Seminário de Pesquisa

As conjecturas de Weil

Hernán Alberto Iriarte Carrasco

Índice general

Introdução

Em 1942 André Weil conseguiu dar uma prova completa à hipótese de Riemann para corpos de funções. Isto levo a ele em 1949 a generalizar a conjectura ao contexto de dimensão maior. O análogo dos corpos de funções passam a ser as variedades algébricas definidas sobre $\mathbb{F}_q$ e o análogo da função zeta do corpo de função passa a ser uma função geradora contendo informação do contagem do número de pontos da variedade sobre os diferentes $\mathbb{F}_{q^n}$. Logo formula uma serie de conjecturas sobre a função zeta que não só generalizam a hipótese de Riemann sino que também dão uma expressão para o número de pontos em $\mathbb{F}_{q^n}$ da variedade e descrevem a relação do contagem destes pontos com a topologia da variedade.

O propósito de este trabalho é

- Mostrar as raízes históricas das conjecturas (Capítulo 2).
- Enunciar as conjecturas, motivar elas pelo estudio dos pontos racionais das variedades em $\mathbb{F}_q$ por medio do morfismo de Frobenius e mostrar a historia que houve na resolução delas. (Capítulo 3)
- Mostrar provas das conjecturas no caso particular das curvas elípticas (Capítulo 4)

Durante o capítulo 1 se dará um resumo rápido dos conceitos necessários para a leitura do documento.

Capítulo 1

Conceitos Previos

Corpos finitos

Dado um corpo k, se existe um inteiro n tal que $1 + 1 + ... + 1$ n-vezes é 0 então o menor de tais inteiros é chamado a **característica** de k. Se por outro lado não existe um tal inteiro n então se diz que k tem característica 0. Assim por exemplo a característica de $\mathbb{Z}/p\mathbb{Z}$ é p e a característica de $\mathbb{Q}$ é 0.

Proposición 1. *A característica de um corpo sempre é zero o um número primo.*

Dado um corpo k temos o mapa canônico $\mathbb{Z} \to k$ dado por $n \mapsto 1+1+...+1$ n-vezes, este mapa é um morfismo de anéis. Se a característica do corpo k é p o núcleo do morfismo é $p\mathbb{Z} = \{pn \mid n \in \mathbb{Z}\}$. Assim pelo teorema do isomorfismo se $p \neq 0$ temos uma inclusão canônica de $\mathbb{Z}/p\mathbb{Z}$ em k e se $p = 0$ temos uma inclusão canônica de $\mathbb{Z}$ em k a qual pode-se estender a uma inclusão de $\mathbb{Q}$ em k. Com isto vemos que

Proposición 2. *Se um corpo tem característica p com $p \neq 0$ então o corpo contem como subcorpo a $\mathbb{Z}/p\mathbb{Z}$ e se tem característica 0 então contem como subcorpo a $\mathbb{Q}$*

Se k é um corpo finito de característica p, pela proposição acima temos uma inclusão canônica de $\mathbb{Z}/p\mathbb{Z}$ em k, assim podemos ver a k como um $\mathbb{Z}/p\mathbb{Z}$ espaço vetorial (onde a multiplicação por escalar e a suma são as operações do corpo k), isto nos da um isomorfismo de espaços vetoriais (e em particular uma bijecção) de k com $(\mathbb{Z}/p\mathbb{Z})^n$ para algum n de onde concluímos que k tem p^n elementos, assim temos o seguinte resultado.

Proposición 3. *Todo corpo finito tiene por número de elementos a potencia de um primo. Em particular todo corpo finito de caracteristíca p tiene por número de elementos uma potencia de p.*

Reciprocamente temos o seguinte resultado.

Proposición 4. *Para todo número da forma $q = p^n$ com p um número primo existe um e só um corpo com q elementos salvo isomorfismo. Este corpo o denotamos por $\mathbb{F}_q$.*

Assim por exemplo se p é um número primo temos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Agora se $q = p^s$, a seguinte proposição nos mostra como se relacionam os distintos $\mathbb{F}_{q^n}$ entre si e com a clausura algébrica[1] de $\mathbb{F}_q$.

Proposición 5. *Denotando por $\bar{\mathbb{F}}_q$ a uma clausura algébrica do $\mathbb{F}_q$ fixa.*

- *Para todo n existe uma soa copia de $\mathbb{F}_{q^n}$ tal que $\mathbb{F}_{q^n} \subset \bar{\mathbb{F}}_q$.*
- *Dado $n \in \mathbb{N}$ e k um divisor de n temos $\mathbb{F}_q \subset \mathbb{F}_{q^k} \subset \mathbb{F}_{q^n} \subset \bar{\mathbb{F}}_q$*
- *Todo elemento de $\bar{\mathbb{F}}_q$ pertence a algum $\mathbb{F}_{q^n}$, isto é, $\bar{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$*

É importante notar que $\bar{\mathbb{F}}_q = \bar{\mathbb{F}}_{q^k}$ para todo k.

Para finalizar nosso passo pelos corpos finitos veiamos um importante automorfismo[2] deles.

Definição 1. O automorfismo de Frobenius de exponente p^k no corpo $\bar{\mathbb{F}}_p$ é o mapa $\text{Frob} : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$ dado por $x \mapsto x^{p^k}$.

É claro que $\text{Frob}(xy) = \text{Frob}(x)\text{Frob}(y)$, o fato que $\text{Frob}(x+y) = \text{Frob}(x) + \text{Frob}(y)$ se prova primeiro para expoente p primo usando o binômio de Newton e o fato que $p \mid \binom{p}{k}$ para $1 \leq k \leq p-1$. O caso geral se deduz deste já que ao compor o automorfismo de Frobenius de expoente p com ele mesmo k vezes obtemos o automorfismo de Frobenius de expoente p^k.

Usando o fato que as raízes da equação $x^{q^k} - x = 0$ em $\bar{\mathbb{F}}_q$ são exatamente os elementos de $\mathbb{F}_{q^k}$ temos o seguinte resultado.

Proposición 6. *Os pontos fixos do automorfismo de Frobenius de peso q^k em $\bar{\mathbb{F}}_q$ são exatamente os elementos do corpo $\mathbb{F}_{q^k}$*

Variedades Algébricas

As variedades algébricas são conjuntos de soluções de um sistema de equações polinomiais. Para ter uma boa teoria de variedades algébricas e evitar que um polinômio tenha associada ao conjunto vazio como variedades algébrica temos que trabalhar sempre com corpos algebricamente fechados.

[1] Lembremos que um corpo é algebricamente fechado se todo polinômio com coeficientes no corpo tem um cero no corpo. A clausura algébrica de um corpo k é um corpo algebricamente fechado K tal que $k \subset K$ e se existe um corpo L algebricamente fechado com $k \subset L \subset K$ então $K = L$.

[2] Um automorfismo de um corpo K é um mapa $f : K \to K$ que é um isomorfismo de corpos, isto é, é bijetivo, $f(x+y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$

Nesta secção partiremos introduzindo as variedades algébricas afins para logo ver as variedades algébricas projetivas que em certa forma são compactificações das variedades algébricas afins.

Variedades Algébricas afins

Definição 2. Dado um corpo K algebricamente fechado definimos o espacio afim de dimensão d, $\mathbb{A}^d(K)$ o simplesmente $\mathbb{A}^d$ como sendo o conjunto $K \times K \times ... \times K = K^d$. Uma variedade algébrica afim X em $\mathbb{A}^d(K)$ é um conjunto da forma

$$X = V(f_1, ..., f_k) := \{(x_1, ...x_d) \in \mathbb{A}^d(K) \mid f_1(x_1, ..., x_d) = ... = f_k(x_1, ..., x_d) = 0\}$$

Onde $f_i \in K[x_1, ..., x_d],\ i = 1, ..., r$. Se existe um subcorpo $k \subset K$ tal que os polinômios tem coeficientes em k então a variedade X se diz definida sobre k.

