

Universidad de Santiago de Chile

Departamento de matemáticas y ciencias de la
computación

Tesis para optar al título de magister en ciencias con mención en
matemática.



Calculo de ℓ -torsiones para curvas de género $g \leq 3$

Profesor guia: Nicolas Theriault

Cotutor: Roger Oyono

Tesis escrita por:

Fernando Hernan Riveros Pilquinao

Años academicos: 2024/2025

Esta investigación fue posible bajo los proyectos:

24-STIC-04.

También gracias a la financiación de la USaCh mediante diversas becas.

Esta tesis se la dedico a mis amigos y familia ya que son las personas más importantes para mí, por lo tanto cualquier acción la cual implique algo positivo la hago teniéndolos a todos ustedes en mente .

Agradezco a toda la gente de la comunidad matematica que me ha entregado conocimientos, desde mis compañeros de licenciatura, hasta todos mis profesores y ayudantes que me han dado conocimiento relacionado, tangente o independiente de la tesis. Agradezco principalmente a mi profesor guía Nicolas Theriault por hacerme aprender cosas cada vez que nos reuniamos y por mostrarme apoyo indirecta o directamente, difícilmente puedo imaginarme un mejor profesor guía. Tambien agradezco a mi cotutor Roger Oyono por ser buena compañía y por ayudarme a clarificar ciertos conceptos de la tesis. Y por ultimo pero no menor, agradezco a Carolina Villagra por ayudarme burocraticamente cada vez que tenia complicaciones

Índice general

1. Preliminares	5
1.1. Curvas Elípticas	5
1.2. Polinomios de división	7
1.3. Logaritmo discreto	8
1.4. Curvas Hiperelípticas	8
1.5. Representación de Mumford	12
1.6. Endomorfismo de Frobenius	13
1.7. Resultados de álgebra lineal	14
2. Introducción	16
2.1. Algoritmo de Schoof	16
2.2. Descripción del algoritmo	17
2.3. ¿Por qué género $g \leq 3$?	19
2.4. Detalles en género mayor	19
3. Cálculo de ℓ-torsiones.	21
3.1. Hipótesis y restricciones	21
3.2. Deducción del sistema	22
3.3. Intersecciones de $f(x, y) = 0$ con $\mathbb{H}(K)$	23
3.4. Linealización del sistema	25
3.5. Derivadas implícitas respecto a x de y	28
3.6. Modificación del sistema lineal vía representación de Mumford	30
3.7. Ejemplos	34
4. Trabajos futuros y conclusiones	38
4.1. Limitantes inherentes al problema	38
4.2. Problemas por resolver	38
4.2.1. Ecuaciones y variables en el sistema	38
4.2.2. Bases de Groebner	39
4.3. Conclusiones	40

Prefacio

En resumen, este trabajo consiste en extrapolar la idea de los polinomios de división a curvas de género mayor, pero en vez de tratarse de polinomios, se trabaja con sistema de ecuaciones polinomiales. Con extrapolar la idea de los polinomios de división me refiero en concreto a que las soluciones del sistema de ecuaciones polinomiales obtenido den las, ℓ -torsiones de la curva. Este trabajo tiene como finalidad aplicarse computacionalmente, por lo tanto muchos detalles que pueden verse complejos a nivel de calculo, son para simplificar las acciones algorítmicamente.

La relevancia de este resultado es su eventual aplicación para el conteo de puntos de curvas hiperelípticas. El conteo de puntos es un problema interesante en si mismo, pero es útil para obtener curvas de orden primo, lo que tiene como finalidad practica generar esquemas criptograficos seguros.

En esta tesis se asumirán conocimientos básicos de álgebra lineal y álgebra abstracta y otros conceptos revisados en cualquier pregrado de matemáticas, sin embargo sera necesario explicar conceptos básicos para dar ciertas precisiones y para explicar ciertos cálculos engorrosos entre otros motivos.

En este trabajo todas las curvas en cuestión serán afines lo cual podría confundir a lectores más teóricos ya que estas curvas se definen en primera instancia como curvas proyectivas. La razón de tomar curvas afines es para simplificar cálculos a nivel computacional, ya que lo más sencillo es trabajar con la menor cantidad de variables posibles. Sin embargo el enfoque proyectivo no lo descartamos del todo, podría ser más útil para obtener resultados abstractos.

Todas las curvas estarán en su forma de Weierstraß reducida, esto se refiere a que tendrán la forma:

Para género 1:

$$x^3 + ax + b = 0$$

Para género 2:

$$x^5 + ax^3 + bx + cx + d = y^2$$

Para género 3:

$$x^7 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f = y^2$$

Para género arbitrario:

$$h(x) = y^2$$

Cabe destacar que para que lo expresado tenga sentido, el discriminante de estas curvas tiene que ser distinto de 0. La principal razón de tomar curvas de Weierstraß en su forma reducida es que los polinomios de división se encuentran definidos para curvas elípticas en esa forma, en caso de expresar la curva de otra forma es posible definir los polinomios de división pero no de la manera mayormente ocupada dentro del contexto de este trabajo. Otra razón por la cual se toman las curvas en su forma de Weierstraß es por la misma que tomamos curvas afines, los cálculos son más sencillos a nivel computacional, pero en este contexto no se pierde información al hacer esto ya que todas las curvas hiperelípticas pueden ser llevadas a su forma de Weierstraß mediante cambios de variables.

Los cuerpos que se trabajaran serán principalmente cuerpos finitos con $\text{char}(K) \neq 2$ de la forma $\mathbb{F}_p$ con p primo, pero las ℓ -torsiones son buscadas en $\overline{\mathbb{F}}_p$. También es buena idea observar que ocurre en $\mathbb{Q}$ y en $\overline{\mathbb{Q}}$ para ver el procedimiento de forma más clara, pero solo a modo de ejemplo ya que los cálculos relevantes son en $\mathbb{F}_p$.

En contexto de geometría algebraica se le llama grupo de Piccard a lo que en este trabajo se le llama Jacobiana, el cual en el contexto dicho anteriormente es un toro multidimensional. La razón por la cual es posible hacer este cambio de lenguaje es porque $\text{Jac}(\mathbb{H}) \cong \text{Pic}^0(\mathbb{H})$.

Capítulo 1

Preliminares

1.1. Curvas Elípticas

Definición: En un cuerpo K , una curva elíptica es una ecuación en el plano de la forma

$$\{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{P_\infty\}$$

Con los parámetros a y b sujetos a $4a^3 + 27b^2 \neq 0$. Estas curvas poseen una ley de grupo la cual está dada por:

El neutro del grupo es P_∞

El opuesto de (x, y) está dado por

$$(x, y) \oplus (x, -y) = P_\infty$$

Para el resto de los puntos se define la variable λ como

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Y si $(x_1, y_1) = (x_2, y_2)$

$$\lambda = \frac{3x_1^2 + a}{y_1}$$

La ley de grupo se describe de la siguiente forma

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$

Geométricamente esta ley de grupo actua de la siguiente manera; al tener 2 puntos P y Q , se considera la recta que pasa por ambos. Si esta recta no es vertical intersecta en un tercer punto, al trazar una vertical el otro punto que intersecta es $P + Q$.

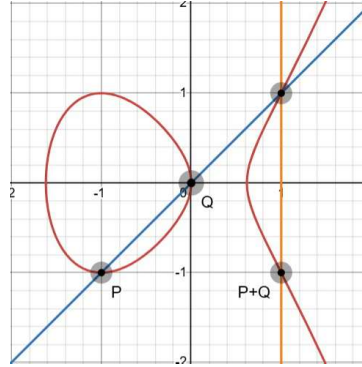


Figura 1.1: visualización geométrica de la suma de P y Q

Observación: Al tratarse de un grupo, siempre es posible tomar la acción de $\mathbb{Z}$ de la siguiente forma $nP = \underbrace{P \oplus P \oplus \dots \oplus P}_{n \text{ veces}}$.

Observación: Al considerar $2P$ geoméricamente lo que se hace es trazar una tangente a $E(K)$ en P para determinar la otra intersección en la curva y luego trazar una vertical en la intersección para determinar el valor de $2P$.

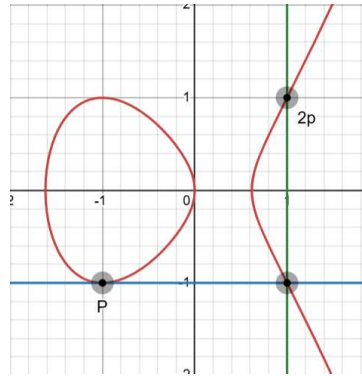


Figura 1.2: visualización geométrica de la obtención de $2P$

Observación: Geométricamente al tomar $-P$ lo que se hace reflejar el punto P en el eje x , a esta acción se dira involucion y se denotara como $\iota(P)$.

Observación: La ley de grupo es esta curva siempre describe un grupo abeliano ya que al considerar la acción geométrica de la ley de grupo, la recta que pasa por P y Q es la misma recta que pasa por Q y P .

Aclaración: Al tener la expresión $P + Q$ con puntos de una curva elíptica se entenderá como $P \oplus Q$

1.2. Polinomios de división

El calculo de las ℓ -torsiones en curvas elípticas es sencillo y viene dado por un polinomio que depende de la curva elíptica en las variables x e y que proveen una manera sencilla de calcular las ℓ torsiones de la curva en cuestión, ya que es posible reducir los polinomios de división a un polinomio solamente en la variable x , y el problema de encontrar las soluciones del polinomio en cuestión se reduce a encontrar los ceros de un polinomio en una variable.

De hecho los polinomios en cuestión resultan tan útiles para el calculo de ℓ -torsiones, que son principalmente lo que se busca extrapolar para el calculo de ℓ -torsiones en curvas hiperelípticas.

Definición: Los polinomios de división son polinomios en $K[a, b, x, y]$ dados por la siguiente recursión

$$\begin{aligned}\psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= 2y \\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\ \psi_4 &= 4y(x^6 + ax^2 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_m - 1\psi_{m+1}^3 \\ \psi_{2m} &= \frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\end{aligned}$$

Observación: Sea $E(K) : x^3 + ax + b = y^2$ a esta curva elíptica es posible tomar los valores de a y b en esta y usarlos para generar polinomios de división, a estos se le llamaran polinomios de división de la curva.

