 - N_1^2) \\
&+ (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
&= \frac{1}{2}N_1^3 - (1+q)N_1^2 + \frac{1}{2}N_1^3 - (2+2q)N_1^2 + N_1^3 \\
&+ (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
3e_3 &= 3N_1^3 - 6(1+q)N_1^2 + (3+3q+3q^2)N_1.
\end{aligned}$$

Comparando con la función zeta de una curva elíptica

$$kE_k = \sum_{i=1}^{k}(-1)^{i-1}N_iE_{k-i},$$

a partir de $p_k[1+q-\alpha_1-\alpha_2] = 1+q^k-\alpha_1^k-\alpha_2^k = N_k$.

Proposición 4.2.2 (2024)**.** *Para* $k \geq 1$

$$kE_k = \sum_{i=1}^{k}(-1)^{i-1}N_iE_{k-i}.$$

Demostración. Sabemos que $E_k = e_k[1+q-\alpha_1-\alpha_2]$ entonces es equivalente a demostrar la identidad

$$ke_k[1+q-\alpha_1-\alpha_2] = \sum_{i=1}^{k}(-1)^{i-1}N_ie_{k-i}[1+q-\alpha_1-\alpha_2], \text{ para } k \geq 1.$$

Consideremos la función generatriz*

$$E(t) = \prod_{i=1}^{n}(1+x_it) = \sum_{k=1}^{n}e_kt^k.$$

Derivando con respecto a t

$$\frac{d}{dt}E(t) = \sum_{i=1}^{n}x_i\prod_{j\neq i}(1+x_jt).$$

*Para más detalles sobre estas identidades, ver [9], Capítulo I, Sección 2.

Luego, dividimos entre la función generatriz $E(t)$

$$\begin{aligned}\frac{\frac{d}{dt}E(t)}{E(t)} &= \sum_{i=1}^{n} x_i \left(\frac{1}{1+x_i t}\right) \\ &= \sum_{i=1}^{n} x_i \left(\sum_{k=0}^{n} (-1)^k (x_i t)^k\right) \\ &= \sum_{i=1}^{n} x_i \left(\sum_{k=0}^{n} (-1)^k x_i^k t^k\right) \\ &= \sum_{i=1}^{n} \left(\sum_{k=0}^{n} (-1)^k x_i^{k+1} t^k\right) \\ \frac{\frac{d}{dt}E(t)}{E(t)} &= \sum_{k=0}^{n} (-1)^k p_{k+1} t^k.\end{aligned}$$

Por otra parte,

$$\frac{d}{dt}E(t) = \sum_{k=1}^{n} k e_k t^{k-1}. \tag{4.14}$$

Ademas, podemos expresar la derivada con respecto a t de la forma

$$\frac{\frac{d}{dt}E(t)}{E(t)} = \sum_{k=0}^{n} (-1)^k p_{k+1} t^k \Leftrightarrow \frac{d}{dt}E(t) = \left(\sum_{k=0}^{n} (-1)^k p_{k+1} t^k\right) E(t). \tag{4.15}$$

Utilizando 4.14 y 4.15

$$\begin{aligned}\sum_{k=1}^{n} k e_k t^{k-1} &= \left(\sum_{k=0}^{n} (-1)^k p_{k+1} t^k\right) E(t) \\ \sum_{k=1}^{n} e_k t^{k-1} &= \left(\sum_{k=0}^{n} (-1)^k p_{k+1} t^k\right) \left(\sum_{k=1}^{n} e_k t^k\right) \\ \sum_{k=1}^{n} k e_k t^{k-1} &= \sum_{k=0}^{n} \left(\sum_{i=1}^{k+1} (-1)^{i-1} p_i e_{k+1-i}\right) t^k.\end{aligned}$$

Igualando los coeficientes t^{k-1}, se tiene que

$$k e_k = \sum_{i=1}^{k} (-1)^{i-1} p_i e_{k-i}.$$

Aplicando el pletismo, se obtiene la identidad deseada

$$k e_k[1+q-\alpha_1-\alpha_2] = \sum_{i=1}^{k} (-1)^{i-1} e_i[1+q-\alpha_1-\alpha_2] p_{k-i}[1+q-\alpha_1-\alpha_2].$$

Por lo tanto, aplicando que $E_k = e_k[1 + q - \alpha_1 - \alpha_2]$

$$kE_k = \sum_{i=1}^{k} (-1)^{i-1} N_i E_{k-i}.$$

■

De forma similar, podemos analizar el caso de la identidad de Newton con la función simétrica completa

$$kh_k = \sum_{i=1}^{k} p_i h_{k-i}.$$

A continuación se presentan una serie de ejemplos relacionados con esta identidad.

