

+

+

# **GALOIS REPRESENTATIONS**

**Richard Taylor**

**<http://www.math.harvard.edu/~rtaylor>**

+

1

+

+

## **RATIONAL NUMBERS:**

$$\mathbb{Q} = \{a/b : a, b \text{ integers, } b \neq 0\}$$

## **FUNCTION FIELD:**

$(\mathbb{Z}/p\mathbb{Z})(X)$  rational functions in one variable over a finite field.

## **LOCAL FIELDS:**

e.g.  $\mathbb{Q}_p$

+

2

+

+

## The Riemann Zeta Function:

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} n^{-s} \\ &= \prod_p (1 - p^{-s})^{-1} \quad (\operatorname{Re} s > 1)\end{aligned}$$

**Riemann (1860):**  $\zeta(s)$  has analytic continuation to  $\mathbb{C}$  except for one simple pole at  $s = 1$  and satisfies a functional equation

$$\pi^{-s/2} \Gamma(s/2) \zeta(s) = \pi^{(s-1)/2} \Gamma((1-s)/2) \zeta(1-s)$$

**Herbrand(1932)-Ribet(1976):** If  $n$  is a positive even integer then

$$\zeta(1-n) \in \mathbb{Q}$$

and

$$p \mid \zeta(1-n) \iff \operatorname{Cl}(\mathbb{Z}[e^{2\pi i/p}])[p]_{1-n} \neq (0)$$

+

3

+

+

## Elliptic Curves:

$$E : y^2 = x^3 + ax + b$$

where  $a, b \in \mathbb{Q}$  and  $4a^3 \neq 27b^2$ .

Mordell (1921):

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \oplus \text{finite abelian group}$$

where  $r_E \in \mathbb{Z}_{\geq 0}$  is the rank of  $E$ .

+

4

+

+

**The  $L$ -function:**

$$L(E, s) = \prod_p (1 + a_p(E)p^{-s} + p^{1-2s})^{-1}$$

**for  $\operatorname{Re} s > 3/2$ , where**

$$p + a_p(E) = \#\{(x, y) \in \mathbf{Z}/p\mathbf{Z} : y^2 \equiv x^3 + ax + b \pmod{p}\}$$

**Faltings (1983):  $L(E, s) = L(E', s)$  if and only if  $E$  and  $E'$  are isogenous.**

+

+

+

**Breuil, Conrad, Diamond, Taylor (2000):**  
 $L(E, s)$  has analytic continuation to  $\mathbb{C}$  and  
 satisfies a functional equation

$$N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s) = \\
 WN^{(2-s)/2}(2\pi)^{s-2}\Gamma(2-s)L(E, 2-s)$$

where  $W = \pm 1$  and  $N \in \mathbb{Z}_{>0}$  are constants  
 dependin on  $E$ .

**Birch-Swinnerton-Dyer Conjecture (1963,**  
 now worth \$1,000,000):

The rank  $r_E$  of  $E$  equals the order of van-  
 ishin of  $L(E, s)$  at  $s = 1$ .

**Gross-Zaier (1986), Kolyva in (1989):**  
 True if the order of vanishin is  $\leq 1$ .

+

+

+

$X/\mathbb{Q}$  a smooth projective variety (i.e. can be defined in projective space by polynomials with rational number coefficients)

The ZET FUNCTION of  $X$  is

$$\zeta(X, s) = \prod_p \prod_{x \in X \times \mathbb{Z}/p\mathbb{Z}} (1 - p^{-s \deg x})^{-1}$$

Examples:

$$\zeta(\mathbf{point}, s) = \zeta(s)$$

$$\zeta(E, s) = \zeta(s)\zeta(s-1)/L(E, s)$$

+

7

+

+

In general we expect  $\zeta(X, s)$  to

- have meromorphic continuation to  $\mathbb{C}$ ,
- satisfy a functional equation relating the value at  $s$  to the value at  $1 + \dim X - s$ , and
- encode important arithmetic information about  $X$ .