Proposición: Sea $E(K)$ una curva elíptica y $\{\psi_\ell\}_{\ell \in \mathbb{N}}$ sus polinomios de división, entonces los ceros de ψ_ℓ en $E(K)$ son las ℓ -torsiones de la curva.[5]

Proposición: Si n es impar entonces $\psi_n(x, y)$ no depende de y y si n es par $\psi_n(x, y)$ es de la forma $\psi_n(x, y) = yp(x)$ por ello al tomar $y \neq 0$ es posible solo considerar las soluciones en x . Por esto en otras secciones los polinomios de

división se describen como solo dependientes de x [5]

Proposición: Si $E(K)$ es una curva elíptica y $(x, y) \in E(K)$, entonces:

$$\ell \cdot (x, y) = \left(x - \frac{\psi_{\ell-1}(x, y)\psi_{\ell+1}(x, y)}{\psi_{\ell}^2(x, y)}, \frac{\psi_{2\ell}(x, y)}{2\psi_{\ell}^4(x, y)} \right)$$

Con $\{\psi_{\ell}\}_{\ell \in \mathbb{N}}$ los polinomios de división de $E(K)$ [5]

1.3. Logaritmo discreto

El logaritmo discreto es un problema definido en el contexto de que: Sea G un grupo y

$$\alpha, \beta \in G, n \in \mathbb{Z} \text{ tq } n \cdot \alpha = \beta$$

Dado esto el logaritmo discreto es un problema tiene como entrada α y β y tiene a n como incógnita para clarificar la situación daré un ejemplo.

Ejemplo: Sea la curva $E(\mathbb{F}_{1031}) : y^2 = x^3 - x + 1$ y considerar los puntos $(1, 1)$ y $(741, 572)$ en este contexto el problema del logaritmo discreto consiste en encontrar un n tal que

$$n \cdot (-4, 4) = (741, 572)$$

A priori es complejo de determinar, pero ya sabiendo que $n = 11$ es fácil de corroborar la igualdad con cualquier calculadora que opere con curvas elípticas.

La relevancia de este problema viene del hecho de que es una buena instancia para la criptografía debido a que es complejo de resolver, más concretamente se resuelve en tiempo exponencial, pero fácil de corroborar, más precisamente se corrobora en tiempo polinomial.

1.4. Curvas Hiperelípticas

Definición: Una curva hiperelíptica sobre un cuerpo K , $\mathbb{H}(K)$ es una curva en el espacio afín de la forma:

$$\{(x, y) \in K^2 \text{ tq } h(x) = y^2\} \cup \{P_{\infty}\}$$

Con $h(x)$ un polinomio libre de cuadrados de grado impar.

Definición: El género de una curva hiperelíptica $H(K) : h(x) = y^2$ es la magnitud dada por $g = \frac{\deg(h)-1}{2}$.

Las curvas Hiperelípticas generalizan las curvas elípticas, ya que una curva elíptica es una curva hiperelíptica de género 1, porque para cualquier polinomio

de grado 3 es posible hacer un cambio de variable y expresar la curva de manera efectiva de la forma $x^3 + ax + b = y^2$.

La ley de grupo en una curva hiperelíptica se define de una manera más compleja mediante su jacobiana. Para poder definir la jacobiana de una curva hiperelíptica, es necesario definir conceptos previos.

Definición: El grupo de divisores de una curva hiperelíptica $\mathbb{H}(K)$, denotados $(Div(\mathbb{H}(K)))$, es el grupo formado por la sumas formales finitas de puntos de la curva. Para ilustrar mejor la definición un divisor arbitrario posee la forma:

$$D = \sum_{k=1}^M n_k P_k, \quad n_k \in \mathbb{Z}, P_k \in \mathbb{H}(K) \cup \{P_\infty\}$$

Otra manera de definir este grupo es el grupo libre abeliano generado por los puntos de la curva $\mathbb{H}(K)$.

Definición: El grupo de los divisores de grado 0 $Div^0(\mathbb{H})$ es el conjunto de todos los divisores D tales que

$$D = \sum_{k=1}^M n_k P_k, \quad n_k \in \mathbb{Z}, P_k \in \mathbb{H}(K)$$

Que cumplen con

$$\sum_{k=1}^M n_k = 0$$

Definición: El anillo de funciones de una curva hiperelíptica $\mathbb{H}(K) : h(x) = y^2$ es el anillo constituido por $\frac{K[x,y]}{h(x)-y^2}$.

Observación*(1): Para fines prácticos los elementos del anillo de funciones pueden ser vistos a partir de sus representantes en $K[x,y]$ por el hecho de que comparten los mismos ceros en $\mathbb{H}(K)$.

Definición: El cuerpo de funciones el cuerpo dado por $frac(\frac{K[x,y]}{h(x)-y^2})$ con $frac$ refiriéndose al cuerpo de fracciones.

Definición: Al considerar una función f en el cuerpo de funciones racionales de una curva $\mathbb{H}(K)$ es posible construir un divisor de la siguiente manera :

$$\langle f \rangle = \sum_{k=1}^M n_{P_k} (P_k - P_\infty)$$

Donde P_k es un cero o polo de la función racional f y n_{P_k} es el orden del cero o del polo en cuestión, en caso de ser un cero n_{P_k} es positivo, en caso de ser un

polo n_{P_k} es negativo. Los divisores de esta forma son llamados divisores principales ($Prin(\mathbb{H}(K))$), y estos cumplen la identidad $\langle f \rangle + \langle g \rangle = \langle fg \rangle$. Por lo tanto al cumplirse que la suma de 2 divisores principales sigue siendo un divisor principal es posible concluir que los divisores principales son un subgrupo de los divisores de grado 0.

Definición: Como los divisores de una curva son un grupo abeliano, lo que implica que los divisores principales son un subgrupo normal, por ello es posible tomar el grupo:

$$Jac(\mathbb{H}(K)) = \frac{Div^0(\mathbb{H}(K))}{Princ(\mathbb{H}(K))}$$

El cual se entiende como la Jacobiana de la curva $\mathbb{H}(K)$.

La ley de grupo en una curva Hiperelíptica $\mathbb{H}(K)$ se entiende como la operación de grupo existente en $Jac(\mathbb{H}(K))$.

Definición: Sea $D = \sum_{i \in I} n_{P_i}(P_i - P_\infty)$ en $Jac(\mathbb{H}(K))$ se considera el soporte de $Supp(D)$ como $\{P_i\}_{i \in I}$

Definición: Sea $D = \sum_{i \in I} n_{P_i}(P_i - P_\infty)$ en $Jac(\mathbb{H}(K))$ se considera el peso de D como $\sum_{i \in I} n_{P_i}$

Definición: Tal cual como ocurre en curvas elípticas es posible considerar el morfismo $\iota(x, y) = (x, -y)$ y es posible extender la acción de este morfismo a todo $Jac(\mathbb{H}(K))$ considerando

$$\iota\left(\sum_{i \in I} n_i P_i\right) = \sum_{i \in I} n_i \iota(P_i)$$

Observación: Notar que el opuesto del punto $Q - P_\infty = (x_0, y_0) - P_\infty$ en $Jac(\mathbb{H}(K))$ es $\iota(Q) - P_\infty$ porque al considerar la recta que pasa por P y Q la función $x - x_0$ se puede ver que sus ceros en $\mathbb{H}(K)$ son Q y $\iota(Q)$, por ende se ve que.

$$Q + \iota(Q) - 2P_\infty = 0$$

$$-(Q - P_\infty) = \iota(Q) - P_\infty$$

Observación: Ya que se tiene una manera explícita de calcular $-(P - P_\infty)$ para cualquier $P \in \mathbb{H}(K)$, es posible expresar cualquier divisor en $Jac(\mathbb{H}(K))$ de la siguiente forma

$$\langle f \rangle = \sum_{k=1}^M n_{P_k}(P_k - P_\infty)$$

Con $0 < n_{P_k}$

Observación: Dado Un divisor principal es posible relacionarlo a un elemento del anillo de funciones en vez del cuerpo de funciones racionales, porque

dada la observación anterior, es posible ignorar funciones que posean polos en el cuerpo de funciones racionales, que es lo mismo que considerar solo el anillo de funciones.

Observación: Para curvas elípticas se cumple que $E(K) \cong \text{Jac}(E(K))$ con el isomorfismo

$$P \mapsto P - P_\infty$$

. Al tomar 2 puntos P_1 y P_2 en $\text{Jac}(E(K))$ la recta que pasa por ellos es una función racional por lo tanto para los 3 puntos P_1, P_2 y P_3 que pasan por aquella recta se cumple que $P_1 + P_2 + P_3 - 3P_\infty$ es un divisor principal. y al considerar la igualdad

$$P_1 + P_2 - 2P_\infty = -(P_3 - P_\infty)$$

Y por la observación anterior y viendo la acción geométrica de la ley de grupo en $E(K)$ es posible concluir el isomorfismo inicialmente mencionado.

Proposición: Si $\mathbb{H}(\overline{K})$ es una curva de género g en un cuerpo algebraicamente cerrado $\overline{K}$ entonces cualquier divisor en $\text{Jac}(\mathbb{H}(\overline{K}))$ de peso $g < w$ es posible reducirlo a un divisor de peso a lo más g .

Demostración: Se procederá a demostrar por inducción, primero se probara que un divisor de peso $g + 1$ se puede reducir a uno de peso $w \leq g$.

Al tener un divisor $D = \sum_{i \in I} n_{P_i} P_i$ de peso $w = g + 1$, se puede considerar una interpolación que pase por todos los puntos de D tomando en cuenta su multiplicidad, de la forma $y = p(x)$ con $p(x)$ un polinomio de grado $\deg \leq g$. Al calcular la intersección de esta interpolación con la curva se ve que los puntos en la intersección cumplen que $h(x) - p^2(x) = 0$ con $\deg(h(x) - p^2(x)) \leq 2g + 1$ por ello se tiene que $\langle h(x) - p^2(x) \rangle = D + C$ con C un divisor de peso $w \leq g$. Por lo anterior $D + C$ es un divisor principal, y esto permite hacer la reducción $D = -C$ lo que convierte a D en un divisor de peso $w = g$, comprobando el caso base.

Al suponer que un arbitrario divisor de peso $w = g + n$ se puede reducir a un divisor de peso $w \leq g$, se tiene que al asumir el peso del divisor reducido como $w < g$ Claramente es posible reducir un divisor arbitrario de peso $w = g + n + 1$ a un divisor de peso $w \leq g$. En caso de tener que el peso del divisor reducido es $w = g$ se puede ver que un divisor arbitrario de peso $w = g + n + 1$ se puede reducir un divisor de peso $g + 1$ y por lo dicho en el párrafo anterior, este divisor se puede reducir nuevamente a un divisor de peso $w \leq g$ comprobando la hipótesis de inducción.

1.5. Representación de Mumford

La representación de Mumford es una forma idónea de expresar un divisor reducido de la Jacobiana de una curva hiperelíptica.