Vejamos alguns exemplos de variedades algébricas afins

- O conjunto vazio $\emptyset$ e o espaço $\mathbb{A}^d(K)$ são variedades algébricas afins, já que $\emptyset = V(1)$ e $\mathbb{A}^d(K) = V(0)$.
- Os pontos $\{(a_1, ..., a_d)\} \in \mathbb{A}^d(K)$ são variedades algébricas afins, já que $\{(a_1, ..., a_d)\} = V(x_1 - a_1, ..., x_d - a_d)$
- As cônicas complexas são variedades algébricas já que são conjuntos da forma $C = \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \mid f(x, y) = 0\}$ onde f é um polinômio quadrático em duas variáveis.

E simples provar que interseção e união de variedades algébricas afins é uma variedade algébrica afim.

Variedades Algébricas Projetivas

Passemos agora a introduzir as variedades algébricas projetivas. Para isto debemos primeiro dar uma olhada ao espaço ambiente delas.

Definição 3. O espaço projetivo $\mathbb{P}^d(K)$ (o $\mathbb{P}^d$ se o corpo fica subentendido) se define como o quociente de $K^{d+1} \setminus \{0\}$ pela relação de equivalência $(x_1, ..., x_{d+1}) \sim (y_1, ..., y_{d+1})$ sse existe $\lambda \in K \setminus \{0\}$ tal que $x_i = \lambda y_i\ \forall i$.

Os pontos de $\mathbb{P}^d(K)$ são representados pelo simbolo $(x_1 : \cdots : x_{d+1})$ onde $(x_1, ..., x_{d+1})$ é um representante da classe do ponto. Os elementos x_i são chamados as coordenadas homogêneas do ponto e os dois pontinhos «:» indicam que apenas os quocientes das coordenadas homogêneas interessam.

O espaço afim $\mathbb{A}^d(K)$ pode-se identificar com o conjunto $\{(x_1 : \cdots : x_{d+1}) \in \mathbb{P}^d(K) \mid x_{d+1} \neq 0\}$ usando o mapa $(x_1, ..., x_n) \mapsto (x_1 : \cdots : x_d : 1)$ cuja inversa é o mapa $(x_1 : \cdots : x_{d+1}) \mapsto (\frac{x_1}{x_{d+1}}, \ldots \frac{x_d}{x_{d+1}})$

Notemos agora que dado um polinômio f não podemos avaliar ele numa coordenada homogênea já que em geral o valor depende do representante. Mas se o polinômio fosse homogêneo temos

$$f(\lambda x_1, ..., \lambda x_{d+1}) = \lambda^c f(x_1, ..., x_{d+1})$$

E assim $f(\lambda x_1, ..., \lambda x_{d+1})$ vale zero sse $f(x_1, ..., x_{d+1})$ vale zero. Assim podemos dizer sem ambiguidade que uma coordenada homogênea anula um polinômio homogêneo, denotamos por $f(x_1 : \dots x_{d+1}) = 0$. Pelo tanto o subconjunto de $\mathbb{P}^d(K)$ que anula um polinômio homogêneo é um subconjunto bem definido.

Definição 4. Dado um corpo K algebricamente fechado. Uma variedade algébrica projetiva X em $\mathbb{P}^d(K)$ é um conjunto da forma

$$X = V_{\mathbb{P}}(f_1, ..., f_r) := \{(x_1 : \cdots : x_{d+1}) \mid f_1(x_1 : \cdots : x_{d+1}) = \cdots = f_r(x_1 : \cdots : x_{d+1}) = 0\}$$

Onde os f_i são polinômios homogêneos em $K[x_1, ..., x_{d+1}]$. Se existe um subcorpo $k \subset K$ tal que os polinômios têm coeficientes em k então a variedade se diz definida sobre k.

Vejamos agora como completar uma variedade algébrica afim para obter uma variedade algébrica projetiva.

Dado um polinômio $f \in K[x_1, ..., x_d]$ definimos sua homogenização como sendo o polinômio homogêneo $f^* \in K[x_1, ..., x_{d+1}]$ definido por $f^*(x_1, ..., x_{d+1}) = x_{d+1}^{\deg(f)} f(\frac{x_1}{x_{d+1}}, ..., \frac{x_d}{x_{d+1}})$.

Se $X = V(f_1, ..., f_r)$ é uma variedade algébrica afim definimos sua projetivização por $X^* = V(f_1^*, ..., f_r^*)$. Usando a identificação de $\mathbb{A}$ com um subconjunto de $\mathbb{P}^d$ vista acima não é difícil ver que $X \subset X^*$, assim podemos pensar em X^* como um jeito de agregar pontos a variedade X para que fique projetiva. No caso $K = \mathbb{C}$, X^* é uma compactificação de X com a topologia euclideana.

Pontos racionais na variedades algébricas

Se X é uma variedade algébrica (afim ou projetiva) definida sobre k então para todo corpo L tal que $k \subset L \subset K$ pomos definir os pontos L-racionais na variedade X, isto é, os pontos em X com coordenadas em L da seguinte forma

Definição 5. Seja X uma variedade definida sobre k e L um corpo tal que $k \subset L \subset K$, se X é uma variedade afim em $\mathbb{A}^n(K)$ então o conjunto de pontos L-racionais de X é o conjunto

$$X[L] := \{(a_1, ..., a_n) \in X \mid a_i \in L \ \forall i\}$$

e se X é uma variedade algébrica projetiva em $\mathbb{P}^n(K)$ então é o conjunto

$$X[L] := \{(a_1 : \cdots : a_{d+1}) \in X \mid \exists \lambda \in K \setminus \{0\} \text{ tal que } a_i\lambda \in L \ \forall i\}$$

Assim por exemplo o problema de resolver equaciones diofânticas nos números racionais é o problema de encontrar os pontos $\mathbb{Q}$-racionais das hipersuperficies, i.e variedades da forma $V(f)$, definidas sobre $\mathbb{Q}$.

A geometria analítica da escola pode-se ver como manipulações com os pontos $\mathbb{R}$-racionais de certas variedades algébricas em $\mathbb{A}^2(\mathbb{C})$ o $\mathbb{A}^3(\mathbb{C})$.

Agora do falado sobre corpos finitos sabemos que se $q = p^n$ com p primo então $\mathbb{F}_q \subset \mathbb{F}_{q^n} \subset \bar{\mathbb{F}}_q$ Logo dada uma variedade algébrica X (afim o projetiva) tem sentido os conjuntos $X[\mathbb{F}_{q^n}]$ para todo n.

Dada uma variedade X definida em $\bar{\mathbb{F}}_q$ definimos o morfismo de Frobenius de X de expoente q^k por $\text{Frob} : X \to X$ donde $(x_1, ..., x_n) \mapsto (\text{Frob}(x_1), ..., \text{Frob}(x_n))$ se $X \subset \mathbb{A}^n(\bar{\mathbb{F}}_q)$ es afim ou $(x_1 : ... : x_{n+1}) \mapsto (\text{Frob}(x_1) : ..., \text{Frob}(x_{n+1}))$ se $X \subset \mathbb{P}^n(\bar{\mathbb{F}}_q)$ é projetiva.

