The functional equation for L-functions of hyperelliptic curves

Jahrestagung SPP 1489, Osnabrück

Michel Börner

Ulm University

September 30, 2015

Setup

Y smooth projective curve over $\mathbb{Q}$ (number field)

Setup

Y	smooth projective curve over $\mathbb{Q}$ (number field)
	for fixed $p \in \mathbb{Q}$ and a model $\mathcal{Y}$ of Y define:
$\bar{Y}$	special fiber, $\bar{Y} = \mathcal{Y} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$

Setup

Y	smooth projective curve over $\mathbb{Q}$ (number field)
	for fixed $p \in \mathbb{Q}$ and a model $\mathcal{Y}$ of Y define:
$\bar{Y}$	special fiber, $\bar{Y} = \mathcal{Y} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$
$L(Y,s)$	L series, $L(Y,s) = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s} = \prod_p L_p(Y,s)$

Setup

Y	smooth projective curve over $\mathbb{Q}$ (number field)
	for fixed $p \in \mathbb{Q}$ and a model $\mathcal{Y}$ of Y define:
$\bar{Y}$	special fiber, $\bar{Y} = \mathcal{Y} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$
$L(Y,s)$	L series, $L(Y,s) = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s} = \prod_p L_p(Y,s)$
g	genus $g = g(Y)$
N	conductor, $N = \prod_p p^{f_p}$

Functional Equation

Conjectured functional equation

$$\Lambda(Y,s) = \pm\Lambda(Y,2-s) \qquad \textbf{(FEq)}$$

where $\Lambda(Y,s) = \sqrt{N}^s \cdot (2\pi)^{-gs} \cdot \Gamma(s)^g \cdot L(Y,s)$

For elliptic curves $/\mathbb{Q}$ this is the modularity theorem (Wiles)

Functional Equation

Conjectured functional equation

$$\Lambda(Y,s) = \pm\Lambda(Y,2-s) \qquad \textbf{(FEq)}$$

where $\Lambda(Y,s) = \sqrt{N}^s \cdot (2\pi)^{-gs} \cdot \Gamma(s)^g \cdot L(Y,s)$

For elliptic curves $/\mathbb{Q}$ this is the modularity theorem (Wiles)

Using `Dokchitser` package in *sage* [D04]

- **(FEq)** may be verified numerically (to a high probability) using all $a_n \leq M \sim \sqrt{N}$.

Functional Equation

Conjectured functional equation

$$\Lambda(Y,s) = \pm\Lambda(Y,2-s) \qquad \textbf{(FEq)}$$

where $\Lambda(Y,s) = \sqrt{N}^s \cdot (2\pi)^{-gs} \cdot \Gamma(s)^g \cdot L(Y,s)$

For elliptic curves $/\mathbb{Q}$ this is the modularity theorem (Wiles)

Using `Dokchitser` package in *sage* [D04]

- **(FEq)** may be verified numerically (to a high probability) using all $a_n \leq M \sim \sqrt{N}$.
- $\sum_n \frac{a_n}{n^s} = \prod_p L_p(Y,s) \rightsquigarrow$ need sufficiently many local factors L_p

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists
- *semistable reduction:* $\bar{Y}$ has at most ordinary double points

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists
- *semistable reduction:* $\bar{Y}$ has at most ordinary double points

Good p:

- $\bar{Y}$ is curve given by equation mod p

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists
- *semistable reduction:* $\bar{Y}$ has at most ordinary double points

Good p:

- $\bar{Y}$ is curve given by equation mod p
- $L_p(Y,s)^{-1}$ = numerator of zeta fctn. of $\bar{Y} = P(\bar{Y}, T = p^{-s})$

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists
- *semistable reduction:* $\bar{Y}$ has at most ordinary double points

Good p:

- $\bar{Y}$ is curve given by equation mod p
- $L_p(Y,s)^{-1}$ = numerator of zeta fctn. of $\bar{Y} = P(\bar{Y}, T = p^{-s})$
- $P(\bar{Y},T) = 1 + c_1 T + \ldots + c_{2g} T^{2g}$ (Weil conjectures)

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists
- *semistable reduction:* $\bar{Y}$ has at most ordinary double points

Good p:

- $\bar{Y}$ is curve given by equation mod p
- $L_p(Y,s)^{-1}$ = numerator of zeta fctn. of $\bar{Y} = P(\bar{Y}, T = p^{-s})$
- $P(\bar{Y},T) = 1 + c_1 T + \ldots + c_{2g} T^{2g}$ (Weil conjectures)
- c_i: point counting on $\bar{Y}$

Good and bad primes

Good, bad and semistable reduction at a prime

- *good reduction:* $\exists$ model $\mathcal{Y}$ of Y with $\bar{Y}$ smooth
- *bad reduction:* no such $\mathcal{Y}$ exists
- *semistable reduction:* $\bar{Y}$ has at most ordinary double points

Good p:

- $\bar{Y}$ is curve given by equation mod p
- $L_p(Y,s)^{-1}$ = numerator of zeta fctn. of $\bar{Y} = P(\bar{Y}, T = p^{-s})$
- $P(\bar{Y},T) = 1 + c_1 T + \ldots + c_{2g} T^{2g}$ (Weil conjectures)
- c_i: point counting on $\bar{Y}$
- $f_p = 0$ $\rightsquigarrow$ no contribution to conductor N

Good and bad primes ctd.

Bad p:

- L_p, f_p depend on Galois representation on $H^1_{\text{et}}(Y_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$

Good and bad primes ctd.

Bad p:

- L_p, f_p depend on Galois representation on $H^1_{\mathrm{et}}(Y_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$
- First compute *semistable reduction* of Y at p

Fact (Deligne–Mumford):

Y has semistable reduction over some finite extension of $\mathbb{Q}_p$

Good and bad primes ctd.

Bad p:

- L_p, f_p depend on Galois representation on $H^1_{\text{et}}(Y_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$
- First compute *semistable reduction* of Y at p

Fact (Deligne–Mumford):

Y has semistable reduction over some finite extension of $\mathbb{Q}_p$

- Algorithm for all bad L_p, f_p for certain types of curves using methods in [BW15]

Good and bad primes ctd.

Bad p:

- L_p, f_p depend on Galois representation on $H^1_{\text{et}}(Y_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$
- First compute *semistable reduction* of Y at p

Fact (Deligne–Mumford):

Y has semistable reduction over some finite extension of $\mathbb{Q}_p$

- Algorithm for all bad L_p, f_p for certain types of curves using methods in [BW15]

Next: Class of hyperelliptic curves over $\mathbb{Q}$
with semistable reduction everywhere

Hyperelliptic curves with semistable red. at all p

Hyperelliptic setup ($p \neq 2$ case)

$g, h \in \mathbb{Z}_p[x]$, g monic, $\deg g = 2g(Y) + 1$, $\deg h \leq g(Y)$, $\gcd(f, f') = 1$

$$Y: \quad y^2 + h(x)y = g(x)$$

$$\Longleftrightarrow \qquad y^2 = f(x) = 4g(x) + h(x)^2$$

Hyperelliptic curves with semistable red. at all p

Hyperelliptic setup ($p \neq 2$ case)

$g, h \in \mathbb{Z}_p[x]$, g monic, $\deg g = 2g(Y) + 1$, $\deg h \leq g(Y)$, $\gcd(f, f') = 1$

$$Y: \quad y^2 + h(x)y = g(x)$$
$$\iff \qquad y^2 = f(x) = 4g(x) + h(x)^2$$

Fact ($p \neq 2$ case)

Y has semistable reduction already over $\mathbb{Q}_p$

$\iff \bar{Y}: y^2 = \bar{f}(x) = r^2(x) \cdot s(x)$

with $r, s \in \mathbb{F}_p[x]$ separable & coprime

Hyperelliptic curves with semistable red. at all p

Hyperelliptic setup ($p \neq 2$ case)

$g, h \in \mathbb{Z}_p[x]$, g monic, $\deg g = 2g(Y) + 1$, $\deg h \leq g(Y)$, $\gcd(f, f') = 1$

$$Y: \quad y^2 + h(x)y = g(x)$$

$$\iff \qquad y^2 = f(x) = 4g(x) + h(x)^2$$

Fact ($p \neq 2$ case)