Definición: En una curva hiperelíptica de género g $\mathbb{H}(\overline{K}) : h(x) = y^2$, la representación de Mumford de un divisor [7]

$$D = \sum_{k=1}^q n_{P_k} (P_k - P_\infty)$$

Con

$$P_k = (x_k, y_k)$$

Es un ideal

$$I = \langle u(x), y - v(x) \rangle$$

Tal que x_k es un cero de orden n_{P_k} de $u(x)$ y también se satisface la expresión $y_k - v(x_k) = 0$ (tomando en cuenta multiplicidad).

Con:

$u(x)$ monico.

$$\deg(v(x)) < \deg(u(x)) \leq g.$$

$$u(x) | h(x) - v(x)^2.$$

Proposición: Cada divisor en $J(\mathbb{H}(\overline{K}))$ posee una única representación de Mumford, donde $u(x)$ y $v(x)$ son de grado minimal.

Demostración: Primero considerar un divisor arbitrario

$$D = \sum_{i \in I} n_{P_i} (P_i - P_\infty)$$

Como se vio anteriormente es posible reducir cualquier divisor en $J(H(K))$ a un divisor de peso $w \leq g$, de la forma:

$$C = \sum_{i \in I'} n_{P'_i} (P'_i - P_\infty)$$

Escribiendo $P'_i = (x_i, y_i)$ es posible definir el polinomio

$$u(x) = \prod_{i \in I} (x - x_i)^{n_{P'_i}}$$

Notar que $u(x)$ es monico, que $\deg(u(x))$ es el peso de C' y que por su construcción es único.

Luego al interpolar todos los puntos $P'_i = (x_i, y_i)$ con una función $y = v(x)$ la cantidad de puntos interpolados para generar esta función son $\#I$ y por esto $\deg(v(x)) = \#I - 1$ lo que implica que $\deg(v(x)) < \deg(u(x)) \leq g$.

Para corroborar la ultima condición es útil tomar la representación de Mumford $I = \langle u(x), y - v(x) \rangle$, por todo lo anterior

$$h(x) - y^2 \equiv 0 \pmod{I}$$

$$h(x) - v^2(x) \equiv 0 \pmod{I}$$

Y esto indica que

$$h(x) - v^2(x) \equiv 0 \pmod{\langle u(x) \rangle}$$

Que es lo mismo que expresar

$$u(x) | h(x) - v^2(x)$$

□

Proposición: Se puede tener un isomorfismo $J(H(K)) \cong Cl(RF(\mathbb{H}(K)))$ mediante asociar un divisor a su representación de Mumford.[8]

1.6. Endomorfismo de Frobenius

Retomando un poco conceptos básicos de la teoría de cuerpos finitos; sea K un cuerpo de característica p , el automorfismo de Frobenius es el isomorfismo definido por

$$\varphi : K \rightarrow K$$

$$x \mapsto x^p$$

Este fija todos los elementos del subcuerpo de K isomorfo a $\mathbb{F}_p$. Para fines de este trabajo el morfismo de Frobenius se definirá de la siguiente forma; sea $\mathbb{F}_q$ un cuerpo finito y sea $\overline{\mathbb{F}_q}$ su clausura, entonces el morfismo de Frobenius de $\mathbb{F}_q$ es el morfismo definido por:

$$\varphi_q : \overline{\mathbb{F}_q} \rightarrow \overline{\mathbb{F}_q}$$

$$x \mapsto x^q$$

Este automorfismo tiene la particularidad de que fija todos los elementos de $\mathbb{F}_q$.

Es posible extender la acción del Frobenius a los puntos de una curva hiperelíptica $\mathbb{H}(\mathbb{F}_q)$ de la siguiente forma:

$$\varphi_q(x, y) = (\varphi_q(x), \varphi_q(y)) = (x^q, y^q)$$

Sea $\mathcal{A}(\mathbb{H}(\overline{\mathbb{F}}_q))$ el conjunto de todos los endomorfismos de $\mathbb{H}(\overline{\mathbb{F}}_q)$, este conjunto tiene una estructura de álgebra, dada por $(\mathcal{A}(\mathbb{H}(\overline{\mathbb{F}}_q)), +, \circ)$. En esta álgebra cada endomorfismo θ tiene un polinomio característico $p_\theta(\theta) = 0$. Para el conteo de puntos resulta muy importante el polinomio $p_\varphi(x)$, el polinomio característico del Frobenius.

Teorema(Hasse Weil): Sea $\mathbb{H}(\overline{\mathbb{F}}_q)$ una curva hiperelíptica de género g , entonces el polinomio característico del Frobenius $\phi_{\varphi_q}(x)$ es de grado $2g$. Y sus raíces ρ_i vienen en pares $\rho_i \rho_{i+1} = q$ y $|\rho_i| = \sqrt{q}$. [7]

1.7. Resultados de álgebra lineal

Para el método de calculo de ℓ -torsiones obtenido, es necesario determinar si una matriz rectangular posee rango incompleto, por ello no esta de más un repaso de conceptos relacionados al rango de matrices rectangulares .

En toda esta sección se asumirá $n < m$ para matrices rectangulares $m \times n$ la razón de esto es que todos los resultados son análogos para el caso $m < n$.

Definición: Sea M una matriz rectangular $m \times n$. Una submatriz N de M , es una matriz cuadrada $n \times n$ formada por filas o columnas de M .

Proposición: Una matriz posee rango completo si y solo alguna de las submatrices posee rango completo.

Demostración:($\leftarrow$):Sea N una submatriz de M , con N de rango completo. Es posible afirmar que

$$\text{rank}(N) \leq \text{rank}(M) \leq n.$$

Con m el rango máximo para M , por el hecho de que N es de rango completo $\text{rank}(N) = n$, y por lo tanto $\text{Rank}(M) = n$, y esto concluye con que M es de rango completo.

($\rightarrow$): Tomando en cuenta que es posible entender el rango de una matriz M como la cantidad máxima de filas o columnas las cuales son linealmente independientes, entonces al considerar la submatriz N de rango completo, es decir con la mayor cantidad de filas o columnas linealmente independientes se tendra:

$$\text{rank}(N) = \text{rank}(M)$$

□

Por ello si M tiene rango completo, también lo tiene N .
Pero lo realmente relevante para este trabajo es el contrareciproco de la proposición anteriormente descrita.

Proposición(Contra recíproco): Una matriz M no posee rango completo si y solo si todas sus submatrices son no invertibles.

Otra manera de expresar esta idea es que una matriz M no posee rango completo si y solo si el determinante de todas las submatrices es 0.

Capítulo 2

Introducción

Entre muchas de las razones que vuelven el conteo de puntos algo importante se encuentra el hecho de que permite crear buenas instancias para el logaritmo discreto. Para que un grupo en general sea buena instancia para el logaritmo discreto tiene que cumplir 3 características, que la ley de grupo sea lo suficientemente compleja como es el caso de curvas hiperelípticas pero a su vez que sea sencilla de calcular y también, el orden del grupo tiene que ser lo menos factorizable posible, idealmente de orden primo. Por ello para poder encontrar grupos de orden primo, se toman muchas curvas aleatorias y se cuentan sus puntos, hasta poder encontrar una curva de orden primo.

Por esto algoritmos de conteo como el de Schoof cobran mucha relevancia, ya que poseen buenos tiempos en lo que respecta a esta materia. La relevancia del algoritmo de Schoof es a tal punto de que muchos otros métodos en género mayor consisten extrapolar técnicas ocupadas para este algoritmo; el problema de esto es que para género mayor no existe un método tan sencillo para determinar las ℓ -torsiones de una curva elíptica como lo son los polinomios de división; Esta es la principal motivación de este trabajo.

2.1. Algoritmo de Schoof

El algoritmo de Schoof es un metodo de conteo de puntos en curvas elípticas sobre cuerpos finitos $\mathbb{F}_q$. Este metodo sirvio de base a otros metodos de conteo de puntos como el algoritmo de Pila o el algoritmo de Gaudry Shoost. Sirve igualmente como motivacion para este proyecto, porque el algoritmo de Schoof descansa en la idea de que las ℓ -torsiones son sencillas de calcular, porque estas vienen dadas por los ceros de los polinomios de division, algo no muy complejo de calcular. Entonces esta tesis tiene como finalidad extrapolar de la mejor manera posible la idea de los polinomios de división, para poder extrapolar las tecnicas ocupadas en el algoritmo de Schoof.

Para empezar a hablar de mejor manera sobre el algoritmo de Schoof primero

es útil enunciar ciertos resultados.

Teorema: Sea $\mathbb{H}(\mathbb{F}_q)$ y $\phi(x)$ el polinomio característico del Frobenius de la curva en cuestión, entonces se cumple que $\#\mathbb{H}(\mathbb{F}_q) = \phi(1)$. [7]

Y en el caso específico de curvas elípticas se tiene el siguiente resultado:

Proposición: Sea $\phi_{\varphi_q}(x)$ el polinomio característico del Frobenius de una curva elíptica $E(\mathbb{F}_q)$ entonces $\phi(x) = x^2 - \tau x + q$.

Demostración: Es consecuencia directa de Hasse y Weil ya que $\phi_{\varphi_q}(x)$ es un polinomio de grado 2 de la forma

$$\phi_{\varphi_q}(x) = (x - \rho_1)(x - \rho_2) = x^2 - (\rho_1 + \rho_2)x + \rho_1\rho_2$$

Pero por teorema de Hasse Weil, y tomando $\tau = \rho_1 + \rho_2$

$$\phi_{\varphi_q}(x) = (x - \rho_1)(x - \rho_2) = x^2 - \tau x + q$$

Dado el polinomio anteriormente mencionado, notar que τ es la única variable desconocida, por ello determinar τ determina todo $\#E(K)$ ya que $\#E(K) = 1 - \tau + q$. Por esto el algoritmo de Schoof se centra únicamente en calcular τ

Para determinar efectivamente τ se tiene una cota la cual esta dada por el teorema de Hasse Weil.

Observación: Al factorizar el polinomio minimal del Frobenius $\phi(x) = (x - \rho_1)(x - \rho_2)$ se puede ver que $\tau = \rho_1 + \rho_2$ y por el teorema de Hasse Weil $|\tau| = |\rho_1 + \rho_2| \leq 2\sqrt{q}$.

Para determinar efectivamente el valor de τ este se determina (mód ℓ_i) con $\{\ell_i\}_{i \in I}$ una sucesión de números primos tales que $\prod_{i \in I} \ell_i < 2\sqrt{q}$ y por teorema chino de los restos, poder determinar el valor de τ en $\mathbb{Z}$.