Ejemplo 4.2.2.

- $k = 2$

$$2h_2 = p_1 h_1 + p_2 h_0.$$

- $k = 3$

$$3h_3 = p_1 h_2 + p_2 h_1 + p_3 h_0.$$

En los siguientes ejemplos se incluyen resultados acerca de curvas elípticas y su función zeta asociada.

Ejemplo 4.2.3. Consideremos a $A = \alpha_1 + \alpha_2$ y recordemos la identidad

$$h_{k-1}[\alpha_1 + \alpha_2] = (-1)^{k-1} E_k / N_1 \;\Leftrightarrow\; N_1 h_{k-1}[\alpha_1 + \alpha_2] = (-1)^{k-1} E_k. \tag{4.16}$$

Luego, reescribimos a E_k con ayuda del resultado 4.2.2

$$E_k = \sum_{i=1}^{k} (-1)^{i-1} N_i E_{k-i}$$

Sustituimos la expresión anterior en (4.16)

$$N_1 h_{k-1}[\alpha_1 + \alpha_2] = (-1)^{k-1} \left(\sum_{i=1}^{k} (-1)^{i-1} N_i E_{k-i} \right)$$

$$N_1 h_{k-1}[\alpha_1 + \alpha_2] = \sum_{i=1}^{k} (-1)^{k+i-2} N_i E_{k-i}$$

$$= \sum_{i=1}^{k} (-1)^{k+i-2} \sum_{j=1}^{i} (-1)^{j-1} P_{j,k}(q) N_1^j E_{k-i}, \text{ por el Teorema 3.1.1.}$$

Seguidamente, despejamos $h_{k-1}[\alpha_1+\alpha_2]$.

$$h_{k-1}[\alpha_1+\alpha_2]=\sum_{i=1}^{k}(-1)^{k+i-2}\sum_{j=1}^{i}(-1)^{j-1}P_{j,k}(q)\frac{N_1^j}{N_1}E_{k-i}$$

$$\begin{aligned}h_{k-1}[\alpha_1+\alpha_2]&=\sum_{i=1}^{k}(-1)^{k+i-2}\sum_{j=1}^{i}(-1)^{j-1}P_{j,k}(q)\frac{N_1^j}{N_1}E_{k-i}\\&=\sum_{i=1}^{k}\sum_{j=1}^{i}(-1)^{k+i+j-3}P_{j,k}(q)N_1^{j-1}E_{k-i}\\&=\sum_{i=1}^{k}\sum_{j=1}^{i}\sum_{l=0}^{k-j}(-1)^{k+i+j-3}\frac{k}{j}\binom{k-1-l}{j-1}\binom{j+l-1}{l}q^lN_1^{j-1}E_{k-i},\ \text{por 3.3.3.}\end{aligned}$$

Por lo tanto,

$$h_{k-1}[\alpha_1+\alpha_2]=\sum_{i=1}^{k}\sum_{j=1}^{i}\sum_{l=0}^{k-j}(-1)^{k+i+j-3}\frac{k}{j}\binom{k-1-l}{j-1}\binom{j+l-1}{l}q^lN_1^{j-1}E_{k-i}.$$

Ejemplo 4.2.4.

Utilizando el pletismo y a $A=1+q-\alpha_1-\alpha_2$.

- $k=2$

$$\begin{aligned}2h_2[A]&=p_1h_1+p_2h_0\\&=(1+q-\alpha_1-\alpha_2)h_1[1+q-\alpha_1-\alpha_2]+(1+q^2-\alpha_1^2-\alpha_2^2)\\&=N_1(1+q-\alpha_1-\alpha_2)+N_2\\&=N_1^2+(2+2q)N_1-N_1^2\\2h_2[A]&=(2+2q)N_1.\end{aligned}$$

- $k=3$

$$\begin{aligned}3h_3[A]&=p_1h_2+p_2h_1+p_3h_0\\&=(1+q-\alpha_1-\alpha_2)h_2[1+q-\alpha_1-\alpha_2]\\&+p_2[1+q-\alpha_1-\alpha_2]h_1[1+q-\alpha_1-\alpha_2]\\&+p_3[1+q-\alpha_1-\alpha_2]\\&=N_1\left(\frac{1}{2}N_1^2+\frac{1}{2}N_2\right)+N_2N_1+N_3\\&=\frac{1}{2}N_1^3+\frac{1}{2}N_1((2+2q)N_1-N_1^2)+(2+2q)N_1^2-N_1^3\end{aligned}$$

$$
\begin{aligned}
&\quad + (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
&= \frac{1}{2}N_1^3 + (1+q)N_1^2 - \frac{1}{2}N_1^3 + (2+2q)N_1^2 - N_1^3 \\
&\quad + (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
&= (1+q)N_1^2 + (2+2q)N_1^2 + (3+3q+3q^2)N_1 - (3+3q)N_1^2 \\
3h_3[A] &= (3+3q+3q^2)N_1.
\end{aligned}
$$