Como Frob é um automorfismo é fácil ver que o morfismo fica bem definido, isto e, a imagem de pontos em X cae em X.

Como o conjunto de pontos fixos do morfismo Frob de expoente q^k é $\mathbb{F}_{q^k}$ temos o seguinte.

Proposición 7. *O conjunto dos pontos fixos do morfismo de Frobenius de X de expoente q^k é $X[\mathbb{F}_{q^k}]$.*

Capítulo 2

Origem Histórica

Neste capítulo mostraremos a historia da hipótese de Riemann para corpos de funções que foi provavelmente o maior motivo de André Weil pelo qual formulo as conjecturas que levam seu nome em 1949. Para fazer isto deveremos mencionar além dos trabalhos prévios de Weil os trabalhos de Riemann, Artin, Schimdt e Hasse.

2.1. A Hipótese de Riemann clássica

Começaremos fazendo um resumo da teoria original da hipóteses de Riemann. Os resultados desta secção forem principalmente demonstrados por Riemann em 1859 em seu paper «On the Number of Primes Less Than a Given Magnitude»

Para partir introduziremos ao protagonista da história.

Definição 6. Definimos a função zeta de Riemann por $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ para s complexo com $\mathrm{Re}(s) > 1$.

Notemos que para a real positivo temos $|a^s| = |e^{\log(a)s}| = e^{\mathrm{Re}(log(a)s)} = a^{\mathrm{Re}(s)}$ e assim quando $\mathrm{Re}(s) > 1$ se tem

$$\sum_{n=0}^{\infty} \left| \frac{1}{n^s} \right| = \sum_{n=0}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} < \infty$$

De onde concluímos que o domínio de convergência da serie que define a função zeta de Riemann é justamente $\mathrm{Re}(s) > 1$. Sobre esta região ζ temos a seguinte formula de produto.

Proposición 8. (Produto de Euler) *Se $Re(s) > 1$ temos*

$$\sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_{p\ primo} \left(1 - \frac{1}{p^{-s}}\right)$$

Onde o produto percorre todos os números primos.

Prova: Temos

$$\prod_{p\leq N \text{ Primos}} \frac{1}{1-p^{-s}} = \prod_{p\leq N \text{ Primos}} \left(\sum_{k=1}^{\infty}(p^{-s})^k\right) = \sum_{n\leq N} \frac{1}{n^s} + R_N(s)$$

Onde $R_N(s) \leq \sum_{n=N+1}^{\infty} n^{-s}$. Passando ao limite concluímos o resultado. ■

É importante mencionar que o produto de Euler se debe entender como uma implicância do Teorema Fundamental da Aritmética (isto é, todo número se escrive de maneira única como produto de primos) sobre a função zeta.

Agora como é comum em análise complexo nasce a pergunta de estudar as extensões analíticas a abertos maiores. Com respeito a isto resulta que a função zeta aceita uma extensão analítica a todo $\mathbb{C}$. Mais precisamente temos o seguinte teorema cuja prova omitiremos.

Teorema 1. *A função*

$$\hat{\zeta}(s) := \pi^{\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$$

tem uma extensão analítica a todo o plano com polos simples em $s = 0, 1$ e satisfaz a equação funcional $\hat{\zeta}(s) = \hat{\zeta}(1-s)$. Isto em particular implica que a função zeta tem uma extensão analítica a todo o plano com um único polo simples em $s = 1$.

O teorema acima também nos mostra que $-2, -4, -6, ...$ são zeros da função zeta, estes são chamados os **zeros triviais** da função zeta. Notemos que os zeros não triviais de ζ são justamente os zeros de $\hat{\zeta}$, agora usando a equação funcional e o fato que $\hat{\zeta}(\overline{s}) = \overline{\hat{\zeta}(s)}$ (já que ao avaliar a $\hat{\zeta}$ nos reais obtemos reais) temos.

$$\overline{\hat{\zeta}(s)} = \overline{\hat{\zeta}(1-s)} = \hat{\zeta}(1-\overline{s}) = \hat{\zeta}(\overline{s})$$

Assim, se s é um zero não trivial de ζ também é $1-s, \overline{s}$ e $1-\overline{s}$. Portanto, o conjunto dos zeros não triviais é simétrico ao respeito das retas $\text{Re}(s) = 1/2$ e $\text{Im}(s) = 0$.

A hipótese de Riemann é a afirmação de que todos os zeros não triviais caem dentro do eixo de simetria $\text{Re}(s) = 1/2$, ou em outras palavras

Conjetura 1. *Se s é um zero não trivial de ζ então $Re(s) = 1/2$.*

Para terminar é importante mencionar que a hipótese de Riemann esta intimamente relacionada com o problema de encontrar aproximações para o número de primos menores que uma constante.

Se definimos $\pi(x) = \#\{p \in \mathbb{N} \mid 1 \leq p \leq x \text{ e } p \text{ é um número primo}\}$ então a hipótese de Riemann é equivalente com a aproximação

$$\left|\pi(x) - \int_2^x \frac{dt}{log(t)}\right| = O(x^{\frac{1}{2}}(logx)^2)$$

Notemos que isto melhora o resultado já conhecido de que

$$\left|\pi(x) - \int_2^x \frac{dt}{log(t)}\right| = O\left(\frac{x}{e^{-2\sqrt{log(x)}}}\right)$$

2.2. A Hipótese de Riemann para corpos de funções

Corpos de funções em uma variável

Um corpo de funções em uma variável[1] é um corpo da forma $K = \mathbb{F}_q(x,y) = \{\frac{\sum_{i,j\geq 0} a_{ij}x^iy^j}{\sum_{i,j\geq 0} b_{ij}x^iy^j} \mid a_{ij}, b_{ij} \in \mathbb{F}_q, a_{ij} = b_{ij} = 0 \text{ para quasi todo } i,j\}$ onde x, y são variáveis formais satisfazendo uma relação da forma $f_K(x,y) = 0$ com $f_K \in \mathbb{F}_q[x,y]$ um polinômio irredutível em duas variáveis.

De maneira equivalente é o corpo de frações do anel cociente $K[x,y]/(f_k(x,y))$.

Assim por exemplo, pegando $f_K(x,y) = y$ vemos que o corpo de funções racionais $\mathbb{F}_q(x) := \{\frac{p(x)}{q(x)} \mid p, q \in \mathbb{F}_q[x]\}$ é um corpo de funções em uma variável.

Um corpo de funções em uma variável K tem associada de jeito natural a curva $C_K = V(f_K) \subset A^2(\overline{\mathbb{F}}_q)^2$. Reciprocamente como se vê num curso de curvas algébricas, dada uma curva C definida sobre $\mathbb{F}_q$ é possível obter um corpo de funções olhando o corpo formado pelas funções $C \to \mathbb{P}^1$ dadas por cocientes de polinômios com coeficientes em $\mathbb{F}_q$. Esta correspondência mostra o origem do nome «Corpo de funções».

Agora para o que segue precisamos falar do anel de inteiros de um corpo de funções.

Definição 7. O anel de inteiros $\mathcal{O}_K$ de um corpo de funções $K = \mathbb{F}_q(x,y)$ se define como a clausura inteira[3] do anel $\mathbb{F}_q[x]$

Assim do mesmo jeito que o anel de inteiros de um corpo de números, o anel de inteiros de um corpo de funções deve-se entender como um novo sistema numérico onde é possível estender os resultados da aritmética.