2.2. Descripción del algoritmo

Paso 1: Seleccionar primos $\{\ell_i\}_{i \in I}$ en orden creciente hasta que se cumpla la desigualdad

$$2\sqrt{q} < \prod_{i \in I} \ell_i$$

Paso 2: Elegir un primo en $\{\ell_i\}_{i \in I}$, luego tomar un valor x_i tal que $\psi_{\ell_i}(x_i) = 0$, luego determinar un valor y_{ℓ_i} tal que $(x_{\ell_i}, y_{\ell_i}) \in E(\mathbb{F}_q)$, este punto servirá como generador de $E(\mathbb{F}_q)[\ell]$.

Paso 3: Calcular la acción del Frobenius en este punto, es decir

$$\varphi(x_{\ell_i}, y_{\ell_i}) = (x_{\ell_i}^q, y_{\ell_i}^q)$$

Luego calcular

$$\varphi^2(x_{\ell_i}, y_{\ell_i}) = (x_{\ell_i}^{q^2}, y_{\ell_i}^{q^2})$$

Y también calcular

$$q(x_{\ell_i}, y_{\ell_i}) = (x_{\ell_i}^q, y_{\ell_i}^q)$$

Observación: Tomar en cuenta que

$$\varphi^2(x_{\ell_i}, y_{\ell_i}) - t\varphi(x_{\ell_i}, y_{\ell_i}) + q(x_{\ell_i}, y_{\ell_i}) = 0$$

en $E(K)[\ell]$, por lo tanto es correcto decir que

$$\varphi^2(x_{\ell_i}, y_{\ell_i}) - \tau\varphi(x_{\ell_i}, y_{\ell_i}) + q(x_{\ell_i}, y_{\ell_i}) \equiv 0 \pmod{\ell}$$

lo que desemboca en la expresión

$$\tau\varphi(x_{\ell_i}, y_{\ell_i}) \equiv \varphi^2(x_{\ell_i}, y_{\ell_i}) + q(x_{\ell_i}, y_{\ell_i}) \pmod{\ell}$$

Paso 4: Elegir valores valores t y corroborar la igualdad

$$t\varphi(x_{\ell_i}, y_{\ell_i}) \equiv \varphi^2(x_{\ell_i}, y_{\ell_i}) + q(x_{\ell_i}, y_{\ell_i}) \pmod{\ell}$$

Tomar todos los valores de t que corroboren la igualdad. Estos valores cumplirán que

$$t \equiv \tau \pmod{\ell}$$

Paso 5: Repetir este procedimiento para todos los ℓ seleccionados, ya que esto permite conocer $\tau \pmod{\ell}$ para todos los ℓ seleccionados.

Paso 6: Obtener el valor efectivo de τ mediante los valores de $\tau \pmod{\ell}$ ocupando el teorema de restos chino. Esto es posible porque se eligieron los primos $\{\ell_i\}_{i \in I}$ de tal manera que:

$$\tau \leq 2\sqrt{q} < \prod_{i \in I} \ell_i$$

2.3. ¿Por qué género $g \leq 3$?

A priori la técnica desarrollada sirve para género arbitrario, el problema es su eficiencia, por ello antes de pensar en $3 < g$ primero hay que realizar suficiente experimentación y refinar el método en $g=3$.

La razón principal por la cual $g = 3$ es de interés, es porque en género 2 ya existen resultados de calculo de ℓ torsiones en general, y en género 1 existen muchísimos más. Para género $2 < g$ no existe virtualmente ningún resultado

La razón principal por la cual se consideran géneros menores es porque en esos géneros es mucho más fácil realizar los procedimientos hechos en este trabajo, tanto conceptualmente como mecánicamente. En género 1 todo se comprueba mucho más fácil mecánicamente por ejemplo, pero se pierde mucha información conceptual, por ejemplo la representación de Mumford en género 1, no entrega ninguna información ya que el divisor (x_0, y_0) tiene como representación de Mumford $\langle x - x_0, y - y_0 \rangle$, lo cual es muy sencillo, pero por ejemplo, en género 2 la representación de Mumford de un divisor da una estructura mucho más rica y fructífera para obtener información.

2.4. Detalles en género mayor

Para poder extrapolar el algoritmo de Schoof, es necesario observar las diferencias y semejanzas de las curvas de género $g = 1$ (Elípticas) con las curvas de género $g > 1$, por ejemplo la "dimensión" del espacio de divisores, cantidad de divisores de ℓ -torsión.

No esta de más decir que el primer contraste es que en curvas elípticas .

Teorema: Sea $\mathbb{F}_q$ un cuerpo finito, sea $\overline{\mathbb{F}_q}$ su clausura, y sea $\mathbb{H}(\overline{\mathbb{F}_q})$ una curva hiperelíptica sobre $\overline{\mathbb{F}_q}$ de género g , entonces:

$$Jac(\mathbb{H}(\overline{\mathbb{F}_q}))[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

Y por esto trivialmente $|Div(\mathbb{H}(\overline{\mathbb{F}_q}))[\ell]| = \ell^{2g} \cdot [9]$

Corolario: Sea $\overline{\mathbb{F}_l}$ la clausura algebraica de un cuerpo finito, y sea $\mathbb{H}(\overline{\mathbb{F}_q})$ una curva hiperelíptica sobre $\overline{\mathbb{F}_q}$ de género arbitrario, entonces al considerar el conjunto definido por:

$$Supp(Div[\ell]) = \{P \in \mathbb{H}(\overline{\mathbb{F}_q}) \text{ tq } P \in Supp(D) \text{ con } D \in Jac(\mathbb{H}(\overline{\mathbb{F}_q}))[\ell]\}$$

Tiene dimensión 0 (como variedad algebraica). [12]

Para simplificar la lectura no esta de más aclarar que este es el conjunto de todos los puntos que se encuentran en el soporte de los divisores de ℓ -torsión. El corolario en cuestión se prueba directamente a partir del hecho de que

$Div_\ell(\mathbb{H}(\overline{\mathbb{F}}_q))$ es finito.

Observación: Primero, es trivial que $P_\infty \in Jac(\mathbb{H}(\overline{\mathbb{F}}_q))[\ell]$. Por lo tanto el método en cuestión puede enfocarse en los $\ell^{2g} - 1$ Divisores restantes. Tomando en cuenta que los divisores de ℓ -Torsión conforman un grupo abeliano, se puede deducir que son estables bajo el automorfismo de inversión ι . También notar que al obtener un divisor D se puede obtener rápidamente $\iota(D)$, por ello un método que obtenga $\frac{Jac(\mathbb{H}(\overline{\mathbb{F}}_q))[\ell] - \{P_\infty\}}{\iota}$ (El conjunto mencionado anteriormente cocientado por la acción de ι) es suficiente. Como ι es una involución y actúa no trivialmente en $Div(\mathbb{H}(\overline{\mathbb{F}}_q))[\ell] - \{P_\infty\}$ es posible deducir que

$$|\frac{Jac(\mathbb{H}(\overline{\mathbb{F}}_q))[\ell] - \{P_\infty\}}{\iota}| = \frac{\ell^{2g} - 1}{2}$$

Cuando ℓ es impar. En el caso de que ℓ sea par ι fija las 2 torsiones, y estas están determinadas por los ceros de $h(x)$, y como $h(x)$ no tiene raíces repetidas, para el caso par la situación se describe así:

$$|\frac{Jac(\mathbb{H}(\overline{\mathbb{F}}_q))[\ell] - \{P_\infty\}}{\iota}| = \frac{\ell^{2g} - 1 - (2g + 1)}{2}$$

Cuando ℓ es par.

Observación: En los polinomios de división es posible ejemplificar esto, ya que $deg(\psi_\ell(x)) = \frac{\ell^2 - 1}{2}$ esto se debe principalmente a que P_∞ no es interpretado como solución de $\psi_\ell(x)$ y también $\psi_\ell(x)$ solo toma soluciones en x y como los valores de x son iguales para P y $\iota(P)$ el polinomio de división contempla como solución solamente a uno de ellos

Capítulo 3

Cálculo de ℓ -torsiones.

Esta sección tiene como finalidad describir en detalle el resultado obtenido. Este procedimiento lo que pretende es que al tener una curva hiperelíptica sobre un cuerpo $\mathbb{H}(K)$, obtener un generador de los divisores de ℓ -torsiones para luego obtener el grupo completo de ℓ -torsiones.

A grandes rasgos el método para encontrar las ℓ -torsiones descansa en la idea de que un divisor sea de ℓ -torsión es equivalente a que ciertas funciones relacionadas al divisor en cuestión cumplan ciertas condiciones, estas condiciones entregan un sistema que a priori es no lineal. Para poder verificar de manera sencilla que el sistema descrito anteriormente cumple con los requisitos mencionados, se procede a traducirlos a que una cierta matriz no tenga rango completo, lo que decanta en otro sistema no lineal, pero más sencillo que el anterior.

3.1. Hipótesis y restricciones

Para todos los cuerpos K en cuestión se asumirán algebraicamente cerrados de la forma $\overline{\mathbb{F}_p}$, e característica $2g + 1 < \text{char}(K)$, idealmente $\text{char}(K)$ lo más grande posible. No esta de más decir que la mayoría de los resultados descritos son para cuerpos algebraicamente cerrados de cualquier tipo.

Las curvas en cuestión serán hiperelípticas $\mathbb{H}(K) : h(x) = y^2$ de género g , y $h(x)$ un polinomio fijo pero arbitrario en $K[x]$.

Los divisores por calcular estas sujetos a ciertas restricciones, estas son:

- D es de peso g .
- D no tiene puntos repetidos.
- D el soporte de D no contiene ningún punto de la forma $(x, 0)$.

$\frac{d}{dx}$ es el operador de derivada formal e implícita sobre x es decir, actúa con las mismas reglas de las derivadas en polinomios, y $\frac{d^n}{d^n x} y = y^{(n)}$ para n arbitrario es una expresión implícita; que un principio es interpretada como una variable extra en el sistema y que luego es simplificada.