Por lo tanto,

$$3h_3[1+q-\alpha_1-\alpha_2] = (3+3q+3q^2)N_1.$$

De los dos casos, se tiene que

$$kh_k[1+q-\alpha_1-\alpha_2] = k(1+q+q^2+\cdots+q^{k-1})N_1.$$

Proposición 4.2.3 (2024)**.** *Para* $k \geq 1$

$$h_k[1+q-\alpha_1-\alpha_2] = (1+q+q^2+\cdots+q^{k-1})N_1.$$

Demostración. Si $k=1$ se verifica que la identidad es cierta, dado que

$$h_1[1+q-\alpha_1-\alpha_2] = p_1[1+q-\alpha_1-\alpha_2] = 1+q-\alpha_1-\alpha_2 = N_1.$$

Entonces consideremos que $k \geq 2$, $A = 1+q$ y $B = \alpha_1+\alpha_2$, aplicamos la identidad del pletismo de funciones simétricas [**]

$$h_k[A-B] = \sum_{i=0}^{k}(-1)^{k-i}h_i[A]e_{k-i}[B],$$

es decir,

$$
\begin{aligned}
h_k[1+q-\alpha_1-\alpha_2] &= \sum_{i=0}^{k} h_i[1+q]e_{k-i}[\alpha_1+\alpha_2] \\
&= (-1)^k h_0[1+q]e_k[\alpha_1+\alpha_2] + \cdots + h_{k-2}[1+q]e_2[\alpha_1+\alpha_2] \\
&\qquad - h_{k-1}[1+q]e_1[\alpha_1+\alpha_2] + h_k[1+q]e_0[\alpha_1+\alpha_2].
\end{aligned}
$$

Como $k \geq 2$ entonces $e_k[\alpha_1+\alpha_2] = 0$, por propiedades de la función simétrica elemental.

$$
\begin{aligned}
h_k[1+q-\alpha_1-\alpha_2] &= h_{k-2}[1+q]e_2[\alpha_1+\alpha_2] - h_{k-1}[1+q]e_1[\alpha_1+\alpha_2] + h_k[1+q]e_0[\alpha_1+\alpha_2] \\
&= (1+q+q^2+\cdots+q^{k-2})q - (1+q+\cdots+q^{k-1})(1+q-N_1) \\
&\quad + (1+q+\cdots+q^k) \\
&= (q+q^2+\cdots+q^{k-1}) - (1+q+\cdots+q^{k-1}) + (1+q+\cdots+q^{k-1})N_1 \\
&\quad - (1+q+\cdots+q^{k-1})q + (1+q+\cdots+q^k), \\
&= (q+q^2+\cdots+q^{k-1}) - (1+q+\cdots+q^{k-1}) + (1+q+\cdots+q^{k-1})N_1 \\
&\quad - (q+q^2+\cdots+q^k) + (1+q+\cdots+q^k).
\end{aligned}
$$

[**] Ver [17], Capítulo 7 para más detalles.

Al realizar las operaciones indicadas, se tiene

$$h_k[1+q-\alpha_1-\alpha_2] = (1+q+\cdots+q^{k-1})N_1.$$

Por lo tanto, se cumple que para $k \geq 1$

$$h_k[1+q-\alpha_1-\alpha_2] = (1+q+\cdots+q^{k-1})N_1.$$

■

De acuerdo con [13], las funciones simétricas h_k para $k \geq 1$ tienen una versión con determinantes que se pueden deducir a partir de las identidades de Newton.

Proposición 4.2.4. *Para $k \geq 1$ se tiene*

$$h_k = \frac{1}{k!}\begin{vmatrix} p_1 & -1 & 0 & 0 & \cdots & 0 \\ p_2 & p_1 & -2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ p_{k-1} & p_{k-2} & p_{k-3} & & & -(k-1) \\ p_k & p_{k-1} & p_{k-2} & \cdots & p_2 & p_1 \end{vmatrix} \text{ y } p_k = \begin{vmatrix} e_1 & 1 & 0 & \cdots & 0 \\ 2e_2 & e_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & 0 \\ & & & & \\ ke_k & e_{k-1} & e_{k-2}\cdots & e_2 & e_1 \end{vmatrix}.$$

Este resultado es una consecuencia de las identidades de Newton, para más detalles de la demostración ver [4].