Temos os seguintes resultados sobre $\mathcal{O}_K$

Proposición 9. *Seja K um corpo de funções e $\mathcal{O}_K$ seu anel de inteiros.*

[1] Para simplificar um pouco as definições daremos uma definição com uma eleição de geradores x, y fixa

[2] Trabalharemos com a corva afim sem seus pontos no infinito, esto é para manter a consistência já que trabalharemos só com as valorações finitas do corpo de funções

[3] A clausura inteira de um anel A num corpo K é o conjunto de todos os elementos de K que são raiz de um polinômio mônico com coeficientes no anel A

1. *Todo ideal $I \subset O_K$ pode-se escrever de maneira única como $I = P_1^{\alpha_1} \cdot ... \cdot P_n^{\alpha_n}$[4] onde os P_i são ideais primos e $\alpha_i \in \mathbb{N}$*

Agora definamos a norma de um ideal $I \subset \mathcal{O}_K$ por $N(I) := \#\mathcal{O}_K/I$, com esta definição temos

2. *para todo ideal I de $\mathcal{O}_K$ existe um inteiro m_I tal que $N(I) = q^{m_I}$*

3. *O número de ideais I tais que $N(I) = q^n$ com n fixo é menor o igual do que q^n.*

Prova: Ver [3]

A função zeta de Riemann de um corpo de funções

Em 1921 Artin em sua tésis de doutorado gerou uma teoria aritmética para uma certa familia de corpos de funções análoga a teoria feita por Dedekind em corpos de números. Com essas ideais ele foi capaz de definir o anel de inteiros e a correspondente função zeta associada ao corpo de funções.

Mais no foi até 1931 quando F.K Schmidt estendeu os resultados e conseguiu definir estes objetos no caso geral. Apresentaremos este enfoque aqui baseado em certo modo nas notas históricas [5].

A função zeta de Riemann pode-se ver como um objeto analítico que codifica informação aritmética sobre o conjunto $\mathbb{Z}$ dos números inteiros. Baixo este ponto de vista é natural perguntar-se se é possível obter uma função análoga para outros sistemas numéricos como o anel de inteiros de um corpo de funções.

Para estender a definição da função zeta a estes contextos notemos que em $\mathbb{Z}$ temos uma correspondência entre $\mathbb{N}$ e os ideais de $\mathbb{Z}$ dada por

$$n \longmapsto n\mathbb{Z}$$

$$I \longmapsto \#(\mathbb{Z}/I) = N(I)$$

Assim a função zeta pode-se expressar da seguinte forma

$$\zeta(s) = \sum_{I \subset \mathbb{Z} \text{ ideais}} \frac{1}{N(I)^s}$$

Isto nos leva a definir a função zeta ζ_K de um corpo de funções pela expressão

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K \text{ ideais}} \frac{1}{N(I)^s}$$

Esta suma converge para $s > 1$ pois por a parte (2) e (3) da proposição 9 temos

$$\sum_{I \subset \mathcal{O}_K \text{ ideais}} \frac{1}{N(I)^s} = \sum_{n=1}^{\infty} \frac{\#\{I \mid N(I) = q^n\}}{q^{ns}} = \sum_{n=1}^{\infty} \frac{1}{(q^{s-1})^n} \leq \infty$$

[4]Dados ideais I, J num anel A definimos o produto deles IJ como o ideal gerado pelos elementos $a \cdot b$ com $a \in I, b \in J$

Usando o primeiro fato do teorema 7 junto com o fato que a norma de um ideal é multiplicativa (isto é, $N(IJ) = N(I) \cdot N(J)$) é possível replicar a prova mostrada na secção anterior para provar uma formula de produto de Euler para a função zeta

$$\zeta_K(s) = \prod_{\substack{P \subset \mathcal{O}_K \\ \text{ideal primo}}} \frac{1}{1 - (\#\mathcal{O}_k/P)^{-s}}$$

Agora vejamos que é possível dar uma expressao para a função zeta usando só informação do número de pontos da curva afim C_K.

Teorema 2. *Dado $K = \mathbb{F}_q(x, y)$ temos*

$$\zeta_K(s) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C[\mathbb{F}_{q^n}]T^n}{n}\right)$$

onde $T = q^{-s}$

Prova: Da proposição 9 temos que $\forall P \subset \mathcal{O}_K$ ideal primo temos $\#\mathcal{O}/P = q^{m_P}$. Logo usando fatos da geometria algébrica é possível provar que $\sum_{P \text{ tais que } m_p|n} = \#C[\mathbb{F}_{q^n}]$. Usando este ultimo fato temos

$$\begin{aligned}
T\frac{d}{dT}\log\zeta_K(S) &= \frac{-1}{\log q}\frac{d}{ds}\log\zeta_K(s) \\
&= \frac{-1}{\log q}\frac{d}{ds}\log \prod_{\substack{P \subset \mathcal{O}_K \\ \text{ideal primo}}} \frac{1}{1 - (q_p^m)^{-s}} \\
&= \frac{1}{\log q}\frac{d}{ds} \sum_{\substack{P \subset \mathcal{O}_K \\ \text{ideal primo}}} \log(1 - q^{-sm_p}) \\
&= \frac{-1}{\log q}\frac{d}{ds} \sum_{\substack{P \subset \mathcal{O}_K \\ \text{ideal primo}}} \sum_{k=1}^{\infty} \frac{q^{-ksm_p}}{k} \\
&= \sum_{\substack{P \subset \mathcal{O}_K \\ \text{ideal primo}}} \sum_{k=1}^{\infty} \frac{-1}{\log q}\frac{d}{ds}\frac{q^{-ksm_p}}{k} \\
&= \sum_{\substack{P \subset \mathcal{O}_K \\ \text{ideal primo}}} \sum_{k=1}^{\infty} m_p q^{-ksm_p} \\
&= \sum_{n=1}^{\infty} (\sum_{m_p|n} m_p)(q^{-s})^n \\
&= \sum_{n=1}^{\infty} \#C[\mathbb{F}_{q^n}]T^n
\end{aligned}$$

Onde obtemos a igualdade pedida logo de integrar e aplicar exponencial. ■

Assim com este teorema se volta intuitivo definir a função zeta associada a uma variedade Algébrica.

Definição 8. Dada uma variedade algébrica X (afim ou projetiva) definimos a função zeta de Hasse-Weil de X por

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

Notemos que se C_K é a curva associada ao corpo de funções K pelo teorema acima temos $\zeta_K(s) = Z(C_K, q^{-s})$.

Em 1933 Schmidt conseguiu provar por médio da teoria de Riemann-Roch que ζ_K satisfaz uma equação funcional similar à equação funcional da função zeta de Riemann e que é uma função racional na variavel q^{-s}. Mas precisamente

Teorema 3. *Para todo corpo de funções K sua função zeta satisfaz*

1. *(Equação funcional)*
$$\zeta_K(1-s) = q^{(g-1)(2s-1)}\zeta_K(s)$$
onde g é um invariante do corpo de funções chamado o gênero.

2. *(Racionalidade) Existe um polinômio $p \in \mathbb{Z}[x]$ de grau $2g$ (com g o gênero) tal que* $\zeta_K(s) = \frac{p(T)}{(1-T)(1-qT)}$ *onde $T = q^{-s}$*

Prova: ver [1]

Notemos que a racionalidade implica em particular a extensão analítica de $\zeta_K(s)$ a todo o plano complexo.

Vejamos agora como se traduz o Teorema 3 ao formato da função zeta de Hasse-Weil. Não é difícil provar que a equação funcional se traduz em

$$Z(C_K, \frac{1}{qT}) = q^{1-g}T^{2-2g}Z(C_K, T)$$

por outro lado a racionalidade se traduz no caso de variedades gerais na seguinte forma.