Los conjunto de variables que se operan a lo largo de las secciones son:

$$\begin{aligned}\Gamma &:= \{a_0, a_1, \dots, b_0, b_1, \dots, x, y\} \\ \Gamma'_0 &:= \Gamma \cup \{y^{(n)}\}_{1 \leq n \leq \ell} \\ \Gamma'_1 &:= \{x, y, y', \dots, y^{(\ell)}\} \\ \Gamma'_2 &= (x, y) \cup \{h_n\}_{0 \leq n \leq g} \\ \Lambda_0 &= \{u_n\}_{1 \leq n \leq g} \cup \{v_n\}_{1 \leq n \leq g-1} \cup \Gamma'_0 \\ \Lambda_1 &= \{u_n\}_{0 \leq n \leq g-1} \cup \{v_n\}_{0 \leq n \leq g-1} \cup \{h_n\}_{0 \leq n \leq 2g-1} \\ \Lambda_2 &= \{u_n\}_{0 \leq n \leq g-1} \cup \{v_n\}_{1 \leq n \leq g-1}\end{aligned}$$

3.2. Deducción del sistema

Sea $\mathbb{H}$ una curva hiperelíptica y sea $Jac(\mathbb{H}(K))$ su jacobiana. Como se aclaró anteriormente lo buscado son divisores de ℓ -torsiones en la jacobiana de la curva, es decir, divisores que cumplen con $\ell \cdot D = 0$, lo que por definición implica la existencia de una función $\mathcal{F}$ en el anillo de funciones de $\mathbb{H}(K)$ de la curva tal que los puntos en el soporte de D sean ceros de orden ℓ de f .

Tomando en cuenta la observación $*(1)$ $\mathcal{F}$ puede ser visto como su representante en $K[x, y]$ el cual es de la forma $f(x, y) = A(x) + yB(x)$. $\mathcal{F}$ tiene los mismos ceros que $f(x, y)$ considerando multiplicidad. Entonces rescatando lo mencionado en el párrafo anterior, que D sea un divisor de ℓ -torsión tiene como consecuencia directa que existe una función $f(x, y)$ en $K[x, y]$ tal que sus ceros son de orden ℓ .

Esta condición es posible de verificar mediante las derivadas formales e implícitas de f de la siguiente forma:

$$\begin{aligned}f(x, y) &= 0 \\ \frac{d}{dx} f(x, y) &= 0 \\ \frac{d^2}{dx^2} f(x, y) &= 0 \\ &\vdots\end{aligned}$$

$$\frac{d^{\ell-1}}{dx^{\ell-1}} f(x, y) = 0$$

Este sistema de ecuaciones polinomiales sera llamado $\mathcal{S}$ y tiene variables en Γ'_0

3.3. Intersecciones de $f(x, y) = 0$ con $\mathbb{H}(K)$

Notar que determinar los puntos donde $\mathcal{F}(x, y) = 0$ en $\mathbb{H}(K)$, es exactamente lo mismo que calcular la intersección de la expresión $f(x, y) = 0$ con $y^2 = h(x)$.

Proposición: Existe un polinomio $N(x)$ tal que si $f(x_0, y_0) = 0$ y $h(x_0) = y_0^2$ entonces $N(x_0) = 0$, y también si $N(x_0) = 0$, entonces existe un valor y_0 , tal que $f(x_0, y_0) = 0$ y $h(x_0) = y_0^2$.

Demostración:($\rightarrow$): Para poder encontrar este polinomio se impondrá que $f(x_0, y_0) = 0$ y que $y_0^2 = h(x_0)$. Tomando en cuenta que $f(x, y) = A(x) + yB(x)$:

$$\frac{A^2(x_0)}{B^2(x_0)} = y_0^2.$$

$$y_0^2 = h(x_0).$$

Y substituyendo y^2 en cualquiera de las 2 ecuaciones, se puede ver que se cumple la condición:

$$A^2(x_0) - h(x_0)B^2(x_0) = 0.$$

($\leftarrow$): Por otro lado si se tiene un polinomio $N(x)$ tal que:

$$N(x_0) = A^2(x_0) - h(x_0)B^2(x_0) = 0$$

Entonces manipulando la expresión

$$h(x_0) = \left(\frac{A(x_0)}{B(x_0)}\right)^2$$

y al definir $y_0 = -\frac{A(x_0)}{B(x_0)}$ se puede verificar que

$$h(x_0) = y_0^2$$

Finalmente por consecuencia de como se definió y_0 se cumple que

$$A(x_0) + yB(x_0) = 0$$

□

Por lo descrito en esta proposición $N(x) = A^2(x) - h(x)B^2(x)$ caracteriza efectivamente la intersección de las 2 expresiones mencionadas

Al imponer que la intersección es de orden ℓ se observa que

$$N(x) = A^2(x) - h(x)B^2(x) = u^\ell(x).$$

Como $\deg(u) = g$. Se tiene que

$$\deg(N(x)) = \max\{\deg(A^2(x)), \deg(h(x)B^2(x))\} = \deg(u^\ell).$$

$$\max\{2\deg(A(x)), \deg(h(x)) + 2\deg(B(x))\} = \ell g.$$

Como $\mathbb{H}$ es una curva de género, por definición $\deg(h(x)) = 2g + 1$.

$$\max\{2\deg(A(x)), 2g + 1 + 2\deg(B(x))\} = \ell g.$$

y por esto

$$\begin{aligned} \deg(A(x)) &\leq \frac{\ell g}{2} \\ \deg(B(x)) &\leq \frac{\ell g - 2g - 1}{2} \end{aligned}$$

Notar que dependiendo de si ℓg es par o impar se pueden hacer cálculos más exactos sobre esta cota, los grados relevantes para este trabajo son 1, 2, 3 así que haremos hincapié en lo que ocurre en esos contextos.

En las siguientes tablas se puede ver que ocurre en los distintos contextos.

$g = 1$	ℓ es par	ℓ es impar
$\deg(A) =$	$\frac{\ell}{2}$	$\frac{\ell-1}{2}$
$\deg(B) =$	$\frac{\ell}{2} - 2$	$\frac{\ell-3}{2}$

En esta table se puede ver el máximo grado que se puede suponer para A y B en género 1

$g = 2$	ℓ es par	ℓ es impar
$\deg(A) =$	ℓ	ℓ
$\deg(B) =$	$\ell - 3$	$\ell - 3$

Notar que en $g = 2$ el valor de $\deg(A)$ y $\deg(B)$ no varia tomando ℓ par o impar, esto se puede

$g = 3$	ℓ es par	ℓ es impar
$\deg(A) =$	$\frac{3\ell}{2}$	$\frac{3\ell-1}{2}$
$\deg(B) =$	$\frac{3\ell}{2} - 4$	$\frac{3\ell-7}{2}$

Observación: Es posible suponer a $A(x)$ y $B(x)$ de grado máximo, porque siempre es posible igualar los coeficientes líderes a 0, por lo tanto al decir $\deg(A)$ o $\deg(B)$ se tomaran en cuenta sus grados máximos

Observación: $\deg(A) + \deg(B) \leq \ell - g - 1$ para los géneros descritos

3.4. Linealización del sistema

Como se aclaró al principio de este capítulo, un divisor de ℓ -torsión de origen al sistema $\mathcal{S}$ en el conjunto de variables Γ'_0

$$\begin{aligned} f(x, y) &= 0 \\ \frac{d}{dx}f(x, y) &= 0 \\ \frac{d^2}{dx^2}f(x, y) &= 0 \\ &\vdots \\ \frac{d^{\ell-1}}{dx^{\ell-1}}f(x, y) &= 0 \end{aligned}$$

Para poder llevar esta expresión a términos más sencillos, es útil expresar este sistema polinomial como sistema lineal, para esto es necesario hacer la siguientes observaciones.

Observación: Es posible expresar un polinomio como producto de vectores de la siguiente forma:

$$p(x) = \sum_{n=0}^m c_n x^n = \begin{bmatrix} \sigma_0 x^0 & \sigma_1 x^1 & \dots & \sigma_m x^m \end{bmatrix} \begin{bmatrix} k_0 \\ k_1 \\ \vdots \\ k_m \end{bmatrix}$$

Con $k_j = \frac{c_j}{\sigma_j}$

En varias variables es posible describir la misma situación:

$$p(x_1, x_2, \dots) = \sum_{n=0}^m \lambda_n \chi_n(x_1, x_2, \dots) = \begin{bmatrix} \chi_0(x_1, x_2, \dots) & \chi_1(x_1, x_2, \dots) & \dots & \chi_m(x_1, x_2, \dots) \end{bmatrix} \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_m \end{bmatrix}$$

Al darse esta situación se dirá que $p(x_0, x_1, \dots)$ depende linealmente del vector $(\lambda_0, \lambda_1, \dots, \lambda_m)$

Ejemplo:

Para poder expresar mejor a que se quiere llegar con estas observaciones, veremos un ejemplo de que sucede con $f(x, y)$

$$f(x, y) = A(x) + yB(x) = \sum_{n=0}^{m_1} a_n x^n + \sum_{n=0}^{m_2} b_n y x^n$$

$$= \begin{bmatrix} x^0 & x^1 & \dots & x^{m_1} & yx^0 & yx^1 & \dots & yx^{m_2} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_m \\ \beta_0 \\ \beta_1 \\ \cdot \\ \cdot \\ \cdot \\ \beta_m \end{bmatrix}.$$

Observación: Al tener un vector formado por polinomios:

$$\begin{bmatrix} p_0(x_1, x_2, \dots) \\ p_1(x_1, x_2, \dots) \\ \cdot \\ \cdot \\ \cdot \\ p_l(x_1, x_2, \dots) \end{bmatrix}$$

Todos estos polinomios dependen linealmente de un mismo vector $(\lambda_0, \lambda_1, \dots, \lambda_k)$ de la forma

$$p_i(x_1, x_2, \dots) = \sum_{n=0}^m \lambda_n \chi_{i,n}(x_1, x_2, \dots) = \begin{bmatrix} \chi_{i,0}(x_1, x_2, \dots) & \chi_{i,1}(x_1, x_2, \dots) & \dots & \chi_{i,m}(x_1, x_2, \dots) \end{bmatrix} \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \cdot \\ \cdot \\ \cdot \\ \lambda_m \end{bmatrix}$$

Por ello, este vector de polinomios se puede expresar como

$$\begin{bmatrix} \chi_{0,0}(x_1, x_2, \dots) & \chi_{0,1}(x_1, x_2, \dots) & \dots & \chi_{0,m}(x_1, x_2, \dots) \\ \chi_{1,0}(x_1, x_2, \dots) & \chi_{1,1}(x_1, x_2, \dots) & \dots & \chi_{1,m}(x_1, x_2, \dots) \\ \vdots & \vdots & & \vdots \\ \chi_{\ell,0}(x_1, x_2, \dots) & \chi_{\ell,1}(x_1, x_2, \dots) & \dots & \chi_{\ell,m}(x_1, x_2, \dots) \end{bmatrix} \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_m \end{bmatrix} = \begin{bmatrix} p_0(x_1, x_2, \dots) \\ p_1(x_1, x_2, \dots) \\ \vdots \\ p_l(x_1, x_2, \dots) \end{bmatrix}$$

Retomando el resultado inicial, es posible expresar el sistema dado por las derivadas implícitas como un sistema lineal:

$$\begin{bmatrix} f(x, y) \\ \frac{d}{dx} f(x, y) \\ \frac{d^2}{dx^2} f(x, y) \\ \vdots \\ \frac{d^{\ell-1}}{dx^{\ell-1}} f(x, y) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

Analizando las dependencias lineales de todos los polinomios en cuestión se puede escribir el siguiente sistema lineal

$$\begin{bmatrix} 1 & x & x^2 & \dots & x^{\deg(A)} & y & yx & \dots & yx^{\deg(B)} \\ 0 & 1 & 2x & \dots & m_1 x^{\deg(A)-1} & y' & y'x + y & \dots & y'x^{\deg(B)} + m_2 yx^{\deg(B)-1} \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & \prod_{n=0}^{\ell-2} (\deg(A) - n) x^{\deg(B) - (\ell-2)} & y^{(\ell-1)} & \frac{d^\ell}{dx^\ell}(xy) & \dots & \frac{d^\ell}{dx^\ell} yx^{\deg(B)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_{\deg(B)} \\ \beta_0 \\ \beta_1 \\ \vdots \\ \vdots \\ \beta_{\deg(B)} \end{bmatrix}$$

Ahora para simplificar la ecuación será necesario declarar variables, $\mathcal{M}_0$ será la matriz en cuestión y $\vec{c}$ será el vector en la que esta matriz esta actuando.