+



r n i 's :

$$H^i, \overline{l} = H^i, \otimes_{\mathbf{Q}} \overline{l}$$

s n inu us i n  $G_{\mathbf{Q}} = Gal \overline{\phantom{x}}$   
n

$$, s = \underset{i}{H^i}, \overline{l}, s (-1)^i$$

l :

$$, s = s \quad s - 1, s$$

**I :**

=  $a b : a, b$  integers,  $b =$

**I :**

$\bar{\phantom{x}}$  =  $\alpha$  :  $\alpha$  **s is s l n i l**  
**u i n i r i n l i n s**

**I P :**

$G_Q = ut \bar{\phantom{x}}$   
 $= i i ns \bar{\phantom{x}} \rightarrow \bar{\phantom{x}} r s r in , \times$

**i s l r i s -**  
**ilis r r l r i nu r is n.**

usu l r i n s lu lu  
 || = || in u s ri n . -  
 l in i is ri i s l  
 R r l nu rs.

$$\overline{\quad} \hookrightarrow \overline{\mathbf{R}} =$$

$$G_{\mathbf{Q}} \leftrightarrow G_{\mathbf{R}} = ut^{cts} = 1, c$$

r ri - i s lu  
 lu n :

$$|\alpha|_p = {}^{-r} i \alpha = {}^r a b i |ab$$

- i nu rs  $_p =$  l i n r  
 |  $_p$ .

$$\overline{\quad} \hookrightarrow \overline{\quad}_p$$

$$G_{\mathbf{Q}} \leftrightarrow G_{\mathbf{Q}_p} = ut^{cts} \overline{\quad}_p$$

-  $i$  in  $\text{rs } p = I$   $n s \alpha$   $p$   $i$   
 $|\alpha_p|_p = 1$ .

$$p \quad p =$$

$$G_{\mathbb{Q}_p} \twoheadrightarrow G_p = \langle \text{Frob}_p \rangle$$

$$\text{rn } I = I_p = \text{in } r i \quad r u \quad .$$

$$\text{Frob}_p = \text{ri } r \text{ nius } I \text{ n} : \\ \text{Frob}_p \alpha^p = \alpha.$$

$$G_{\mathbb{Q}_p} \subset G_{\mathbb{Q}} \supset 1, c$$

**IV I I P :**

**s ri  $G_{\mathbb{Q}}$  I n i  $G_{\mathbb{Q}_p}, I_p, \text{Frob}_p$  .**  
**insi i .**

relations:

$$H^i, \overline{l} = H^i, \otimes_{\mathbb{Q}} \overline{l}$$

is induced in  $G_{\mathbb{Q}}$  by

$$,s = \sum_i H^i, \overline{l}, s (-1)^i$$

. r n i , 's r l l u n i l  
 n in r i r u  $I_p$  s  
 r i i l l n  $H^i$  ,  $\overline{l}$  i . is 'un-  
 r i ' .

. n in , ssin , l in s ,  
 su i, J n ;  $\sim$  - 5  
 $H^i$  ,  $\overline{l}$  is r r s n-  
 i n  $G_{Q_l}$  n r l i is r s-  
 llin .

. l i n , 4 r r -  
 r i i l n i l  $Frob_p$  n  $H^i$  ,  $\overline{l}$   
 r l = s i n s in  $\overline{n}$  l l  
 i s r s in s l u l u  $i^2$   
 i . is ' ur ' i i .

$\mathbb{I} \overline{V}_l$  is a normal subgroup

$$r : G_{\mathbb{Q}} \longrightarrow G(V)$$

is a normal subgroup of  $G(V)$  and is the kernel of the map  $r : G_{\mathbb{Q}} \longrightarrow G(V)$  in  $V, s$ .

$$p \neq l \text{ et } 1_V - {}^{-s}Frob_p \mid_{V}^{-1}$$

$$\times \text{ si } \text{il } r \text{ est } r \text{ l}$$

in  $e_s$  1  $i$ .