Proposición 10. *Dada uma variedade X. $Z(X,T)$ é uma função racional na forma*

$$Z(X,T) = \frac{\prod_{i=1}^{r}(1-\alpha_i T)}{\prod_{j=1}^{s}(1-b_j T)}$$

com $\alpha_i, \beta_j \in \mathbb{C}$ sse

$$\#X[\mathbb{F}_{q^n}] = \sum_{j=1}^{s}\beta_j^n - \sum_{i=1}^{r}\alpha_i^n \quad \forall n \in \mathbb{N}$$

Prova: Temos $\#X[\mathbb{F}_{q^n}] = \sum_{j=1}^{s} \beta_i^n - \sum_{i=1}^{r} \alpha_i^n \iff$

$$\begin{aligned} Z(X,T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\left(\sum_{j=1}^{s} \beta_j^n - \sum_{i=1}^{r} \alpha_i^n\right)}{n} T^n\right) \\ &= \frac{\prod_{j=1}^{s} \exp\left(\sum_{n=1}^{\infty} \frac{(\beta_j T)^n}{n}\right)}{\prod_{i=1}^{r} \exp\left(\sum_{n=1}^{\infty} \frac{(\alpha_i T)^n}{n}\right)} \\ &= \frac{\prod_{j=1}^{s} \exp(-log(1-\beta_j T))}{\prod_{i=1}^{r} \exp(-log(1-\alpha_i T))} \\ &= \frac{\prod_{i=1}^{r}(1-\alpha_i T)}{\prod_{j=1}^{s}(1-\beta_j T)} \end{aligned}$$

Onde temos a equivalência procurada ■

Passemos agora a estudar a Hipótese de Riemann para corpos de funções, esta é dada por

Conjetura 2. (Hipótese de Riemann para Corpos de funções) *Todos os zeros de ζ_K em sua extensão analítica estão na reta $Re(s) = \frac{1}{2}$.*

Usando a parte 2 do Teorema 3 temos a seguinte reformulação da hipótese de Riemann acima.

Proposición 11. *$Re(s) = \frac{1}{2}$ para todo zero de $\zeta_K \iff$ ao expressar $Z(T, C_K) = \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)}$ temos $|\alpha_i| = \sqrt{q}\ \forall i$.*

prova: Notemos que os zeros de ζ_K são os valores de s tais que $1 - \alpha_i q^{-s} = 0$ para algum i, i.e, os zeros estão dados por $s = \frac{\log \alpha_i}{\log q}$ para $i = 1, 2, ..., 2g$.

Logo $|s| = \frac{1}{2}$ para todo zero ssi $|\alpha_i| = \sqrt{q}\ \forall i$. ■

Vejamos agora que este reformulação da hipótese de Riemann nos permite dar uma cota no número de pontos $\#C[\mathbb{F}_{q^n}]$ de uma curva.

Proposición 12. *Assumindo a hipótese de Riemann para curvas temos a seguinte cota para o numero de puntos de uma curva C em $\mathbb{F}_{q^n}$.*

$$|\#C[\mathbb{F}_{q^n}] - q^n - 1| \leq 2g\sqrt{q^n}$$

Prova: Pegando um corpo de funções cuja curva associada seja C temos pela reformulação acima da hipótese de Riemann que $Z(T, C) = \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)}$ com $|\alpha_i| = \sqrt{q}$. Assim pela proposição 8 temos $\#C[\mathbb{F}_{q^n}] = q^n + 1 - \alpha_1^n - ... - \alpha_{2g}^n$ de onde.

$|\#C[\mathbb{F}_{q^n}] - q^n - 1| = |\alpha_1^n + ... + \alpha_{2g}^n| \leq \sum_{i=1}^{2g} |\alpha_i|^n = 2g\sqrt{q^n}$.■

Reciprocamente, assumindo o Teorema 3 e a desigualdade acima é possivel dar uma prova muito simples da hipótese de Riemann em corpos de funções [ver [4] pp. 450]. Assim vemos que esta versão da hipótese de Riemann é equivalente a encontrar aproximações a $\#C[\mathbb{F}_{q^n}]$ do mesmo jeito que a hipótese de Riemann clássica é equivalente a encontrar aproximações da função $\pi(x)$.

A primeira prova da hipótese de Riemann num caso particular foi dada por Hasse em 1931 quem conseguiu provar ela no caso das curvas elípticas. Uma versão moderna dessa prova será dada no capítulo 4.

Mas a primeira prova completa da hipótese de Riemann foi dada por André Weil em 1942. Esta foi basada no teorema de Riemann-Roch, o teorema do índice de Hodge e a desigualdade de Castelnuovo-Severi.

Mais tarde ele deu uma segunda prova usando o morfismo de Frobenius, se cree que esta segunda prova foi o passo crucial para que ele tivesse as ideais precisas para dar com as conjecturas de Weil. Estas ideias são presentadas na secção a seguir.

Capítulo 3

As Conjecturas de Weil

3.1. Motivação

Fixa uma variedade X nos estamos tentando calcular $\#X[\mathbb{F}_{q^n}]$ para diferentes valores de n. Mas como se viu no capítulo 1, um elemento esta em $X[\mathbb{F}_{q^n}]$ sse ele e um ponto fixo do operador Frob : $X \to X$ de expoente q^n. Assim o problema se traduz em um problema de ponto fixo de um operador.

Esto nos leva a pensar na área da topologia algébrica donde se tem o seguinte teorema de Lefschetz para contar o número de pontos fixos de um operador.

Teorema 4. ***(Ponto Fixo de Lefschetz)*** *Seja $f : X \to X$ um mapa continuo de um espaço topológico triangulável em se mesmo tal que o grafo de f é transversal à diagonal em $X \times X$. O número de pontos fixos de f é dado por*

$$\#Fix(f) = \sum_{k=0}^{\dim(X)} (-1)^k Tr(f_* \mid H_k(X, \mathbb{Q}))$$

Onde $Tr(f_* \mid H_k(X, \mathbb{Q}))$ é a traça da transformação linear induzida por f na cohomologia $H_k(X, \mathbb{Q})$ de X.

E simples provar que a o gráfico do automorfismo de Frobenius é transversal à diagonal de $X \times X$. Assim um jeito de calcular $\#X[\mathbb{F}_{q^n}]$ seria provando a existência de uma teoría de cohomologia para a variedade X onde vale o Teorema de ponto fixo de Lefschetz.

Notemos que esto é algo nada trivial já que a variedade X não possui nenhuma topologia de qualidade para poder usar métodos topológicos na construção da cohomologia. Mas pelo momento pensemos de jeito optimista que tal cohomologia existe.

Chamando $\alpha_{i,1}, ..., \alpha_{i,b_j}$ aos auto-valores de $(\text{Frob}_* \mid H_i(X, \mathbb{Q}))$ onde $b_i := \dim(H_i(X, \mathbb{Q}))$ teríamos que os autovalores de $(Frob_* \mid H_i(X, \mathbb{Q}))^n$ são $\alpha_{i,1}^n, ..., \alpha_{i,b_j}^n$, e assim
$Tr((Frob^n)_* \mid H_i(X, \mathbb{Q})) = Tr((Frob_* \mid H_i(X, \mathbb{Q}))^n) = \sum_{j=1}^{b_i} \alpha_{i,j}^n$, logo

$$\begin{aligned} \#X[\mathbb{F}_{q^n}] &= \#Fix(\text{Frob}^n) \\ &= \sum_{i=0}^{\dim(X)} (-1)^i Tr((Frob^n)_* \mid H_i(X, \mathbb{Q})) \\ &= \sum_{i=0}^{\dim(X)} (-1)^i \sum_{j=1}^{b_i} \alpha_{i,j}^n \end{aligned}$$

Assim se $p_j(T) = \prod_{i=0}^{b_j}(1 - \alpha_{i,j}T)$ pela proposição 8 podemos escrever a função zeta de X na forma.

$$\zeta(X, T) = \frac{p_1(T)p_3(T)...p_{2n-1}(T)}{p_0(T)p_2(T)...p_{2d}(T)}$$

Onde $d = \dim(X)$.