Observación Considerando las filas de $\mathcal{M}_0$ y llamándolas $\{L_n\}_{0 \leq n \leq m}$ más específicamente:

$$L_n = \left[\underbrace{0 \dots 0}_{n \text{ veces}} \quad \kappa_{n,0} \quad \kappa_{n,1}x \quad \dots \quad \kappa_{n,m_1}x^{m_1-n} \quad \eta_{n,0}(x, y, y', \dots) \quad \dots \quad \eta_{n,m_2}(x, y, y', \dots) \right]$$

Con $\kappa_{i,j}$ constantes en K , y $\eta_{i,j}$ polinomios en $K[\Gamma']$. Es posible aplicar eliminación Gaussiana y simplificar la matriz en cuestión mediante la siguiente recursión

$$L_\ell^* = \frac{L_\ell}{\kappa_{0,\ell}}$$

$$L_n^* = \frac{L_n}{\kappa_{n,0}} - \sum_{n < i \leq \ell} \frac{x^{i-n} \kappa_{i,i-n}}{\kappa_{n,0}} L_i^*$$

Luego es posible escribir la matriz

$$\mathcal{M}_1 = \begin{bmatrix} L_1^* \\ L_2^* \\ L_3^* \\ \vdots \\ \vdots \\ \vdots \\ L_\ell^* \end{bmatrix}$$

Observación: La matriz $\mathcal{M}_1$ se puede dividir en 3 bloques de la forma

$$\begin{bmatrix} \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} & \begin{bmatrix} \theta_{0,0}(x) & \dots & \theta_{0,m_1-\ell}(x) \\ \vdots & \dots & \vdots \\ \vdots & \dots & \vdots \\ \theta_{0,\ell}(x) & \dots & \theta_{\ell,m_1-\ell}(x) \end{bmatrix} & \begin{bmatrix} \Theta_{0,0}(x, y, y', \dots) & \dots & \Theta_{0,m_2}(x, y, y', \dots) \\ \vdots & \dots & \vdots \\ \vdots & \dots & \vdots \\ \Theta_{0,\ell}(x, y, y', \dots) & \dots & \Theta_{\ell,m_2}(x, y, y', \dots) \end{bmatrix} \end{bmatrix}$$

Donde el primer bloque es la identidad, $\theta_{i,j}$ depende unicamente de x , y $\Theta(x, y, y', \dots)$ depende de todo Γ'_1 .

3.5. Derivadas implícitas respecto a x de y

Para reducir el numero de variables del sistema lineal obtenido, es útil expresar las derivadas implícitas de y .

Proposición: En la curva hiperelíptica $\mathbb{H}(K) : h(x) = y^2$ Es posible expresar $y^{(n)}$ en función de x e y de forma recursiva con la siguiente recursión

$$y^{(n)} = \frac{y r_n(x)}{2^n h^n(x)}$$

Con

$$r_{n+1}(x) = 2r'_n(x)h(x) - (2n-1)h'(x)r_n(x)$$

$$r_1(x) = h'(x)$$

Demostración: Para probar este hecho se procederá por inducción: Primero se vera que ocurre para $n = 1$. Es claro que.

$$2yy' = h'(x).$$

Manipulando esta expresión.

$$y' = \frac{h'(x)}{2y}.$$

$$y' = \frac{yh'(x)}{2y^2}.$$

Y ya que todo esto se cumple dentro de la curva hiperelíptica.

$$y' = \frac{yh'(x)}{2h(x)}.$$

Lo cual prueba la recursión dada para $n = 1$ Ahora suponiendo que la recursión es cierta para n .

$$y^{(n)} = \frac{yr_n(x)}{2^n h^n(x)}.$$

Ya que esta expresión se encuentra en una curva hiperelíptica es posible hacer la siguiente simplificación

$$y^{(n)} = \frac{yr_n(x)}{2^n y^{2n}} = \frac{r_n(x)}{2^n y^{2n-1}}.$$

$$y^{(n)} = \frac{yr_n(x)}{2^n y^{2n}} = \frac{r_n(x)}{2^n y^{2n-1}}.$$

Ahora, al tomar la derivada implícita de esta expresión

$$\begin{aligned} y^{(n+1)} &= \frac{1}{2^n} \frac{r'_n(x)y^{2n-1} - (2n-1)r_n(x)y'y^{2n-2}}{(y^{2n-1})^2} \\ &= \frac{1}{2^n} \frac{r'_n(x)y^{2n-1} - (2n-1)r_n(x)\frac{h'(x)}{2y}y^{2n-2}}{(y^{2n-1})^2} \\ &= \frac{1}{2^n} \frac{2r'_n(x)y^{2n-1} - (2n-1)r_n(x)h'(x)y^{2n-1}y^{-2}}{2(y^{2n-1})^2} \\ &= \frac{1}{2^n} \frac{2r'_n(x)y^2 - (2n-1)r_n(x)h'(x)}{2y^{2n+1}} \\ &= \frac{1}{2^n} \frac{2r'_n(x)h(x) - (2n-1)r_n(x)h'(x)}{2y^{2n+1}} \\ y^{(n+1)} &= \frac{r_{n+1}(x)}{2^{n+1}y^{2n+1}} \end{aligned}$$

Con esto se prueba la recursión para $n + 1$ suponiendo que se cumple para n , por ello se concluye la demostración por inducción

□

Ahora si se reemplazan esos valores en $\mathcal{M}_0$ la matriz generada sera $\mathcal{M}'_0$, y en $\mathcal{M}'_1$. Las matrices resultantes toman solo valores en $\mathbb{M}[\Gamma'_2]$

3.6. Modificación del sistema lineal vía representación de Mumford

Tomando en cuenta lo dicho en la sección 3.1, los divisores considerados tienen la forma

$$D = \sum_{k=1}^g n_{P_k} P_k.$$

Luego es posible considerar su representación de Mumford.

$$I = \langle u(x), y - v(x) \rangle.$$

Con $\deg(u(x)) = g$ y $\deg(v(x)) = g - 1$. Por ello $u = \sum_{n=0}^g u_n x^n$. y $v(x) = \sum_{n=0}^{g-1} v_n x^n$. con $u_n = 1$.

Dado que los puntos que anulan la representación de Mumford el soporte del divisor, es posible escribir un nuevo sistema en Λ_0

$$\begin{aligned} f(x, y) &\equiv 0 \quad (\text{mód } I) \\ \frac{d}{dx} f(x, y) &\equiv 0 \quad (\text{mód } I) \\ \frac{d^2}{dx^2} f(x, y) &\equiv 0 \quad (\text{mód } I) \\ &\vdots \\ &\vdots \\ &\vdots \\ \frac{d^{\ell-1}}{dx^{\ell-1}} f(x, y) &\equiv 0 \quad (\text{mód } I) \end{aligned}$$

Lo que tiene como consecuencia directa que:

$$\mathcal{M}_0 \vec{c} \equiv 0 \quad (\text{mód } I)$$

Y luego de reemplazar las derivadas implícitas de y :

$$\mathcal{M}'_0 \vec{c} \equiv 0 \quad (\text{mód } I)$$

Al expresar $\mathcal{M}'_0 \vec{c} = 0 \quad (\text{mód } I)$, se puede ver de la forma

$$\begin{bmatrix} \sum_{1 \leq n \leq g-1} x^n \omega_{n,0,0} & \cdots & \sum_{1 \leq n \leq g-1} x^n \omega_{n,0,\ell+1-g} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \sum_{1 \leq n \leq g-1} x^n \omega_{n,\ell,0} & \cdots & \sum_{1 \leq n \leq g-1} x^n \omega_{n,\ell,\ell+1-g} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_{deg(A)} \\ \beta_0 \\ \cdot \\ \cdot \\ \cdot \\ \beta_{deg(B)} \end{bmatrix} = 0$$

Con $\omega_{n,i,j}$ polinomios en $K[\Lambda_1]$

A raíz de esto se puede tener otra expresión lineal descrita en la siguiente pagina

$$\begin{bmatrix}
\begin{pmatrix} \omega_{0,0,0} & \dots & \omega_{0,0,\deg(A)+\deg(B)+2} \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \omega_{0,\ell,0} & \dots & \omega_{0,\ell,\deg(A)+\deg(B)+2} \end{pmatrix} \\
\begin{pmatrix} \omega_{1,0,0} & \dots & \omega_{1,0,\deg(A)+\deg(B)+2} \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \omega_{1,\ell,0} & \dots & \omega_{1,\ell,\deg(A)+\deg(B)+2} \end{pmatrix} \\
\cdot \\
\cdot \\
\cdot \\
\begin{pmatrix} \omega_{g-1,0,0} & \dots & \omega_{g-1,0,\deg(A)+\deg(B)+2} \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \cdot & \dots & \cdot \\ \omega_{g-1,\ell,0} & \dots & \omega_{g-1,\ell,\deg(A)+\deg(B)+1} \end{pmatrix}
\end{bmatrix}
\begin{bmatrix}
\alpha_0 \\
\cdot \\
\cdot \\
\cdot \\
\alpha_{\deg(A)} \\
\beta_0 \\
\cdot \\
\cdot \\
\cdot \\
\beta_{\deg(B)} \\
\alpha_0 x \\
\cdot \\
\cdot \\
\cdot \\
\alpha_{\deg(A)} x \\
\beta_0 x \\
\cdot \\
\cdot \\
\cdot \\
\beta_{m_2} x \\
\cdot \\
\cdot \\
\cdot \\
\cdot \\
\alpha_0 x^{g-1} \\
\cdot \\
\cdot \\
\cdot \\
\alpha_{\deg(A)} x^{g-1} \\
\beta_0 x^{g-1} \\
\cdot \\
\cdot \\
\cdot \\
\beta_{\deg(B)} x^{g-1}
\end{bmatrix} = 0$$

A la matriz en cuestión se le dirá $\mathcal{W}_0$ y al vector en cuestión se le dirá $\vec{\gamma}$.