Y has semistable reduction already over $\mathbb{Q}_p$

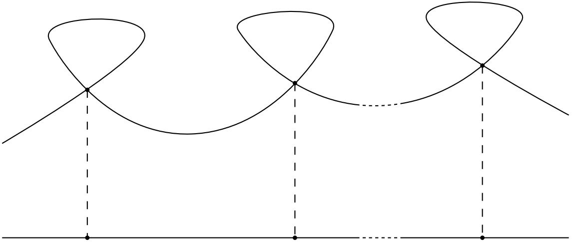
$\iff$ $\bar{Y} : y^2 = \bar{f}(x) = r^2(x) \cdot s(x)$

with $r, s \in \mathbb{F}_p[x]$ separable & coprime

$\boldsymbol{p = 2}$ **:** A little more work

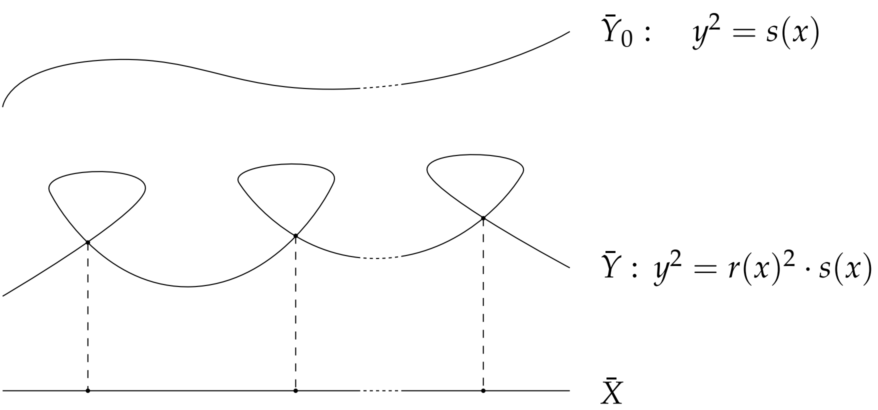
Computations at bad primes $p \neq 2$

$$\bar{Y} : y^2 = r^2(x) \cdot s(x)$$



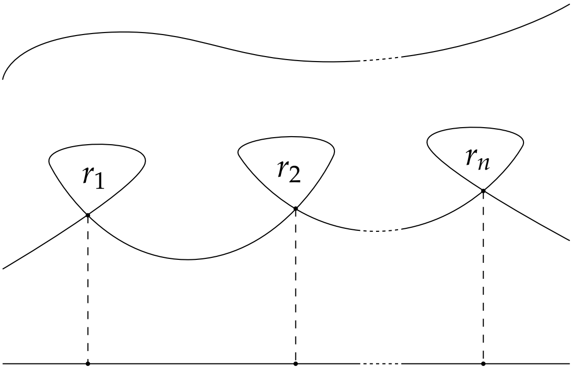
Computations at bad primes $p \neq 2$

$$\bar{Y}: \; y^2 = r^2(x) \cdot s(x)$$



Computations at bad primes $p \neq 2$

$$\bar{Y} : y^2 = r^2(x) \cdot s(x)$$



$\bar{Y}_0 : \quad y^2 = s(x)$

$\bar{Y} : y^2 = r(x)^2 \cdot s(x)$

$r = \prod_i r_i \in \mathbb{F}_p[x]$

$\bar{X}$

Algorithm

Bad primes

- Exponent $f_p = \#\text{loops} = \sum_i \deg(r_i)$

Algorithm

Bad primes

- Exponent $f_p = \#\text{loops} = \sum_i \deg(r_i)$
- Nodes have *split* or *non-split* reduction and

$$L_p(Y, T = p^{-s}) = \frac{L_p(\bar{Y}_0, T)}{\prod_i (1 \pm T^{d_i})}$$

with $d_i = \deg(r_i)$.

Algorithm

Bad primes

- Exponent $f_p = \#\text{loops} = \sum_i \deg(r_i)$
- Nodes have *split* or *non-split* reduction and

$$L_p(Y, T = p^{-s}) = \frac{L_p(\bar{Y}_0, T)}{\prod_i (1 \pm T^{d_i})}$$

  with $d_i = \deg(r_i)$.
- $L_p(\bar{Y}_0, T)$: Just point counting on $\bar{Y}_0$

Algorithm

Bad primes

- Exponent $f_p = \#\text{loops} = \sum_i \deg(r_i)$
- Nodes have *split* or *non-split* reduction and

$$L_p(Y, T = p^{-s}) = \frac{L_p(\bar{Y}_0, T)}{\prod_i (1 \pm T^{d_i})}$$

with $d_i = \deg(r_i)$.