$W$   $n$   $n$   $r$   $ll$

$$\supset \overline{\quad} \subset \overline{\quad}_l.$$

**J** :

u s i s r i ri-  
 . n r is si i n

$$H^i, \overline{\phantom{x}} = \bigoplus_j M_j$$

su r ri l n -  
 in  $\iota : \overline{\phantom{x}} \hookrightarrow \overline{\phantom{x}}_l, M_j \otimes_{\overline{\mathbb{Q}, \iota}} \overline{\phantom{x}}_l$  is n irr -  
 u i l su r r s n i n  $H^i, \overline{\phantom{x}}_l$  .  
 r r

$$M_j \otimes_{\overline{\mathbb{Q}, \iota}} \overline{\phantom{x}}_l, \mathcal{S}$$

is in n n l n  $\iota$  .



**S**

$1, s = 2, s$   
is ul i ris i n  
 $, s = j, s \pm 1$   
i  $j$  irr u i l r r s n i ns .

I -

u s

$r : -$

is n inu us irr u i l r r s n i n  
s is in r r i s . n . n:

•  $i, \overline{l}$  is urs in s

• ls s is s r r .

•  $,s$  is s n l i n inu i n  
ssi l r n si l l  
i i = 1 n s is s n li i  
un i n l u i n r l in ,s  
\*, 1 - s .

. r n i , 's r l l u n i l  
 n in r i r u p s  
 r i l l n <sup>i</sup> , <sup>l</sup> i . is 'un-  
 r i ' .

. n in , ssin , l in s ,  
 su i, n ; ~ -  
<sup>i</sup> , <sup>l</sup> is r r s n-  
 i n <sup>l</sup> n r l i is r s-  
 llin .

. li n , r r -  
 ris i l n i l *rob*<sub>p</sub> n <sup>i</sup> , <sup>l</sup>  
 r l = s i n s in <sup>l</sup> n ll  
 i s r s in s lu lu <sup>i</sup> 2  
 i . is ' ur ' i i .

i s  
ri i s  
r i. .  
i s

l is r r -  
s n i ns  
s is in .  
n .

n ir  
- un i ns  
i

I i I rin I s:

$$= \times_p^p \times_p^p$$

- is r n -

I Y:

$$rt_p : \times_p^p - ab_p \text{ in } i, \text{ ns } i$$

$$rt : \times \times_0^{\sim}$$

$$rt =_x rt_x : \times \times_0 \setminus \times^{\sim} ab$$

:

l r i u s i -  
l u r i  
r r s n i n s  
*n*

irr u i l *n*-  
i n s i n l r -  
r s n i n s

Irr u i l r r s n i n s

$$\pi = \bigotimes_x \pi_x$$

r I I i  
ur in

$$\chi_{,0}^2 \quad n \setminus n ,$$

$$r \quad f \quad h = f \quad h .$$

$$n \setminus n \quad p \quad n \quad p = n \setminus n$$

- $\pi_x: \pi_p \text{ r s } . \pi \text{ is r r s n i n}$   
 $n \quad p \text{ r s } . \quad n \quad .$

- $\chi: f z = \chi z \quad \text{r z} \quad \times_0$

- $: \int_{N( )} N( ) f n \quad dn = \quad \text{r} \quad \text{su} -$   
 $\text{r u}$

$$\binom{m \quad *}{n-m}$$

$n \cdot$

$\pi \text{ is} \quad \text{I} \quad \text{r} \quad \text{i} \quad \pi \text{ is.}$

$$\pi, s = \int_p \pi_p, s$$

X :

1: us i l u r i r r s n i ns  
~ iri l r rs  
× ×

2: ul r l r i us i l u r-  
i r s ~  
us i l l r i ul r r s i  
r n r s.



i s  
ri i s  
r i. .  
i s

l is r r -  
s n i ns  
s is in .  
n .

l r i  
us i l u-  
r i  
r r s n i ns

n ir  
- un i ns  
i

ni u s r I -  
 I = I -  
 I :

- l s s l r 's

- s n n l n s , r ur-  
l z l

- n rs r s il , ... ,  
ll- i s i- ir

- i in r s il s, l r- il s  
, ...

- r u r's r

**I**

*rt* :  $\times \times_0 \times \sim ab$

**r in ll s r 1.**

is n l u r u-  
 r i r s r s r i i n -  
 l i s r r s n i n n n n r l s u -  
 r u i n i l i u i n . s s  
 r r u l .

ss r -  
 u n i n s i r r i s r i s r  
 u r i r r s n i n s .