Relacionado con curvas elípticas, esta identidad se puede utilizar con el pletismo de h_k y $A = 1+q-\alpha_1-\alpha_2$.

Ejemplo 4.2.5. Para $k \geq 1$ y $A = 1+q-\alpha_1-\alpha_2$.

$$h_k[A] = \frac{1}{k!}\begin{vmatrix} N_1 & -1 & 0 & 0 & \cdots & 0 \\ N_2 & N_1 & -2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ N_{k-1} & N_{k-2} & & & & -(k-1) \\ N_k & N_{k-1} & N_{k-2} & \cdots & N_2 & N_1 \end{vmatrix}.$$

A partir de la operación de pletismo entre funciones simétricas encontramos otra forma de expresar a la suma de potencias $\alpha_1^k + \alpha_2^k$, este valor tiene un significado combinatorio y proporciona una descripción para los coeficientes N_k tal como se estudió en el Capítulo 3. Al realizar operaciones de forma adecuada con la función completa h_k, podemos expresar la suma $\alpha_1^k + \alpha_2^k$ en términos de un determinante. Una primera pista de que esta identidad es posible viene del hecho de que podemos escribir a la suma como el pletismo de p_k con $\alpha_1 + \alpha_2$, es decir

$$p_k[\alpha_1+\alpha_2] = \alpha_1^k + \alpha_2^k.$$

Con esta idea en mente, consideremos el siguiente resultado.

Proposición 4.2.5. *Para $k \geq 1$ se cumple que*

$$1+q^k-N_k = \begin{vmatrix} 1+q-N_1 & 1 & 0 & 0 & \cdots & 0 \\ 2q & 1+q-N_1 & 1 & 0 & \cdots & 0 \\ 0 & q & 1+q-N_1 & 1 & & 0 \\ \vdots & \vdots & \ddots & & & \vdots \\ 0 & 0 & 0 & & & 1 \\ 0 & 0 & 0 & \cdots & q & 1+q-N_1 \end{vmatrix}.$$

Demostración. Sea $k \geq 1$ y aplicamos el pletismo de p_k con $\alpha_1+\alpha_2$ donde $\alpha_1\alpha_2 = q$ son conjugados complejos. Por definición, sabemos que

$$p_k[\alpha_1+\alpha_2] = \alpha_1^k + \alpha_2^k = 1+q-N_k. \tag{4.17}$$

Luego, por la Proposición 4.2.4 se tiene

$$p_k[\alpha_1+\alpha_2] = \begin{vmatrix} e_1[\alpha_1+\alpha_2] & 1 & 0 & \cdots & 0 \\ 2e_2[\alpha_1+\alpha_2] & e_1[\alpha_1+\alpha_2] & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & 0 \\ ke_k[\alpha_1+\alpha_2] & e_{k-1}[\alpha_1+\alpha_2] & e_{k-2}[\alpha_1+\alpha_2]\cdots & e_2[\alpha_1+\alpha_2] & e_1[\alpha_1+\alpha_2] \end{vmatrix},$$

$$= \begin{vmatrix} \alpha_1+\alpha_2 & 1 & 0 & \cdots & 0 \\ 2\alpha_1\alpha_2 & \alpha_1+\alpha_2 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & 0 \\ 0 & 0 & 0\cdots & \alpha_1\alpha_2 & \alpha_1+\alpha_2 \end{vmatrix}, \text{ porque } e_i = 0 \text{ para } i > 2,$$

$$p_k[\alpha_1+\alpha_2] = \begin{vmatrix} 1+q-N_1 & 1 & 0 & \cdots & 0 \\ 2q & 1+q-N_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & 0 \\ 0 & 0 & 0\cdots & q & 1+q-N_1 \end{vmatrix}. \tag{4.18}$$

Igualando las expresiones (4.1) y (4.18) encontramos el resultado deseado.

$$1+q^k-N_k = \begin{vmatrix} 1+q-N_1 & 1 & 0 & 0 & \cdots & 0 \\ 2q & 1+q-N_1 & 1 & 0 & \cdots & 0 \\ 0 & q & 1+q-N_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & & & & 1 \\ 0 & 0 & 0 & \cdots & q & 1+q-N_1 \end{vmatrix}, \text{ para todo } k \geq 1.$$

■

Así, hemos encontrado otra forma de expresar a la suma $\alpha_1^k + \alpha_2^k$ con determinantes.