Alem disto e esperável pensar que se X é a redução modulo p de uma variedade algébrica complexa definida sobre $\mathbb{Q}$, então as dimensões destas cohomologías em $\bar{\mathbb{F}}_q$ vão a coincidir com as dimensões das cohomologias de X como variedade complexa, i.e, b_i são os números de Betti da variedade.

3.2. Os enunciados das conjecturas

Com á intuição da secção anterior já estamos em condições de enunciar as conjecturas de Weil para variedades algébricas.

Conjetura 3. (Conjecturas de Weil)

Seja X uma variedade algébrica (afim o projetiva) de dimensão n definida sobre o corpo finito $\mathbb{F}_q$. Temos que a função $Z(X, T)$ satisfaz as seguintes propriedades.

- **(Racionalidad)** *Existem polinômios $p, q \in \mathbb{Z}$ tais que $Z(X, T) = \frac{p(T)}{q(T)}$.*
- **(Hipótese de Riemann)** *Existe uma fatoração*

  $$Z(X, T) = \frac{p_1(T)p_3(T)...p_{2n-1}(T)}{p_0(T)p_2(T)...p_{2n}(T)}$$

  Tal que $p_i(T) \in \mathbb{Z}[T] \forall i$, alem disto temos $p_0(T) = 1-T$, $p_{2n}(T) = 1-q^nT$ e para cada $1 \leq i \leq 2n-1$ pomos fatorar p_i sobre $\mathbb{C}$ na forma

  $$p_i(T) = \prod_j (1 - \alpha_{ij}T) com |\alpha_{ij}| = q^{\frac{i}{2}}$$

- **(Equação funcional)** *Existe um inteiro E chamado a característica de Euler de X, tal que*

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

- **(Comparação com homologia singular)** *Se X é a redução modulo p de uma variedade complexa $\tilde{X}$ definida sobre $\mathbb{Q}$ então*

$$\deg p_i(T) = b_i$$

Onde b_i são os números de Betti de $\tilde{X}$ com a topologia euclidiana de $\mathbb{C}$.

3.3. A historia das probas

As teorias de cohomologia que servem para provar as conjecturas de Weil passarão se a chamar cohomologias de Weil. A pesquisa de uma cohomologia de Weil foi um dos problemas mais importantes da Geometria algébrica na segunda metade do seculo 20.

A primeira pessoa em fazer intentos sérios de obter esta cohomologia foi Serre mas seus intentos de Cohomologia com valores nos vetores Witt não tiverem exito.

Sem embargo o mesmo Serre foi quem teve a ideia de trabalhar com a «topologia étale» para definir a cohomologia. Esto ideia abrirão o caminho para a pesquisa do grupo de Grodenthieck que foi os que primeiro acharão uma cohomologia de Weil.

A ideia da construção desta cohomologia, chamada cohomologia etale, é pegar a «topologia etale» e tentar definir um feixe sobre ele para logo definir uma cohomologia de funtor derivado.

Mais precisamente. A topologia Etale é uma categoria associada a variedade X cujos objetos são mapas de recobrimento de X (mapas Etales) por abertos de zariski (complementos de subvariedades algebraicas) de X. Estes mapas Etales se podem pensar como abertos com uma noção de inclusão natural entre eles. Esta categoria com ar de topologia e suficiente para definir sobre ela (com ferramentas categóricas) um feixe de grupos com el cual uno pode obter (usando a teoria de functores derivados) uma cohomología para a variedade. Finalmente pegando um limite inverso sobre diferentes de estas cohomologias obtemos uma cohomologia da variedade com valores a um corpo de característica 0, como se precisa.

Mais e importante mencionar que encontrando uma cohomologia de Weil no fica provada automaticamente a hipótese de Riemann para variedades (a diferencia das demais partes das conjecturas). De fato passaram 10 anos desde que Grothendieck desenvolveu a cohomologia etale ate que Deligne provo a hipótese de Riemann.

Numa linha diferente à seguida por Grothendieck e Deligne temos as provas das conjecturas de Weil por medio de ferramentas do analise p-adico.

O primeiro que uso elas foi Dwork quem conseguiu provar em 1960 a racionalidade da função zeta no caso geral usando uma versão p-adica do teorema de preparação de Weierstrass para provar primeiro (como passo intermédio) que a função zeta da variedade é uma função inteira no sentido p-adico.

Logo no ano 2006 Kedlaya da uma nova prova usando metodos p-adicos da hipótese de Riemann remplazando a cohomologia etale com a cohomologia Rigida e fazendo uso da transformada de Fourier.

Capítulo 4

Provas no caso elíptico

No momento em que Weil formulo suas conjecturas já se tinham provas por Hasse e o mesmo Weil de que elas valiam para curvas elípticas. A ideia de este capítulo é mostrar uma prova disso. Para isto empezaremos introduzindo o conceito de curva elíptica e duas ferramentas muito importante nas provas: O modulo de Tate e o emparelhamento de Weil.

Este capítulo terá um pouco mais de prerrequisito que os capítulos anteriores já que usaremos as noções de limite inverso, anel dos inteiros p-adicos e divisor de uma curva.

Por simplicidade, assumiremos que a característica dos corpos com os que trabalhamos é distinta de 2 e 3.

4.1. Curvas elípticas

As curvas elípticas são uma família de variedades projetivas em $\mathbb{P}^2(K)$ que tem a particularidade de ter uma estrutura de grupo definida entre seus pontos.

Mais especificamente.

Definição 9. Uma curva elíptica é uma variedade algébrica projetiva $E = V(f) \subset \mathbb{P}^2(K)$ onde o polinômio f tem a forma

$$f(x, y, z) = y^2z - x^3 - axz^2 - bz^3$$

Com $a, b \in K$ e $4a^3 + 27b^2 \neq 0$ (esta condição é para que E não seja singular)

Notemos que o polinômio mostrado acima é a homogenização de $f(x, y) = y^2 - x^3 - ax - b$, assim uma curva elíptica é a projetivização de uma variedade afim dada por uma equação do tipo $y^2 = x^3 + ax + b$.

Esta variedade tem um único ponto no infinito (i.e, com z=0), o ponto $(0 : 1 : 0)$. Este punto «no infinito» sera chamado de O.

Temos o seguinte resultado muito importante no qual no podemos aprofundar na prova.

Teorema 5. *Dada uma curva elíptica E, é possível dotar de uma estrutura natural de grupo abeliano a esta de jeito tal que as operações de grupo (suma e inversa) são dada por funções racionais em x e y e o ponto no infinito O e o neutro do grupo.*

Prova: ver [6] III.2

Finalmente vejamos os mapas naturais entre curvas elípticas.

Definição 10. Dadas duas curvas elípticas E_1 e E_2. Uma isogenia $\phi : E_1 \to E_2$ é um mapa que é um morfismo entre os grupos de E_1 e E_2 mas além disto as coordenadas do mapa estão dadas por funções racionais em x, y.

Assim a estrutura de grupo na curva sera a que nos fornecera a ferramente extra para dar uma prova relativamente simples das conjecturas de Weil neste contexto.