+ -  
 = i n s i n l r r s n -  
 i n s r i I I I -  
 r s s i u r i r -  
 r s n i n s 2 n r , s i s l -  
 r i .

n l n s, un n ll

I I n r l r :

I r, r' : n l , i r o l = r' o l ,  
i r' ris s r n u r i r r s n -  
i n n i ... n r ls ris s r n  
u r i r r s n i n .

+ n l n s- unn ll = i n -  
si n l r r s n i ns i -  
i +... ris r u r i  
r r s n i ns .

= il s, r uil- nr - i n - l r  
i ur - ni n ur .  
2 3 is r -s lu l

= r , i , il s r 's l s -  
r .

I :

•  $r$  s ul n s l - u l i . r  
is r irin i  $r \sigma x, r \sigma =$   
 $\mu \sigma x, n x, = \mu c , x .$

•  $r$  s ul i is in  
nu rs.

•  $r$  s ul r in r r r s llin i  
nu rs s ll r l i l.

•  $r$  o l s ul l r i ?

• i r = ?

,

I r is r r s n i n ni r u  
 n r r nil n su r u s i,  
 r rs i i n in rs n<sub>i</sub> su

$$r = \sum_i n_i n \frac{G}{H_i} i.$$

I I I : I r is r r s n-  
 i n i I I I n  
 r, s s r r i n inu i n n  
 .

$$r, s = \sum_i n \frac{G}{H_i} i, s n_i$$

$$= \sum_i i, s n_i$$

$$: I \quad i \quad r = , \quad r \quad p = 1 \quad r$$

$$n \quad r \quad is \quad r \quad s \quad llin \quad i \quad -$$
 nu 
$$rs \quad n_1, n_2 \quad s \quad is \quad in$$

$$< |n_1 - n_2| < l - 1$$

$$n \quad r \quad is \quad ur \quad n \quad r, s \quad s \quad r \quad r -$$

$$i \quad n \quad inu \quad i \quad n \quad n \quad s \quad is \quad s$$

$$un \quad i \quad n \quad l \quad u \quad i \quad n.$$

$$: \quad - \quad un \quad i \quad n \quad n \quad r \quad -$$

$$ul \quad r \quad is \quad in \quad nu \quad rs \quad r \quad n \quad -$$

$$i \quad s \quad r \quad r \quad i \quad n \quad inu \quad i \quad n$$

$$n \quad s \quad is \quad s \quad un \quad i \quad n \quad l \quad u \quad -$$

$$i \quad n.$$



:

I is ri i i. . 2,1 , =  
l i- u - l n ,s s r -  
r i n inu i n n s is s  
. . r l in ,s n , -  
s .

# I

:  $r$  o l s r  
n u r i r r s l is -  
ll r l l . is n n us s  
ll in r .

r si i n r - ill , : u s  
is s n ri ll n-  
n n =  $\emptyset$ . n r is  
in  $x$  — ll s n u s li in  
.

Q I : n x s n in s l-  
u l nsi n

$r$  :  $r$  s r n u-  
 $r$  i r r s l is ll  
 $r$  l l li in r .

$r$  : u r s n  
 $r$  s r n u r i r n n  
 in r i l  $K_i$  i  $K_i$  s lu-  
 l .

: s r u r ri

$$1 = \sum_i n_i n \frac{\text{al}(F)}{\text{al}(F K_i)} i$$

s

$$r = \sum_i n_i n \frac{Q}{K_i} r |_{K_i} i$$

n

$$r, s = \sum_i r |_{K_i} i, s^{n_i}.$$

$n$   $n$  is r ni - lu

$n$   $n$   $n$   $p$  =  $n$   $n$   
 $p$

**I** :  $\times_0$   $\times$  **n**

$\chi, 0$   $n$   $n$  =  $\pi$

is s i-si l r r s n i n

=

$n$  , s irr u i l ns i u n s

$$\pi = \int_x \pi_x$$

r II I I I  
I .