Nota 8. *Existe otra versión de este resultado y es demostrado utilizando propiedades de los polinomios ortogonales (ver [12], Sección 4 y [2] para más detalles sobre polinomios ortogonales).*

Ejemplo 4.2.6. Algunos casos particulares son los siguientes:

1. Si $k = 2$

$$1 + q^2 - N_2 = \begin{vmatrix} 1 + q - N_1 & 1 \\ 2q & 1 + q - N_1 \end{vmatrix}.$$

2. Si $k = 3$

$$1 + q^3 - N_3 = \begin{vmatrix} 1 + q - N_1 & 1 & 0 \\ 2q & 1 + q - N_1 & 1 \\ 0 & q & 1 + q - N_1 \end{vmatrix}.$$

Los coeficientes N_k, también se pueden expresar directamente en forma de determinante, el cual es abordado en el artículo [12], Sección 4.1. Las funciones simétricas estudiadas hasta el momento permiten establecer identidades con curvas elípticas, adicionalmente existen más tipos de funciones simétricas que por medio del pletismo también es posible relacionar con las curvas elípticas.

4.3. Polinomios de Macmahon

A continuación presentamos otro tipo de polinomios simétricos con la finalidad de establecer algunas identidades que conecten datos ya conocidos sobre los coeficientes N_k de la función zeta asociada a una curva elíptica $E/\mathbb{F}_q$.

Definición 4.3.1. *(Polinomios de Macmahon[***]) Sea $1 \leq r \leq k$, definimos el polinomio simétrico*

$$S_{k,r}(x_1, x_2, \ldots, x_n) := \sum_{\substack{\alpha_1+\alpha_2+\cdots+\alpha_r=k \\ 1\leq j_1<j_2<\cdots<j_r}} x_{j_1}^{\alpha_1} x_{j_2}^{\alpha_2} \cdots x_{j_r}^{\alpha_r}.$$

Analizando la definición de esta familia de polinomios, se comprueba que están compuestos por algunos términos de la función completa h_k.

Ejemplo 4.3.1. Algunos ejemplos de polinomios de la familia $\{S_{k,r}\}$ con i variables son los siguientes.

[***]Este tipo de polinomios son ampliamente estudiados por Percy MacMahon en [10].

i \ k	1	2	3
1	$S_{1,1} = x_1$	$S_{2,1} = x_1^2$ $S_{2,2} = 0$	$S_{3,1} = x_1^3$ $S_{3,2} = 0$ $S_{3,3} = 0$
2	$S_{1,1} = x_1 + x_2$	$S_{2,1} = x_1^2 + x_2^2$ $S_{2,2} = x_1x_2$	$S_{3,1} = x_1^3 + x_1^2x_2 + x_2^3$ $S_{3,2} = x_1^2x_2 + x_1x_2^2$ $S_{3,3} = 0$
3	$S_{1,1} = x_1 + x_2 + x_3$	$S_{2,1} = x_1^2 + x_2^2 + x_3^2$ $S_{2,2} = x_1x_2 + x_1x_3 + x_2x_3$	$S_{3,1} = x_1^3 + x_2^3 + x_3^3$ $S_{3,2} = x_1^2x_2 + x_1^2x_3 + x_1x_2^2$ $+x_2^2x_3 + x_1x_3^2 + x_2x_3^2$

Tomando de base los resultados obtenidos en [13], estos polinomios simétricos se pueden escribir en términos de las funciones simétricas elementales, completas y de potencias.

Proposición 4.3.1. *Para* $1 \leq r \leq k$ *se tiene que*

$$S_{k,r} = \sum_{j=r}^{k} (-1)^{j-r} \binom{j}{r} e_j h_{k-j}.$$

La demostración de la proposición realizada en [6], utiliza como herramienta principal las funciones generatrices de la función simétrica completa y elemental.

De acuerdo con la Proposición 4.3.1, resulta natural la conexión entre la función zeta de una curva elíptica con esta nueva definición para la familia de polinomios $\{S_{k,r}\}$.

Ahora veremos ejemplos utilizando resultados ya conocidos acerca de los coeficientes de una función zeta asociada a una curva elíptica E.

Ejemplo 4.3.2. Aplicamos el pletismo de $S_{k,2}$ con $A = 1 + q - \alpha_1 - \alpha_2$ tenemos que por la Proposición 4.3.1 se cumple

$$S_{k,2}[A] = \sum_{j=2}^{k} (-1)^{j-2} \binom{j}{2} e_j[A] h_{k-j}[A].$$

Sabemos que el pletismo de $e_j[A] = E_j$ por definición y por la Proposición 4.2.3, tenemos que $h_{k-j}[A] = (1 + q + q^2 + \cdots + q^{(k-j)-1})N_1$.

