p-adic L-function in Sage

Christian Wuthrich

March 22, 2016

A good ordinary example

Let E be the following curve

```
sage : e = EllipticCurve('446d1'); p=5; show(e)
```

$$y^2 + xy = x^3 - x^2 - 4x + 4$$

A good ordinary example

Let E be the following curve

```
sage : e = EllipticCurve('446d1'); p=5; show(e)
```

$$y^2 + xy = x^3 - x^2 - 4x + 4$$

It has rank 2 and good ordinary reduction at $p = 5$.

```
sage : e.rank()
```

$$2$$

```
sage : e.is_ordinary(p)
```

True

But it has anomalous reduction

```
sage : e.Np(p)
```

$$10$$

But it has anomalous reduction

```
sage : e.Np(p)
```

$$10$$

with Tamagawa numbers

```
sage : e.tamagawa_numbers()
```

$$[2, 1]$$

But it has anomalous reduction

```
sage : e.Np(p)
```

$$10$$

with Tamagawa numbers

```
sage : e.tamagawa_numbers()
```

$$[2, 1]$$

and no torsion point in $E(\mathbb{Q})$.

```
sage : tors= e.torsion_order();tors
```

$$1$$

The p-adic L-function is approximated by

```
sage : lp = e.padic_lseries(p);lps =
lp.series(5,prec=7);lps
```

$$O(5^7) + O(5^4) \cdot T + (5 + 5^2 + 3 \cdot 5^3 + O(5^4)) \cdot T^2$$
$$+(2 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^3 + O(5^4)) \cdot T^3$$
$$+(4 \cdot 5^2 + 4 \cdot 5^3 + O(5^4)) \cdot T^4$$
$$+(4 \cdot 5 + 4 \cdot 5^2 + O(5^3)) \cdot T^5$$
$$+(1 + 2 \cdot 5 + 5^2 + O(5^3)) \cdot T^6 + O(T^7)$$

The p-adic L-function is approximated by

```
sage : lp = e.padic_lseries(p);lps =
lp.series(5,prec=7);lps
```

$$O(5^7) + O(5^4) \cdot T + (5 + 5^2 + 3 \cdot 5^3 + O(5^4)) \cdot T^2$$
$$+(2 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^3 + O(5^4)) \cdot T^3$$
$$+(4 \cdot 5^2 + 4 \cdot 5^3 + O(5^4)) \cdot T^4$$
$$+(4 \cdot 5 + 4 \cdot 5^2 + O(5^3)) \cdot T^5$$
$$+(1 + 2 \cdot 5 + 5^2 + O(5^3)) \cdot T^6 + O(T^7)$$

- Here we used a Riemann sum on $\mathbb{Z}_p^\times = \bigsqcup (a + p^5\mathbb{Z}_p)$.

The p-adic L-function is approximated by

```
sage : lp = e.padic_lseries(p);lps =
lp.series(5,prec=7);lps
```

$$O(5^7) + O(5^4)\cdot T + (5 + 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^2$$
$$+(2\cdot 5 + 3\cdot 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^3$$
$$+(4\cdot 5^2 + 4\cdot 5^3 + O(5^4))\cdot T^4$$
$$+(4\cdot 5 + 4\cdot 5^2 + O(5^3))\cdot T^5$$
$$+(1 + 2\cdot 5 + 5^2 + O(5^3))\cdot T^6 + O(T^7)$$

- Here we used a Riemann sum on $\mathbb{Z}_p^\times = \bigsqcup (a + p^5\mathbb{Z}_p)$.
- We have $\operatorname{ord}_{T=0} \mathcal{L}_p(E,T) \leqslant 2$.

The p-adic L-function is approximated by

```
sage : lp = e.padic_lseries(p);lps =
lp.series(5,prec=7);lps
```

$$O(5^7) + O(5^4)\cdot T + (5 + 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^2$$
$$+(2\cdot 5 + 3\cdot 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^3$$
$$+(4\cdot 5^2 + 4\cdot 5^3 + O(5^4))\cdot T^4$$
$$+(4\cdot 5 + 4\cdot 5^2 + O(5^3))\cdot T^5$$
$$+(1 + 2\cdot 5 + 5^2 + O(5^3))\cdot T^6 + O(T^7)$$

- Here we used a Riemann sum on $\mathbb{Z}_p^\times = \bigsqcup (a + p^5\mathbb{Z}_p)$.
- We have $\operatorname{ord}_{T=0} \mathcal{L}_p(E, T) \leqslant 2$.
- The leading term has valuation 1.