4.2. O modulo de Tate

Durante esta secção E será uma curva elíptica definida sobre um corpo K de característica p (por exemplo $K = \mathbb{F}_q$ onde $q = p^n$). Para cada inteiro m, definimos o mapa $[m] : E \to E$ dado por $[m]P = P + ... + P$ m-vezes, este mapa é claramente uma isogenia.

O m-subgrupo de torsao de $E[m]$ é o núcleo deste mapa, isto e, os elementos de ordem no grupo um divisor de m.

$$E[m] = \{P \in E : [m]P = O\}$$

Este é de fato um subgrupo do grupo da curva. Alem disto, note que que se $nk = m$ então temos um morfismo natural de $E[m] \to E[n]$ dado por $P \mapsto [k]P$.

Temos o seguinte teorema sobre a estrutura dos subgrupos de torsao.

Teorema 6. *Seja E uma curva elíptica sobre o corpo K de característica p e $p \nmid m$ um inteiro. Temos*

1. $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$
2. *Uma das seguintes duas cosas acontecem, $E[p^k] = \{O\}$ $\forall k = 1, 2, ...$ ou $E[p^k] = \mathbb{Z}/p^k\mathbb{Z}$ $\forall k = 1, 2, ...$*

Prova: ver [6] III. 6.4

Agora já temos as ferramentas para definir o modulo de Tate.

Definição 11. Para uma curva eliptica E e um número primo l, definimos o moulo de Tate (l-adico) em E pelo limite inverso

$$T_l(E) = \lim_{\leftarrow} E[l^n]$$

Onde o limite esta tomado com respeito aos mapas

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

Esta construção é análoga à construção dos inteiros l-adicos, pelo que não é surpreendente que $T_l(E)$ seja um $\mathbb{Z}_l$-módulo. A ação de $\mathbb{Z}_l$ em $T_l(E)$ extrapola de um jeito natural a ação de $\mathbb{Z}/l^n\mathbb{Z}$ em $E[l^n]$ para cada n.

Temos o seguinte resultado de estrutura para os módulos de Weil proveniente do teorema acima para os grupos de torsao.

Teorema 7. *Se E é uma curva eliptica definida num corpo K de característica p então.*

1. $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ *se* $l \neq char(K)$.
2. $T_l(E) \cong \{O\}$ *o* $\mathbb{Z}_l$ *se* $l = char(K)$

Agora consideremos $End(E)$, o conjunto de isogenias em E. Se $\phi \in End(E)$ e $P \in E[l^n]$ temos

$$[l^n]\phi(P) = \phi([l^n]P) = \phi(O) = O$$

Assim ϕ induz por restrição mapas $\phi : E[l^n] \to E[l^n]$. Alem disto, os mapas comutam com os mapas usados para formar o limite inverso do modulo de Tate. Logo ϕ induz um mapa entre os módulos de Tate.

$$\phi_l : T_l(E) \to T_l(E)$$

Temos que ϕ_l é $\mathbb{Z}_l$-linear. Assim o mapa $\phi \mapsto \phi_l$ nos da um morfismo de anéis entre $End(E)$ e $End(T_l(E))$ (o primeiro conjunto são as isogenias e o segundo são as transformações $\mathbb{Z}_l$-lineares de $T_l(E)$ em si mesmo), este mapa é injetivo e de fato podemos dizer algo ainda mais forte.

Proposición 13. *Seja E uma curva elíptica e $l \neq char(K)$, temos que o mapa natural.*

$$End(E) \otimes \mathbb{Z}_l \to End(T_l(E))$$

é injetivo.

Prova:ver [6] III. 7.4

4.3. O emparelhamento de Weil

Notemos primeiro o seguinte fato sobre divisores na curva eliptica E:

Proposición 14. *Para toda família de inteiros $\{n_P\}_{P\in E}$ o divisor principal*

$$D = \sum n_P P \in Div(E)$$

é principal (isto é, o divisor de alguma função racional) se e só se $D \in Div^0(E)$ (i.e, $\deg(D) = \sum n_P = 0$) e $\sum [n_P]P = O$ no grupo da curva elíptica.

Prova: ver [6] III. 3.5

Seja E uma curva elíptica definida sobre um corpo K de característica p e $m \geq 2$ um inteiro coprimo com p. Para qualquer $T \in E[m]$, sabemos pela proposição acima que existe uma função $f \in \bar{K}(E)$ (o corpo de funções de E) tal que

$$\mathrm{div}(f) = mT - mO$$

De jeito similar, se $T' \in E$ com $[m]T' = T \in E[m]$, existe uma função $g \in \bar{K}(V)$ tal que

$$\mathrm{div}(g) = [m] * (T) - [m] * (O) = \sum_{R\in E[m]} (T' + R) - (R)$$

A função $f \circ [m]$ e g^m tem o mesmo divisor, assim multiplicando por uma constate se é preciso podemos assumir que

$$f \circ [m] = g^m$$

Agora suponha $S \in E[m]$ (S pode ser igual a T). Logo para algum $X \in E$ temos
$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$
Assim pomos definir o emparelhamento de Weil e_m por:

$$e_m : E[m] \times E[m] \to \mu_m$$
$$(S, T) \mapsto \frac{g(X + S)}{g(X)}$$

Onde μ_m é o grupo multiplicativo das raízes da unidade em $\bar{K}$ (note que este grupo é isomorfo ao grupo das raízes da unidade em $\mathbb{C}$ já que m é coprimo com p) e $X \in E$ é qualquer ponto tal que $g(X+S)$ e $g(x)$ estão os dois bem definidos e são não zero.

O emparelhamento de Weil tem as seguintes propriedades importantes.

Proposición 15. *O emparelhamento de Weil é*

1. *Bilinear:*

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$$

2. *Alternado:*

$$e_m(T, T) = 1 \text{ e logo concluimos que } e_m(S, T) = e_m(T, S)^{-1}$$

3. *Não degenerado:*

$$e_m(S, T) = 1 \forall S \Rightarrow T = 0$$

4. *Compatível com* $[m]$*:*

$$e_{mk}(S, T) = e_k([m]S, T)$$

Prova: ver [6] III. 8.1

Como o emparelhamento de Weil esta baseado no m-subgrupo de torsao de E, é natural perguntar-se quando pode ser extendido ao modulo de Tate, que é um limite inverso destes subgrupos. De fato, é possível fazer isto mas primeiro temos que fazer uma construção análoga à construção do módulo de Tate com μ_m para que esteja no lugar do codominio.

Definição 12. Se K é um corpo de característica p e $l \neq p$ definimos o Modulo de Tate (l-adico) do corpo K como o limite inverso

$$T_l(K) = \varprojlim \mu_{l^n}$$

Tomado com respeito aos mapas

$$\mu_{l^{n+1}} \xrightarrow{\pi_l} \mu_{l^n}$$

Dados por $\pi_l(x) = x^l$

Agora notemos que $\pi_l(e_{l^{n+1}}(S, T)) = e_{l^{n+1}}(S, T)^l = e_{l^{n+1}}(S, [l]T) = e_{l^n}([l]S, [l]T)$ $\forall S, T \in E[l^{n+1}]$ onde usamos a linearidade e a compatibilidade na proposição 13. Assim temos que os emparelhamentos de Weil são compatíveis entre eles e logo induzem um emparelhamento de Weil

$$e : T_l(E) \times T_l(E) \to T_l(K)$$

É simples ver tomando limites que o emparelhamento de Weil definido nos módulos de Tate satisfaz todas as propriedades análogas ao proposição 13. Mas precisamente

Proposición 16. *Para toda curva eliptica E e um primo $l \neq p$ o emparelhamento de Weil $e : T_l(V) \times T_l(V) \to T_l(K)$ é bilinear, alternado e não degenerado.*

.