- $L_p(\bar{Y}_0, T)$: Just point counting on $\bar{Y}_0$

Point counting (good/bad p): Just for $p^k \leq M$ where $M \sim \sqrt{N}$

Example

$$Y: y^2 + h(x)y = g(x)$$

$$g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$$

$$h = -x^3 + x^2 + x + 2$$

Example

$$Y: \; y^2 + h(x)y = g(x) \quad \overset{p\neq 2}{\Longrightarrow} \quad \bar{Y}: \quad y^2 = r^2(x)\cdot s(x)$$

$$g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$$

$$h = -x^3 + x^2 + x + 2 \qquad \text{bad } p\text{: } 2, 3, 11, 37 \qquad g(Y) = 3$$

Example

$$Y: \; y^2 + h(x)y = g(x) \quad \overset{p \neq 2}{\Longrightarrow} \quad \bar{Y}: \quad y^2 = r^2(x) \cdot s(x)$$

$$g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$$

$$h = -x^3 + x^2 + x + 2$$

bad p: $2, 3, 11, 37$

$$g(Y) = 3$$

$p = 3$:

$$\bar{Y}: \quad y^2 = (x+1)^2 \cdot (x^2+1)^2 \cdot x$$

Example

$$Y: \; y^2 + h(x)y = g(x) \quad \overset{p \neq 2}{\Longrightarrow} \quad \bar{Y}: \quad y^2 = r^2(x) \cdot s(x)$$

$$g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$$

$$h = -x^3 + x^2 + x + 2 \qquad \text{bad } p\text{: } 2, 3, 11, 37 \qquad g(Y) = 3$$

$\boldsymbol{p = 3}$**:**

$$\bar{Y}: \quad y^2 = (x+1)^2 \cdot (x^2+1)^2 \cdot x$$

$$L_3(T)^{-1} = \frac{\prod_i (1 \pm T^{d_i})}{L_3(\bar{Y}_0, T)} = (1+T) \cdot (1 - T^2)/1$$

$$f_3 = \deg(r) = 3$$

Example

$$Y:\ y^2 + h(x)y = g(x) \quad \overset{p\neq 2}{\Longrightarrow} \quad \bar{Y}: \quad y^2 = r^2(x)\cdot s(x)$$

$$g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$$

$h = -x^3 + x^2 + x + 2$ bad p: $2, 3, 11, 37$ $g(Y) = 3$

$p = 3$:

$$\bar{Y}: \quad y^2 = (x+1)^2 \cdot (x^2+1)^2 \cdot x$$

$$L_3(T)^{-1} = \frac{\prod_i (1 \pm T^{d_i})}{L_3(\bar{Y}_0, T)} = (1+T)\cdot(1-T^2)/1$$

$$f_3 = \deg(r) = 3$$

$p = 11, 37$: similar

Example

$$Y: \; y^2 + h(x)y = g(x) \quad \overset{p \neq 2}{\Longrightarrow} \quad \bar{Y}: \quad y^2 = r^2(x) \cdot s(x)$$

$$g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$$

$$h = -x^3 + x^2 + x + 2 \qquad \text{bad } p\text{: } 2, 3, 11, 37 \qquad g(Y) = 3$$

$\boldsymbol{p = 3:}$

$$\bar{Y}: \quad y^2 = (x+1)^2 \cdot (x^2+1)^2 \cdot x$$

$$L_3(T)^{-1} = \frac{\prod_i (1 \pm T^{d_i})}{L_3(\bar{Y}_0, T)} = (1+T) \cdot (1 - T^2)/1$$

$$f_3 = \deg(r) = 3$$

$\boldsymbol{p = 11, 37:}$ similar

$\boldsymbol{p = 2:}$ more work

Example ctd.

Other primes:

$$L_2^{-1} = (1 - T^2) \cdot (1 - T + 2T^2) \qquad f_2 = 2$$

$$L_{11}^{-1} = (1 + T)^2 \cdot (1 - 4T + 11T^2) \qquad f_{11} = 2$$

$$L_{37}^{-1} = (1 - T) \cdot (1 + \ldots + 37^2 T^4) \qquad f_{37} = 1$$

Example ctd.