The p-adic L-function is approximated by

```
sage : lp = e.padic_lseries(p);lps =
lp.series(5,prec=7);lps
```

$$O(5^7) + O(5^4)\cdot T + (5 + 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^2$$
$$+(2\cdot 5 + 3\cdot 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^3$$
$$+(4\cdot 5^2 + 4\cdot 5^3 + O(5^4))\cdot T^4$$
$$+(4\cdot 5 + 4\cdot 5^2 + O(5^3))\cdot T^5$$
$$+(1 + 2\cdot 5 + 5^2 + O(5^3))\cdot T^6 + O(T^7)$$

- Here we used a Riemann sum on $\mathbb{Z}_p^\times = \bigsqcup (a + p^5\mathbb{Z}_p)$.
- We have $\mathrm{ord}_{T=0}\,\mathcal{L}_p(E,T) \leqslant 2$.
- The leading term has valuation 1.
- The sixth coefficient is a unit.

The p-adic regulator

$$\mathrm{Reg}_p(E/\mathbb{Q})/\log(\gamma)^2$$

evaluates to

The p-adic regulator

$$\mathrm{Reg}_p(E/\mathbb{Q})/\log(\gamma)^2$$

evaluates to

```
sage : reg = e.padic_regulator(p);R =
Qp(p,10);lg = log(R(1+p));reg = R(reg)/lg^2;reg
```

$$2\cdot 5^{-1}+4+3\cdot 5+2\cdot 5^2+5^4+5^5+2\cdot 5^6+3\cdot 5^7+O(5^8)$$

The p-adic regulator

$$\mathrm{Reg}_p(E/\mathbb{Q})/\log(\gamma)^2$$

evaluates to

```
sage : reg = e.padic_regulator(p);R =
Qp(p,10);lg = log(R(1+p));reg = R(reg)/lg^2;reg
```

$$2\cdot 5^{-1}+4+3\cdot 5+2\cdot 5^2+5^4+5^5+2\cdot 5^6+3\cdot 5^7+O(5^8)$$

Its valuation is -1; that is minimal for anomalous primes.

The p-adic regulator

$$\mathrm{Reg}_p(E/\mathbb{Q})/\log(\gamma)^2$$

evaluates to

```
sage : reg = e.padic_regulator(p);R =
Qp(p,10);lg = log(R(1+p));reg = R(reg)/lg^2;reg
```

$$2\cdot 5^{-1}+4+3\cdot 5+2\cdot 5^2+5^4+5^5+2\cdot 5^6+3\cdot 5^7+O(5^8)$$

Its valuation is -1; that is minimal for anomalous primes.
Kedlaya !!!!

Putting things together

```
sage : eps = (1-1/lp.alpha())^2;
lps[2]/eps/reg/e.tamagawa_product()*tors^2
```

$$1 + O(5^3)$$

Putting things together

```
sage : eps = (1-1/lp.alpha())^2;
lps[2]/eps/reg/e.tamagawa_product()*tors^2
```

$$1 + O(5^3)$$

- So $Ш(E/\mathbb{Q})[5^\infty] = 0$.

Putting things together

```
sage : eps = (1-1/lp.alpha())^2;
lps[2]/eps/reg/e.tamagawa_product()*tors^2
```

$$1 + O(5^3)$$

- So $\text{Ш}(E/\mathbb{Q})[5^\infty] = 0$.
- The p-adic BSD predicts $\#\text{Ш}(E/\mathbb{Q}) \equiv 1 \pmod{125}$.

Putting things together

```
sage : eps = (1-1/lp.alpha())^2;
lps[2]/eps/reg/e.tamagawa_product()*tors^2
```

$$1 + O(5^3)$$

- So $Ш(E/\mathbb{Q})[5^\infty] = 0$.
- The p-adic BSD predicts $\#Ш(E/\mathbb{Q}) \equiv 1 \pmod{125}$.

```
sage : e.sha().an_padic(5,prec=7)
```

$$1 + O(5^5)$$

Actually we have

$$\mathcal{L}_5(E,T) = T \cdot \big((T+1)^5 - 1\big) \cdot u$$

for some unit $u \in \Lambda^\times$.

Actually we have

$$\mathcal{L}_5(E,T) = T \cdot \left((T+1)^5 - 1\right) \cdot u$$

for some unit $u \in \Lambda^\times$. It tells us $\mu = 0$ and $\lambda = 6$, but more

Actually we have

$$\mathcal{L}_5(E,T) = T \cdot \left((T+1)^5 - 1\right) \cdot u$$

for some unit $u \in \Lambda^\times$. It tells us $\mu = 0$ and $\lambda = 6$, but more

- $\mathrm{rank}(E(K_n)) = 2 + 4 = 6$ for all $n > 0$ and

Actually we have

$$\mathcal{L}_5(E,T) = T \cdot \left((T+1)^5 - 1\right) \cdot u$$

for some unit $u \in \Lambda^\times$. It tells us $\mu = 0$ and $\lambda = 6$, but more

- $\operatorname{rank}(E(K_n)) = 2 + 4 = 6$ for all $n > 0$ and
- $Ш(E/K_n)[5^\infty]$ is finite of bounded order.