Observación central: El hecho de que el sistema $\mathcal{S}$ tenga solución en Γ' es equivalente a que exista un vector $\vec{\gamma}$ cualquiera tal que $\mathcal{W}_0 \vec{\gamma} = 0$ y esto a su vez resulta equivalente a que $\ker(\mathcal{W}_0) \neq \{0\}$. Y todo esto resulta equivalente a que $\mathcal{W}_0$ no es de rango completo.

Es posible ilustrar todas las equivalencias dadas en esta observación de la siguiente forma:

$$\begin{aligned} \mathcal{S} \text{ Tiene solución en } \Gamma &\iff \exists \vec{\gamma} \in K(x)^{\deg(A)+\deg(B)-\{0\}} \text{ tq } \mathcal{W}_0 \vec{\gamma} = 0 \iff \ker(\mathcal{W}_0) \neq \{0\} \\ &\iff \mathcal{W}_0 \text{ No posee rango completo} \end{aligned}$$

Esta observación resulta central por el hecho de que reduce el calcular la solución de un sistema de ecuaciones polinomiales, encontrar una condición que diga en que contexto $\mathcal{W}$, tiene rango completo, que es un problema de álgebra lineal.

Observación: Es posible hacer el mismo proceso con $\mathcal{M}_1$ y generar una matriz llamada $\mathcal{W}_1$:

$$\left[\begin{array}{c} \left(\begin{array}{cccccc} 1 & \dots & 0 & \rho_{0,0,0} & \dots & \rho_{0,0,\deg(A)+\deg(B)-\ell} \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \end{array} \right) \\ \left(\begin{array}{cccccc} 0 & \dots & 1 & \rho_{0,\ell,0} & \dots & \rho_{0,\ell,\deg(A)+\deg(B)-\ell} \\ 0 & \dots & 0 & \rho_{1,0,0} & \dots & \rho_{1,0,\deg(A)+\deg(B)-\ell} \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ 0 & \dots & 0 & \rho_{1,\ell,0} & \dots & \rho_{1,\ell,\deg(A)+\deg(B)-\ell} \end{array} \right) \\ \cdot \\ \cdot \\ \cdot \\ \left(\begin{array}{cccccc} 0 & \dots & \cdot & \rho_{g-1,0,0} & \dots & \rho_{g-1,0,\deg(A)+\deg(B)-\ell} \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ \cdot & \dots & \cdot & \cdot & \dots & \cdot \\ 0 & \dots & 0 & \rho_{g-1,\ell,0} & \dots & \rho_{g-1,\ell,\deg(A)+\deg(B)-\ell} \end{array} \right) \end{array} \right]$$

Con $\rho_{i,j,k}$ polinomios en $K[\lambda_1]$ esta matriz cumple con la identidad

$$\text{rank}(\mathcal{W}_1) = \text{rank}(\mathcal{W}_0)$$

Observación: Sea la matriz $\mathcal{W}_2$ la matriz de la forma

$$\begin{bmatrix} \begin{pmatrix} \rho_{1,0,0} & \cdots & \rho_{1,0,\deg(A)+\deg(B)-\ell} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \rho_{1,\ell,0} & \cdots & \rho_{1,\ell,\deg(A)+\deg(B)-\ell} \end{pmatrix} \\ \cdot \\ \cdot \\ \cdot \\ \begin{pmatrix} \rho_{g-1,0,0} & \cdots & \rho_{g-1,0,\deg(A)+\deg(B)-\ell} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \rho_{g-1,\ell,0} & \cdots & \rho_{g-1,\ell,\deg(A)+\deg(B)-\ell} \end{pmatrix} \end{bmatrix}$$

Esta matriz si tiene rango incompleto, entonces el rango de $\mathcal{W}_1$ también es incompleto. Entonces es posible escribir la equivalencia:

$$\mathcal{S} \text{ Tiene soluciones en } \Gamma'_0 \iff \mathcal{W}_2 \text{ No posee rango completo}$$

Como los valores de $\{h_i\}_{0 \leq i \leq 2g-1}$ están fijos al dar la curva, entonces los valores en Λ_2 que hacen que $\mathcal{W}_2$ no tenga rango completo, son aquellos que dan origen a los divisores de orden ℓ de $\mathbb{H}(K)$.

Para ver que valores en Λ_2 hacen que $\mathcal{W}_2$ no tenga rango completo, es necesario calcular los subdeterminantes de $\mathcal{W}_2$ e igualarlos a 0, eso genera otro sistema de ecuaciones polinomiales que contiene $\binom{\ell(g-1)}{(\ell-1)(g-1)}$ ecuaciones y $2g$ variables

3.7. Ejemplos

Ejemplo 1:

Para $g = 1$ y $\ell = 3$ la situación es así:

El divisor $P = (x, y)$ es un cero de orden 3 de la función $f(x, y) = A(x) + yB(x)$ con $\deg(A(x)) = 1$ y $\deg(B(x)) = 0$, entonces se tiene el sistema $\mathcal{S}$ dado por derivadas implícitas de la siguiente forma:

$$\begin{aligned} \alpha_0 + \alpha_1 x_0 + y_0 \beta_0 &= 0 \\ 0 + \alpha_1 + y' \beta_0 &= 0 \\ 0 + 0 + y'' \beta_0 &= 0 \end{aligned}$$

Luego es posible escribir el sistema lineal

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & y' \\ 0 & 0 & y'' \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \end{bmatrix} = 0$$

Ahora reemplazando los valores de $y^{(n)}$ dados por la recursión se tiene que la matriz en cuestión es

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & \frac{y(3x^2+a)}{x^3+ax+b} \\ 0 & 0 & y \frac{12x(x^3+ax+b)-(3x^2+a)^2}{(x^3+ax+b)^2} \end{bmatrix}$$

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & \frac{y(3x^2+a)}{x^3+ax+b} \\ 0 & 0 & y \frac{3x^4+6ax^2+12bx-a^2}{(x^3+ax+b)^2} \end{bmatrix}$$

Observar que $3x^4+6ax^2+12bx-a^2 = \psi_3(x)$ para simplificar la matriz aun más y terminar con una matriz de la forma

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & \frac{y(3x^2+a)}{x^3+ax+b} \\ 0 & 0 & y \frac{\psi_3(x)}{(x^3+ax+b)^2} \end{bmatrix}$$

Ahora aplicar representación de Mumford no tiene mucho sentido ya que en la representación de Mumford $x = u_0$ y $y = v_0$, lo que en esencia significa que se mantendrían las mismas variables. Por ello en este contexto se procede a corroborar si $\mathcal{M}_0$ no tiene rango completo directamente. Para esto se puede calcular el determinante de $\mathcal{M}_0$ e igualarlo a 0.

$$\det(\mathcal{M}_0) = 0$$

$$y \frac{\psi_3(x)}{(x^3+ax+b)^2} = 0$$

$$y\psi_3(x) = 0$$

Y como se supuso en un inicio que $y \neq 0$ se puede concluir que todos los puntos que son de 3 torsión son los que en x cumplen que $y\psi_3(x) = 0$.

Ejemplo 2:

Para $g = 2$ y $\ell = 3$ la situación es así:

Se tiene que el divisor $D = P_1 + P_2$ es de orden ℓ de $f(x, y)$ por lo tanto en el sistema $\mathcal{S}$, $\deg(A(x)) = 3$ y $\deg(B(x)) = 0$. Por lo tanto el sistema $\mathcal{S}$ se puede escribir de la forma:

$$\begin{aligned}
&\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \beta_0 y \\
&0 + \alpha_1 + \alpha_2 2x + \alpha_3 3x^3 + \beta_0 y' \\
&0 + 0 + \alpha_2 2x + \alpha_3 3x^3 + \beta_0 y'' = 0
\end{aligned}$$

Luego el sistema lineal en cuestión es:

$$\begin{bmatrix} 1 & x & x^2 & x^3 & y \\ 0 & 1 & 2x & 3x^2 & y' \\ 0 & 0 & 2 & 6x & y'' \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \beta_0 \end{bmatrix} = 0$$

Después reemplazando los valores de $y^{(n)}$ la matriz en cuestión es de la forma

$$\begin{bmatrix} 1 & x & x^2 & x^3 & y \\ 0 & 1 & 2x & 3x^2 & y \frac{5x^4 + 32h_3x^2 + 2h_2x + h_1}{2h(x)} \\ 0 & 0 & 2 & 6x & y \frac{(20x^3 + 6h_3x + 2h_2)(x^5 + h_3x^3 + h_2x^2 + h_1x + h_0 - (5x^4 + 3x^2h_3 + 2h_2x + h_1)^2)}{4h^2(x)} \end{bmatrix}$$

La expresión de los términos en la ultima columna es muy compleja, así que se expresaran como $\zeta(x, h_0, h_1, h_2, h_3)$ dejando la matriz de la forma:

$$\begin{bmatrix} 1 & x & x^2 & x^3 & y \\ 0 & 1 & 2x & 3x^2 & y\zeta_1(x, h_0, h_1, h_2, h_3) \\ 0 & 0 & 2 & 6x & y\zeta_2(x, h_0, h_1, h_2, h_3) \end{bmatrix}$$

Ahora considerando el cociente por la representación de Mumford:

$$\begin{bmatrix} 1 & x & -u_1x - u_0 & (u_1^2 - u_0)x + u_1u_0 & v_1x + v_0 \\ 0 & 1 & 2x & 3u_1x - 3u_0 & (v_1x + v_0)\Omega_1(x, u_0, u_1, h_0, h_1, h_2, h_3) \\ 0 & 0 & 2 & 6x & (v_1x + v_0)\Omega_2(x, u_0, u_1, h_0, h_1, h_2, h_3) \end{bmatrix}$$