Other primes:

$$L_2^{-1} = (1 - T^2) \cdot (1 - T + 2T^2) \qquad f_2 = 2$$

$$L_{11}^{-1} = (1 + T)^2 \cdot (1 - 4T + 11T^2) \qquad f_{11} = 2$$

$$L_{37}^{-1} = (1 - T) \cdot (1 + \ldots + 37^2 T^4) \qquad f_{37} = 1$$

Conductor N:

$$N = 2^2 \cdot 3^3 \cdot 11^2 \cdot 37 \approx 500\,000$$

Example ctd.

Other primes:

$$L_2^{-1} = (1-T^2)\cdot(1-T+2T^2) \qquad f_2 = 2$$
$$L_{11}^{-1} = (1+T)^2\cdot(1-4T+11T^2) \qquad f_{11} = 2$$
$$L_{37}^{-1} = (1-T)\cdot(1+\ldots+37^2T^4) \qquad f_{37} = 1$$

Conductor N:

$$N = 2^2\cdot 3^3\cdot 11^2\cdot 37 \approx 500\,000$$

Point counting:

$$\#\text{points of } \bar{Y}/\mathbb{F}_{p^k} \text{ for } p^k \le 15\,000$$

Example ctd.

Other primes:

$$L_2^{-1} = (1 - T^2) \cdot (1 - T + 2T^2) \qquad f_2 = 2$$
$$L_{11}^{-1} = (1 + T)^2 \cdot (1 - 4T + 11T^2) \qquad f_{11} = 2$$
$$L_{37}^{-1} = (1 - T) \cdot (1 + \ldots + 37^2 T^4) \qquad f_{37} = 1$$

Conductor N:

$$N = 2^2 \cdot 3^3 \cdot 11^2 \cdot 37 \approx 500\,000$$

Point counting:

$$\#\text{points of } \bar{Y}/\mathbb{F}_{p^k} \text{ for } p^k \leq 15\,000$$

Verification of (**FEq**) via `Dokchitser` package in *sage*: ✓

Overview and loose ends

Hyperelliptic curves

- All L_p, f_p computable for $g = 2, 3, 4, 5, 6$ with reasonable effort

  Limitation: point count for good $p \sim \sqrt{N} = \prod_{\text{bad } p} p^{f_p/2}$

Overview and loose ends

Hyperelliptic curves

- All L_p, f_p computable for $g = 2, 3, 4, 5, 6$ with reasonable effort
  Limitation: point count for good $p \sim \sqrt{N} = \prod_{\text{bad } p} p^{f_p/2}$
- (**FEq**) verified for hundreds of examples, N up to 10^{10} [B15]

Overview and loose ends

Hyperelliptic curves

- All L_p, f_p computable for $g = 2, 3, 4, 5, 6$ with reasonable effort
  Limitation: point count for good $p \sim \sqrt{N} = \prod_{\text{bad } p} p^{f_p/2}$
- (**FEq**) verified for hundreds of examples, N up to 10^{10} [B15]

Superelliptic curves

$$Y : \; y^n = f(x)$$

- Find algorithms for L_p and f_p for wider range of curves

Overview and loose ends

Hyperelliptic curves

- All L_p, f_p computable for $g = 2, 3, 4, 5, 6$ with reasonable effort
  Limitation: point count for good $p \sim \sqrt{N} = \prod_{\text{bad } p} p^{f_p/2}$
- (**FEq**) verified for hundreds of examples, N up to 10^{10} [B15]

Superelliptic curves

$$Y : \; y^n = f(x)$$

- Find algorithms for L_p and f_p for wider range of curves
- Find (all) curves of certain class with small N (in preparation)

Thank you!

[BW15] *Computing L-functions and semistable reduction of superelliptic curves,* Irene Bouw and Stefan Wewers. To appear in Glasgow Math. J.

[BBW15] *The functional equation for L-functions of hyperelliptic curves,* Michel Börner, Irene I. Bouw, Stefan Wewers, arXiv:1504.00508

[B15] *Examples of [BBW15],* M.B., `https://www.uni-ulm.de/index.php?id=64504`

[D04] *Computing special values of motivic L-functions,* Tim Dokchitser, Exper. Math. 13, No. 2 (2004), 137-149