Consideremos los siguientes casos particulares cuando variamos k.

- $k = 2$.

$$S_{2,2}[A] = e_2[A]h_0[A] = e_2[A] = q.$$

- $k = 3$

$$\begin{aligned} S_{3,2}[A] &= e_2[A]h_1[A] - 3e_3[A]h_0[A] \\ &= E_2(1+q)N_1 - 3E_3 \\ S_{3,2}[A] &= (1+q)N_1E_2 - 3E_3. \end{aligned}$$

- $k = 4$.

$$\begin{aligned} S_{4,2}[A] &= e_2[A]h_2[A] - 3e_3[A]h_1[A] + 6e_4[A]h_0[A] \\ &= E_2(1+q)N_1 - 3E_3N_1 + 6E_4 \\ S_{4,2}[A] &= (1+q)N_1E_2 - 3N_1E_3 + 6E_4. \end{aligned}$$

Luego, para $k \geq 2$ tenemos la siguiente expresión para el polinomio $S_{k,2}$

$$S_{k,2}[A] = \sum_{j=2}^{k} (-1)^{j-2} \binom{j}{2} (1 + q + q^2 + \cdots + q^{k-j}) N_1 E_{k-j}.$$

Además, podemos reescribir este polinomio de tal forma que quede expresado en términos de q y N_1 utilizando la Proposición 3.3.4. Así, obtenemos la identidad

$$\begin{aligned} S_{k,2}[A] &= \sum_{j=2}^{k} (-1)^{j-2} \binom{j}{2} (1 + q + q^2 + \cdots + q^{k-j}) N_1 \left(\sum_{i=1}^{k-j} \frac{(-1)^{k+i} \cdot i}{k} P_{i,k-j}(q) N_1^i \right) \\ &= \sum_{j=2}^{k} \sum_{i=1}^{k-j} \frac{i}{k} (-1)^{k+i+j-2} \binom{j}{2} (1 + q + q^2 + \cdots + q^{k-j}) P_{i,k-j}(q) N_1^{i+1}. \end{aligned}$$

Por lo tanto,

$$S_{k,2}[A] = \sum_{j=2}^{k} \sum_{i=1}^{k-j} \frac{i \cdot (-1)^{k+i+j-2}}{k} \binom{j}{2} (1 + q + q^2 + \cdots + q^{k-j}) P_{i,k-j}(q) N_1^{i+1}.$$

Ejemplo 4.3.3. En este ejemplo se muestra el pletismo de polinomios de la familia $\{S_{k,2}\}$ y $\alpha_1 + \alpha_2$.

- Si $k = 2$ entonces

$$S_{2,2}[\alpha_1 + \alpha_2] = \alpha_1\alpha_2 = q.$$

- Si $k = 3$ entonces

$$\begin{aligned} S_{3,2}[\alpha_1 + \alpha_2] &= e_2[\alpha_1 + \alpha_2]h_1[\alpha_1 + \alpha_2] - 3e_3[\alpha_1 + \alpha_2]h_0[\alpha_1 + \alpha_2] \\ &= e_2[\alpha_1 + \alpha_2]h_1[\alpha_1 + \alpha_2] \\ &= \alpha_1\alpha_2(\alpha_1 + \alpha_2) \\ &= q(1 + q - N_1) \\ S_{3,2}[\alpha_1 + \alpha_2] &= q + q^2 - qN_1. \end{aligned}$$

- Si $k = 4$ entonces

$$\begin{aligned} S_{4,2}[\alpha_1 + \alpha_2] &= \sum_{j=2}^{4}(-1)^{j-2}\binom{j}{2}e_j[\alpha_1 + \alpha_2]h_{4-j}[\alpha_1 + \alpha_2] \\ &= e_2[\alpha_1 + \alpha_2]h_2[\alpha_1 + \alpha_2], \text{ porque } e_j[\alpha_1 + \alpha_2]h_{4-j}[\alpha_1 + \alpha_2] = 0 \text{ cuando } j > 2 \\ &= q(\alpha_1^2 + \alpha_2^2 + \alpha_1\alpha_2) \\ &= q(1 + q^2 - N_2 + q) \\ &= q(1 + q^2 - (2 + 2q)N_1 + N_1^2 + q) \\ &= q + q^3 - (2q + 2q^2)N_1 + qN_1^2 + q^2 \\ S_{4,2} &= q + q^2 + q^3 - (2q + 2q^2)N_1 + qN_1^2 \end{aligned}$$