Luego separando la matriz en los valores de x y tomando los coeficientes de x^0

$$\begin{bmatrix} 1 & 0 & -u_0 & u_1u_0 & v_0 \\ 0 & 1 & 0 & -3u_0 & \omega_{0,1}(u_0, u_1, v_0, v_1, h_0, h_1, h_2, h_3) \\ 0 & 0 & 2 & 0 & \omega_{0,2}(u_0, u_1, v_0, v_1, h_0, h_1, h_2, h_3) \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & -u_1 & (u_1^2 - u_0) & v_1 \\ 0 & 0 & 2 & 3u_1 & \omega_{1,1}(u_0, u_1, v_1, v_2, h_0, h_1, h_2, h_3) \\ 0 & 0 & 0 & 6 & \omega_{2,1}(x, u_0, u_1, h_0, h_1, h_2, h_3) \end{bmatrix}$$

y juntando los términos de esta matriz se puede formar $\mathcal{W}_0$:

$$\begin{bmatrix} 1 & 0 & -u_0 & u_1 u_0 & v_0 \\ 0 & 1 & 0 & -3u_0 & \omega_{0,1}(u_0, u_1, v_0, v_1, h_0, h_1, h_2, h_3) \\ 0 & 0 & 2 & 0 & \omega_{0,2}(u_0, u_1, v_0, v_1, h_0, h_1, h_2, h_3) \\ 0 & 1 & -u_1 & (u_1^2 - u_0) & v_1 \\ 0 & 0 & 2 & 3u_1 & \omega_{1,1}(u_0, u_1, v_1, v_2, h_0, h_1, h_2, h_3) \\ 0 & 0 & 0 & 6 & \omega_{2,1}(u_0, u_1, h_0, h_1, h_2, h_3) \end{bmatrix}$$

Y por la observación central, esta es la matriz que se debe corroborar si tiene rango completo, para hacer esto es necesario calcular $\mathcal{W}_1$, que es $\mathcal{M}_1$ (mód I)

$$\begin{bmatrix} 1 & 0 & 0 & x^3 & y - xy\zeta_1(x, h_0, h_1, h_2, h_3) - \frac{3}{2}x^2y\zeta_2(x, h_0, h_1, h_2, h_3) \\ 0 & 1 & 0 & -3x^2 & y\zeta_1(x, h_0, h_1, h_2, h_3) - 2xy\zeta_2(x, h_0, h_1, h_2, h_3) \\ 0 & 0 & 1 & 3x & \frac{1}{2}y\zeta_2(x, h_0, h_1, h_2, h_3) \end{bmatrix}$$

Luego al considerar el cociente por la representación de Mumford

$$\begin{bmatrix} 1 & 0 & 0 & (u^2 - u_0)x + u_1u_0 & \epsilon_1(x, u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 1 & 0 & 3u_1x + 3u_0 & \epsilon_2(x, u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 0 & 1 & 3x & \epsilon_1(x, u_0, u_1, v_0, v_1, h_0, h_2, h_3) \end{bmatrix}$$

Luego hacer el mismo proceso de separar la matriz por los valores en x

$$\begin{bmatrix} 1 & 0 & 0 & u_1u_0 & \delta_{0,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 1 & 0 & 3u_0 & \delta_{0,2}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 0 & 1 & 0 & \delta_{0,3}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 0 & 0 & u^2 - u_0 & \delta_{1,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 0 & 0 & 3u_1 & \delta_{2,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 0 & 0 & 0 & 3 & \delta_{3,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \end{bmatrix}$$

Como el primer bloque posee rango completo, es necesario imponer que el segundo bloque no posea rango completo, obteniendo los 3 determinantes de las submatrices

$$\begin{bmatrix} u^2 - u_0 & \delta_{1,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 3u_1 & \delta_{2,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \\ 3 & \delta_{3,1}(u_0, u_1, v_0, v_1, h_0, h_2, h_3) \end{bmatrix}$$

Esta es finalmente la matriz $\mathcal{M}_2$, y por lo observado en la sección anterior, los valores de Λ_2 que hacen que todos los subdeterminantes de $\mathcal{M}_2$ sean distintos de 0, son aquellos que dan origen a la representación de Mumford de los divisores de 3 torsión

Capítulo 4

Trabajos futuros y conclusiones

En esta sección se describirán desafíos que aun no se han resuelto relacionados a este trabajo, muchos de estos desafíos pueden ser visto con la óptica de diversas disciplinas, por esto esta sección puede verse como una invitación a cooperar de manera interdisciplinaria.

Como se dijo antes, una de las finalidades de este trabajo era extrapolar la idea de los polinomios de división para curvas hiperelípticas, porque las soluciones de estos pueden ser rápidamente determinadas, pero esto tiene limitantes inherentes que serán detalladas en la subsección siguiente.

4.1. Limitantes inherentes al problema

Al trabajar en una curva hiperelíptica de género g y buscar los divisores de peso g que son de ℓ -torsión, la representación de Mumford de estos divisores posee $2g$ variables, pero las ℓ -torsiones son de dimensión 0 como variedad algebraica, lo que implica que aun en el caso de que se puedan ignorar g variables (aquellas que provienen de $v(x)$), seria necesario mínimo un sistema de g variables y por lo tanto de g ecuaciones. Todo esto implica que la idea de los polinomios de división no se puede extrapolar completamente, ya que 1 variable y 1 ecuación es una realidad que al parecer solo se puede dar en género 1, o al menos con la lógica que se esta trabajando actualmente

4.2. Problemas por resolver

4.2.1. Ecuaciones y variables en el sistema

Al resolver un sistema de ecuaciones polinomiales, la complejidad del problema depende, en su mayoría, de la cantidad de variables y de ecuaciones que

estén en juego. Por ello muchos de los esfuerzos futuros estaran dirigidos a reducir la cantidad de ecuaciones y variables, aunque nos veamos sujetos a las limitaciones descritas anteriormente.

La cantidad de ecuaciones dependen de ℓ : Este significa un problema ya que al aumentar el valor de ℓ . La posible solución a esto es que para cada género, la cantidad de ecuaciones sea fija. Una manera de llegar a esto es que dentro del sistema se puedan reconocer las dependencias de ciertas ecuaciones, y ver cuales "sobran". Otra manera es, encontrar una manera más eficiente de determinar el rango de estas matrices en específico que no sea calcular cada uno de los subdeterminantes de la matriz.

Cantidad de variables: Como se dijo antes, actualmente el sistema a determinar posee $2g$ variables, cuando en teoría podría ser un sistema de g variables.

Optimizaciones computacionales: Más allá de simplificar el proceso a nivel matemático, es posible adaptar las operaciones matemáticas para que sean más eficientes al trabajarlas computacionalmente, por ejemplo se pueden realizar esfuerzos para obtener determinantes de manera más eficiente .

4.2.2. Bases de Groebner

Uno de los principales problemas por resolver en este trabajo fue lidiar con las bases de Groebner, de hecho, uno de los objetivos era simplificar el cálculo de las ℓ -torsiones al punto de ocupar lo menos posible bases de Groebner, en otras palabras, terminar con un sistema de ecuaciones polinomiales lo más simple posible, o en su defecto, terminar con un sistema lineal que se pueda resolver con métodos no tan específicos. Los problemas principales en el uso de las bases de Groebner son los siguientes:

Mucha generalidad: Como las bases de Groebner están pensadas para la resolución de cualquier sistema polinomial, por el hecho de ser muy generales recurren a métodos poco eficientes, pero útiles en cualquier caso.

Dificultad de determinar su complejidad asintótica: Las bases de Groebner poseen en general una complejidad asintótica exponencial, pero en casos muy específicos su complejidad se reduce mucho, el problema es que es difícil determinar hasta que punto se reduce.

El hecho de que sea difícil determinar la complejidad asintótica complica mucho las cosas, porque fuera de resultados experimentales es difícil tener una idea de cuanto podría demorar el cálculo de las ℓ -torsiones para ciertos ℓ .

4.3. Conclusiones

En conclusión el método provee una forma para calcular efectivamente la ℓ -torsión en género arbitrario, a partir de un sistema de $2g$ variables y $\binom{\ell(g-1)}{(\ell-1)(g-1)}$ ecuaciones dadas por los determinantes de una matriz determinada. Como fue mencionado en la sección anterior en lo que respecta a variables y ecuaciones aun se pueden realizar optimizaciones.

En cuanto a los programas escritos aun no logramos los tiempos deseados en género $g = 3$, pero el método viene bien encaminado. Uno de los objetivos iniciales de esta idea era poder reducir el problema de calcular divisores de ℓ -torsión algo que a priori es teórico y complejo un problema algorítmico como lo es calcular determinantes de una matriz.

En resumen es posible concluir que siguiendo todo lo propuesto en los trabajos futuros, como lo es optimizar la solución del sistema (optimizar el proceso donde se utilizan bases de Groebner), reduciendo la cantidad de variables descritas en el sistema, idealmente al punto de que la cantidad de ecuaciones no dependa de ℓ , y optimizando computacionalmente el método, seria posible obtener algo aplicable para el conteo de puntos en curvas de género $g = 3$,

Bibliografía

- [1] P. Gaudry and E. Schost, *Genus 2 point counting over prime fields*, Journal of Symbolic Computation, **47** (4), 368-400, 2012.
- [2] J. Miret, J. Pujolàs and N. Thériault, *On ℓ -th roots and division by ℓ* , preprint, 2024, <https://arxiv.org/abs/2403.06619>.
- [3] N. Thériault, *Speeding up the computation of group order of genus 2 curves over finite fields*, charla, Rene 25 conference, 2025.
- [4] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography, Second Edition*, Chapman & Hall/CRC, New York, 2008. MR2404461.
- [5] I.F. Blake, G. Serousii and N.P Smart *Elliptic Curves in Cryptography* 1999. Cambridge University Press. 39-42
- [6] H. Cohen and Gerard Frey *Handbook of Elliptic and Hyperelliptic Curve Cryptography* Chapman & Hall/CRC 84
- [7] H. Cohen and Gerard Frey *Handbook of Elliptic and Hyperelliptic Curve Cryptography* Chapman & Hall/CRC 110-112
- [8] H. Cohen and Gerard Frey *Handbook of Elliptic and Hyperelliptic Curve Cryptography* Chapman & Hall/CRC 548-551
- [9] H. Cohen and Gerard Frey *Handbook of Elliptic and Hyperelliptic Curve Cryptography* Chapman & Hall/CRC 309
- [10] Wolfgang Kampkötter *Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven* Universität Gesamthochschule essen
- [11] J.Pila *Frobenius Maps Of Abelian Varieties And Finding Roots Of Unity In Finite Fields* Mathematics of Computation Volume 55 Number 192
- [12] Robin Hasthorne *Algebraic Geometry* Springer Graduate Texts in Mathematics 5-6