4.4. As provas

Agora temos todas as ferramentas para começar as provas. Seja E uma curva elíptica definida em $\mathbb{F}_q$ onde $q = p^k$. Para todo primo l pomos construir o módulo de Tate $T_l(E)$, temos um mapa injetivo natural $\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_l(E))$ dado por $\phi \mapsto \phi_l$. Alem disto se $l \neq p$ sabemos que

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$$

Pelo tanto podemos escolher uma base $B = \{v_1, v_2\}$ de $T_l(E)$ como $\mathbb{Z}_l$-modulo. O mapa ϕ_l vai ser representado com respeito a esta base como uma matriz de $2x2$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

com coeficientes em $\mathbb{Z}_l$ Escreveremos $\det(\phi_l)$ e $\mathrm{tr}(\phi_l)$ para o determinante e a traça da matriz. E claro que isto é independente da base escolhida.

Agora afirmamos o seguinte.

Proposición 17. *Para todo $\phi \in End(E)$ temos*

$$\det(\phi_l) = \deg(\phi)$$

e

$$tr(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi)$$

Onde $deg(\psi) = \#ker(\psi)$. Em particular temos que $\det(\phi_l)$ e $tr(\phi_l)$ estão em $\mathbb{Z}$ e não dependem de l.

Prova: Pela discussão acima temos $[\phi_l]_B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Agora sabemos que o produto de Weil $e : T_l(E) \times T_l(E) \to T_l(K)$ é bilinear, não degenerado e alternado. Sendo $\hat{\phi}_l$ a isogenia dual de ϕ_l (que se sabe que é a «adjunta» respeito do emparelhamento de Weil) temos

$$\begin{aligned} e(v_1, v_2)^{\deg \phi} &= e([\deg \phi]v_1, v_2) \\ &= e(\hat{\phi}_l \phi_l v_1, v_2) \\ &= e(\phi_l v_1, \phi_l v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det \phi_l} \end{aligned}$$

Finalmente como e é não degenerada concluímos $\deg \phi = \det \phi$.

Para a formula da traca notemos que $1 + \deg(\phi) - \deg(1-\phi) = 1 + det(\phi) - \det(1-\phi) = 1 + (ad - bc) - ((1-a)(1-d) + bc) = a + d = \mathrm{tr}(\phi_l)$ ■

Com estes resultados estabelecidos seja $\mathrm{Frob} : E \to E$ o automorfismo de Frobenius (i.e, $\mathrm{Frob}(x, y) \mapsto (x^q, y^q)$). Pelo visto no capítulo 1 de conceitos prévios, $\mathrm{Fix}(\mathrm{Frob}) = \ker(1 - \mathrm{Frob}) = E[\mathbb{F}_q]$. Isto nos da a formula

$$\deg(1 - \mathrm{Frob}) = \#E[q]$$

Em geral temos $\mathrm{Fix}(\mathrm{Frob}^k) = E[\mathbb{F}_q]$ de onde obtemos a formula $\deg(1 - \mathrm{Frob}^k) = \#E[q^k]$.

Denotemos $\psi := \mathrm{Frob}$. Pela proposição acima o polinômio característico $\xi(T) = \det(1 \cdot T - psi_l)$ tem coeficientes inteiros. Fatorizando ele temos

$$\xi(T) = (T - \alpha)(T - \beta)$$

Para alguns $\alpha, \beta \in \mathbb{C}$. Alem disto, pela mesma proposição temos.

$\det(\frac{m}{n} - \psi_l) = \frac{1}{n^2} \det(m - n\psi_l) = \frac{1}{n^2} \deg(m - n\phi) \geq 0$

Para todo $\frac{m}{n} \in \mathbb{Q}$. Como um polinômio quadrático monico com duas raízes reales distintas deve tomar algum valor negativo. Segue que as raízes de $\xi(T)$ devem ser iguais o complexas conjugadas. Em qualquer caso temos $|\alpha| = |\beta|$.

Mais como $\alpha\beta = \det(\phi_l) = \deg(\phi) = q$ concluímos

$$|\alpha| = |\beta| = \sqrt{q} \qquad (*)$$

Agora como os valores propios de ψ_l^k são as k-potencias dos valores propios de ψ_l temos que o polinômio característico de ψ_l^k debe ser

$$\det(1 \cdot T - \psi_l^k) = (T - \alpha^k)(T - \beta^k)$$

Assim temos

$$\#E[\mathbb{F}_{q^k}] = \deg(1 - \phi^k) = \det(1 - \phi_l^k) = 1 - \alpha^k - \beta^k + q^r \qquad (**)$$

Com esta já temos essencialmente feitas as provas das conjecturas de Weil. Agora recolheremos toda esta informação.

Teorema 8. Conjecturas de Weil, Caso elíptico *Seja E uma curva elíptica definida sobre o corpo $\mathbb{F}_q$. Existe um $a \in \mathbb{Z}$ tal que.*

1. **(Racionalidade)**

$$\zeta(E, T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}$$

2. **(Equação funcional)**

$$\zeta(E, \frac{1}{qT}) = \zeta(E, T)$$

3. **(Hipótese de Riemann)**

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

Onde $|\alpha| = |\beta| = \sqrt{q}$.

Prova:

1. Pela equação (**) temos $\#E[\mathbb{F}_{q^k}] = 1 - \alpha^k - \beta^k + q^r$, assim pela proposição 8 do capítulo 2 obtemos. $Z(E, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-aT+qT}{(1-T)(1-qT)}$
onde $a = \alpha + \beta = \mathrm{tr}(\phi_l)$.

2. Usando que $\alpha\beta = q$ temos.

$$\begin{aligned} Z\left(E, \frac{1}{qT}\right) &= \frac{(1 - \frac{\alpha}{qT})(1 - \frac{\beta}{qT})}{(1 - \frac{1}{qT})(1 - \frac{1}{T})} \\ &= \frac{(\alpha - qT)(\beta - qT)}{(1 - qT)(q - qT)} \\ &= \frac{\alpha\beta}{q} \frac{(1 - \frac{q}{\alpha}T)(1 - \frac{q}{\beta}T)}{(1 - qT)(1 - T)} \\ &= \frac{(1 - \beta T)(1 - \alpha T)}{(1 - qT)(1 - T)} = Z(E, T) \end{aligned}$$

3. Isto foi provado ao momento de provar a equação (*).

A relação com os números de Betti segue direto do fato que uma curva elíptica sobre os complexos tem a topologia de um toro, logo os números de Betti são $b_0 = 1$, $b_1 = 2$ e $b_2 = 1$ que são justamente os graus dos polinômios na fatorização.

Bibliografía

[1] Schmidt, F. K. (1931) *Analytische Zahlentheorie in Körpern der Charakteristik p.*. Math. Zeitschr. 33 1–32.

[2] Weil, A. (1949). *Numbers of Solutions of Equations over Finite Fields*. Bulletin of the American Mathematical Society, 55 (5): 497–508.

[3] Jarden, Fried. (2008). *Field arithmetic, 3rd edition*. Springer.

[4] Hartshorne, R. (1977). *Algebraic geometry* (No. 52). Springer.

[5] Roquette, P. (2003). *The Riemann hypothesis in characteristic p, its origin and development. Part 1 of 4*.

[6] Silverman, J. (2008). *The arithmetic of elliptic curves*. Springer.