En general, si observamos los ejemplos anteriores del pletismo aplicado obtenemos una expresión general para estos polinomios cuando $k \geq 2$ y $r = 2$

$$S_{k,2}[\alpha_1 + \alpha_2] = qh_{k-2}[\alpha_1 + \alpha_2].$$

Notemos que esta expresión se puede reescribir en término de los valores E_k, recurriendo al Lema 3.3.1.

$$\Rightarrow S_{k,2}[\alpha_1 + \alpha_2] = q(-1)^{k-2}E_{k-1}/N_1.$$

Proposición 4.3.2 (2024). *Sea $k \geq 2$ y $r = 2$ entonces el pletismo de $S_{k,2}$ y $\alpha_1 + \alpha_2$ es*

$$S_{k,2}[\alpha_1 + \alpha_2] = q(-1)^{k-2}E_{k-1}/N_1.$$

Demostración. Sea $S_{k,2}$ un polinomio simétrico de Macmahon con $k \geq 2$, se quiere mostrar que el pletismo de $S_{k,2}$ con $\alpha_1 + \alpha_2$ es

$$S_{k,2}[\alpha_1 + \alpha_2] = q(-1)^{k-2}E_{k-1}/N_1.$$

Para la demostración, partimos del lado izquierdo de la igualdad y verificamos cuando $k = 2$.

$$S_{2,2}[\alpha_1 + \alpha_2] = e_2[\alpha_1 + \alpha_2]h_0[\alpha_1 + \alpha_2] = e_2[\alpha_1 + \alpha_2] = q = qE_1/N_1.$$

Ahora se debe demostrar cuando $k > 2$. Partimos del lado izquierdo de la igualdad y aplicamos la Proposición 4.3.1

$$S_{k,2}[\alpha_1 + \alpha_2] = \sum_{j=2}^{k} (-1)^{j-2} \binom{j}{2} e_j[\alpha_1 + \alpha_2] h_{k-j}[\alpha_1 + \alpha_2].$$

Observemos que $e_j = 0$ cuando $j > 2$, por definición de las funciones simétricas elementales. En consecuencia, la expresión anterior es de la forma

$$\begin{aligned} S_{k,2}[\alpha_1 + \alpha_2] &= e_2[\alpha_1 + \alpha_2] h_{k-2}[\alpha_1 + \alpha_2] \\ &= \alpha_1 \alpha_2 h_{k-2}[\alpha_1 + \alpha_2] \\ &= q h_{k-2}[\alpha_1 + \alpha_2] \\ &= q(-1)^{k-2} E_{k-1}. \end{aligned}$$

Por lo tanto,

$$S_{k,2}[\alpha_1 + \alpha_2] = q(-1)^{k-2} E_{k-1}.$$

■

Conclusiones

Con el trabajo realizado se han estudiado propiedades e identidades combinatorias de curvas elípticas sobre campos finitos utilizando la función zeta para curvas.

La función zeta de una curva elíptica $Z(E/\mathbb{F}_q; T)$ brinda información sobre el conteo de puntos en una curva elíptica por medio de sus coeficientes N_k con $k \geq 1$, estos dependen de N_1 y q que a su vez están conformados por una familia de polinomios con coeficientes positivos $\{P_{i,k}\}$, gracias a las interpretaciones combinatorias de los números de Fibonacci y Lucas ($(q,t)-$ analogías de Fibonacci y Lucas abordadas en el Capítulo 3) se obtienen fórmulas e identidades del tipo combinatorio para N_k. Una interpretación importante viene de la sucesión de números de Lucas pares $\{L_{2k} - 2\}$ que enumera los árboles generadores de un grafo de rueda W_k con $k+1$ vértices, esto permite deducir una fórmula explícita para N_k. Cabe destacar que la familia de polinomios $\{P_{i,k}\}$ son objetos interesantes, con ellos se obtiene una descripción para N_k y se deduce una identidad clásica de combinatoria (ver Proposición 4.1.1).