Further examples

389a1	5	$1 + O(5^5)$
389a1	7	$1 + O(7^5)$
389a1	11	$1 + O(11^5)$
389a1	13	$1 + O(13^3)$
389a1	17	$1 + O(17^3)$
389a1	19	$1 + O(19^3)$
433a1	5	$1 + O(5^5)$
433a1	7	$1 + O(7^5)$
433a1	11	$1 + O(11^3)$
433a1	13	$1 + O(13^2)$
433a1	17	$1 + O(17^3)$
433a1	19	$1 + O(19^3)$
446d1	5	$1 + O(5^4)$
446d1	7	$1 + O(7^4)$
446d1	11	$1 + O(11^3)$
446d1	13	$1 + O(13^3)$
446d1	17	$1 + O(17^3)$

. . . and then

```
sage : e.sha().an_padic(19)
```

$$1 + O(19)$$

gives a warning:
/usr/local/sage/. . . /polynomial_quotient_ring_element.py:391:
****
Extended gcd computations over p-adic fields are performed using the standard Euclidean algorithm which might produce mathematically incorrect results in some cases.
This issue is being tracked at `http://trac.sagemath.org/sage_trac/ticket/13439`.
****

What could be better ?

What could be better ?

- Higher precision

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols
- More info

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols
- More info $\rightarrow$ use Kurihara

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols
- More info $\rightarrow$ use Kurihara
- More fields

What could be better ?

- Higher precision $\to$ Overconvergent guys
- More curves $\to$ Numerical modular symbols
- More info $\to$ use Kurihara
- More fields $\to$ twist by characters

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols
- More info $\rightarrow$ use Kurihara
- More fields $\rightarrow$ twist by characters
- More objects

What could be better ?

- Higher precision $\to$ Overconvergent guys
- More curves $\to$ Numerical modular symbols
- More info $\to$ use Kurihara
- More fields $\to$ twist by characters
- More objects $\to$ class groups, cm, ab.var, ...

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols
- More info $\rightarrow$ use Kurihara
- More fields $\rightarrow$ twist by characters
- More objects $\rightarrow$ class groups, cm, ab.var, ...
- More approaches

What could be better ?

- Higher precision $\rightarrow$ Overconvergent guys
- More curves $\rightarrow$ Numerical modular symbols
- More info $\rightarrow$ use Kurihara
- More fields $\rightarrow$ twist by characters
- More objects $\rightarrow$ class groups, cm, ab.var, ...
- More approaches $\rightarrow$ Euler systems? ...?

Numerical modular symbols

Given E with nice, but large N. Compute $\int_r^{\infty} 2\pi i f(z)dz$

Numerical modular symbols

Given E with nice, but large N. Compute $\int_r^\infty 2\pi i f(z)dz$

```
sage : E = EllipticCurve([101,103]);
E.conductor().factor()
```

$$2^3 * 79 * 55793$$

Numerical modular symbols

Given E with nice, but large N. Compute $\int_r^\infty 2\pi i f(z)dz$

```
sage : E = EllipticCurve([101,103]);
E.conductor().factor()
```

$$2^3 * 79 * 55793$$

```
sage : m=E.modular_symbol(method="num"); m(2/7)
```

$$-1/2$$

Numerical modular symbols

Given E with nice, but large N. Compute $\int_r^\infty 2\pi i f(z)dz$

```
sage : E = EllipticCurve([101,103]);
E.conductor().factor()
```

$$2^3 * 79 * 55793$$

```
sage : m=E.modular_symbol(method="num"); m(2/7)
```

$$-1/2$$

$[0]^\pm$ takes < 1 sec. $\{[\frac{a}{5^2}]\}$, too. $[\frac{137}{731}]^\pm$ takes < 1 min

Kurihara's theorem

If . . . then there is an effective way of computing integers m_i such that

$$Ш(E/\mathbb{Q})[p^\infty] = \left(\mathbb{Z}/p^{m_1}\mathbb{Z}\right)^2 \oplus \cdots \oplus \left(\mathbb{Z}/p^{m_s}\mathbb{Z}\right)^2$$

Kurihara's theorem

If … then there is an effective way of computing integers m_i such that

$$Ш(E/\mathbb{Q})[p^\infty] = \left({}^{\mathbb{Z}}/_{p^{m_1}\mathbb{Z}}\right)^2 \oplus \cdots \oplus \left({}^{\mathbb{Z}}/_{p^{m_s}\mathbb{Z}}\right)^2$$

This uses Stickelberger elements

$$\Theta_m = \sum_{a \bmod^\times m} \left[\frac{a}{m}\right]^+ \sigma_a \in \mathbb{Q}\big[\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\big]$$

```
sage : any questions?
```

$\ldots$