Por otra parte, siguiendo el enfoque de las funciones generatrices con las herramientas de la teoría de funciones simétricas permiten conocer otra forma de definir ciertos aspectos de curvas elípticas nuevamente relacionados con el problema de enumeración. Por ejemplo, con la operación del pletismo de funciones simétricas y la dualidad entre las funciones simétricas completa h_k, elemental e_k y de potencias p_k, encontramos identidades y fórmulas de la enumeración de puntos N_k, estos resultados también muestran la dependencia con q y N_1 (son datos finitos) que a su vez tienen una interpretación combinatoria porque se originan de propiedades de las funciones simétricas como es el caso de las identidades de Newton. Asimismo, al trabajar con otra clase de polinomios simétricos llamados *Polinomios de Macmahon* también se pueden establecer expresiones que dependen de N_k en parte es consecuencia de la definición de estos polinomios puesto que estos quedan determinados por elementos de las funciones simétricas usuales. Para más detalles ver el Capítulo 4, Sección 4.3.

Proyectos a futuro

A pesar que se abordaron diversas propiedades de las curvas elípticas con un enfoque combinatorio, aún quedan pendientes otras temáticas interesantes que surgieron durante la construcción del proyecto.

- El desarrollo de este proyecto de tesis se centró principalmente en las buenas propiedades de las funciones generatrices y estudiamos que existe una conexión con teoría de grafos por lo que se propone estudiar y analizar las posibles aplicaciones o identidades con las curvas elípticas desde un punto de vista de la teoría de grafos.

- Explorar otras interpretaciones de los números de Fibonacci y Lucas para intentar relacionarla con los resultados ya conocidos sobre la enumeración de puntos N_k de curvas elípticas. Un libro que habla acerca de estos temas y que cuenta con muchos ejemplos es: *Fibonacci and Lucas Numbers with Applications* [7].

- Estudiar los polinomios de Chebyshev y su relación con curvas elípticas. Para estudiar con más detalle estos polinomios se recomienda ver el libro [2], Capítulo 2 y el artículo [12], Sección 4.

- Analizar y estudiar aplicaciones de la enumeración de puntos de una curva elíptica a la criptografía. Para profundizar en estos temas se recomienda leer el libro *Elliptic curves: Number Theory and cryptography* [18], Capítulo 4.

Referencias

[1] Alexey Beshenov. *Curso de Álgebra: El Salvador*. 2018. URL: https://cadadr.org/teaching/san-salvador/algebra/2018/salvador-algebra-2018.pdf.

[2] Peter Borwein y Tamás Erdélyi. *Polynomials and polynomial inequalities*. Vol. 161. Springer Science, 2012.

[3] William Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry*. 2008.

[4] Henry W Gould. *The Girard-Waring power sum formulas for symmetric functions and Fibonacci sequences*. 1997. URL: https://www.mscs.dal.ca/FQ/Scanned/37-2/gould.pdf.

[5] R.L. Graham, D.E. Knuth y O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Pearson Education, 1994. ISBN: 9780134389981.

[6] Michael E. Hoffman. "Harmonic-number summation identities, symmetric functions, and multiple zeta values". En: *The Ramanujan Journal* 42.2 (ene. de 2016), págs. 501-526. ISSN: 1572-9303. DOI: 10.1007/s11139-015-9750-4. URL: http://dx.doi.org/10.1007/s11139-015-9750-4.

[7] T. Koshy. *Fibonacci and Lucas Numbers with Applications, Volume 2*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2001. ISBN: 9780471399698.

[8] Matthew Lam. "A Combinatorial Exploration of Elliptic Curves.HMC Senior Theses.91". En: (2015). URL: https://scholarship.claremont.edu/hmc_theses/91.

[9] I.G. Macdonald. *Symmetric Functions and Hall Polynomials*. Oxford classic texts in the physical sciences. Clarendon Press, 1998. ISBN: 9780198504504.

[10] Percy MacMahon. *Combinatory analysis*. Vol. I. Cambridge University Press, 1915.

[11] C. Moreno. *Algebraic curves over finite fields*. 97. Cambridge University Press, 1991.

[12] Gregg Musiker. *Combinatorial Aspects of Elliptic Curves*. 2007. arXiv: 0707.3179 [math.CO].

[13] Cormac O'Sullivan. *Symmetric functions and a natural framework for combinatorial and number theoretic sequences*. 2022. arXiv: 2203.03023 [math.NT]. URL: https://arxiv.org/abs/2203.03023.

[14] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2.ª ed. Springer New York, 2009.

[15] N.J.A. Sloane. *he On-Line Encyclopedia of Integer Sequences*. The OEIS Foundation Inc. 1964. URL: https://oeis.org/A004146/internal.

[16] Richard Stanley. *Enumerative Combinatorics: Volume 1*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1997.

[17] Richard Stanley. *Enumerative Combinatorics: Volumen 2*. Cambridge University Press, 2001.

[18] Lawrence C Washington. *Elliptic curves: Number Theory and cryptography*. CRC press, 2008.