# Exemples of computations with `shark`

christian wuthrich

June 5th, 2007

# 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()
```

$$2$$

# 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
```

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

The $p$-adic L-function is approximated by

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

$$\begin{gathered}
O(5^7) + O(5^4) \cdot T + (5 + 5^2 + 3 \cdot 5^3 + O(5^4)) \cdot T^2 \\
+(2 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^3 + O(5^4)) \cdot T^3 \\
+(4 \cdot 5^2 + 4 \cdot 5^3 + O(5^4)) \cdot T^4 \\
+(4 \cdot 5 + 4 \cdot 5^2 + O(5^3)) \cdot T^5 \\
+(1 + 2 \cdot 5 + 5^2 + 4 \cdot 5^3 + O(5^4)) \cdot T^6 + O(T^7)
\end{gathered}$$

- 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
```

$$\begin{aligned} &O(5^7) + O(5^4)\cdot T + (5 + 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^2 \\ &+(2\cdot 5 + 3\cdot 5^2 + 3\cdot 5^3 + O(5^4))\cdot T^3 \\ &+(4\cdot 5^2 + 4\cdot 5^3 + O(5^4))\cdot T^4 \\ &+(4\cdot 5 + 4\cdot 5^2 + O(5^3))\cdot T^5 \\ &+(1 + 2\cdot 5 + 5^2 + 4\cdot 5^3 + O(5^4))\cdot T^6 + O(T^7) \end{aligned}$$

- 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 $p$-adic L-function is approximated by

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

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

- 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 $p$-adic L-function is approximated by

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

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

- 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.

## Putting things together

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

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

## Putting things together

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

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

- The valuation of the order of $Ш(E/\mathbb{Q})(p)$ is $0$. So

$$Ш(E/\mathbb{Q})(5) = 0\,.$$

## Putting things together

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

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

- The valuation of the order of $Ш(E/\mathbb{Q})(p)$ is $0$. So

$$Ш(E/\mathbb{Q})(5) = 0\,.$$

- The $p$-adic BSD predicts $\#Ш(E/\mathbb{Q}) \equiv 1 \pmod{125}$.

## Putting things together

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

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

- The valuation of the order of $\text{Ш}(E/\mathbb{Q})(p)$ is $0$. So

$$\text{Ш}(E/\mathbb{Q})(5) = 0\,.$$

- The $p$-adic BSD predicts $\#\text{Ш}(E/\mathbb{Q}) \equiv 1 \pmod{125}$.
- The main conjecture holds for $E$ at $p$.

Actually we have

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

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

Actually we have

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

for some unit $u \in \Lambda^\times$. If we assume that all Tate-Shafarevich groups over number fields are finite, then this tells us that

Actually we have

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

for some unit $u \in \Lambda^\times$. If we assume that all Tate-Shafarevich groups over number fields are finite, then this tells us that

- $\mathrm{rank}(E(\mathbb{Q}_\infty)) = 2 + 4 = 6$ and that

Actually we have

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

for some unit $u \in \Lambda^\times$. If we assume that all Tate-Shafarevich groups over number fields are finite, then this tells us that

- $\mathrm{rank}(E(\mathbb{Q}_\infty)) = 2 + 4 = 6$ and that
- $Ш(E/\mathbb{Q}_\infty)(p)$ is finite.

# Further examples

| | | |
|---|---|---|
| 389a1 | 5 | $1 + O(5^4)$ |
| 389a1 | 7 | $1 + O(7^3)$ |
| 389a1 | 11 | $1 + O(11^2)$ |
| 389a1 | 13 | $1 + O(13^2)$ |
| 389a1 | 17 | $1 + O(17^2)$ |
| 389a1 | 19 | $1 + O(19^2)$ |
| 433a1 | 5 | $4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + O(5^4)$ |
| 433a1 | 7 | $6 + 6 \cdot 7 + 6 \cdot 7^2 + O(7^3)$ |
| 433a1 | 11 | $10 + 10 \cdot 11 + O(11^2)$ |
| 433a1 | 13 | $12 + O(13)$ |
| 433a1 | 17 | $16 + 16 \cdot 17 + O(17^2)$ |
| 433a1 | 19 | $18 + 18 \cdot 19 + O(19^2)$ |
| 446d1 | 5 | $1 + O(5^3)$ |
| 446d1 | 7 | $1 + O(7^2)$ |
| 446d1 | 11 | $1 + O(11^2)$ |
| 446d1 | 13 | $1 + O(13^2)$ |
| 446d1 | 17 | $1 + O(17^2)$ |

# A split multiplicative example

We may also look at the prime $p = 223$

```
sage : p=223; eq = e.tate_curve(p);
eq.parameter(4)
```

$$16 \cdot 223 + 19 \cdot 223^2 + 97 \cdot 223^3 + 118 \cdot 223^4 + O(223^5)$$

# A split multiplicative example

We may also look at the prime $p = 223$

```
sage : p=223; eq = e.tate_curve(p);
eq.parameter(4)
```

$$16 \cdot 223 + 19 \cdot 223^2 + 97 \cdot 223^3 + 118 \cdot 223^4 + O(223^5)$$

where $E$ has split multiplicative reduction.

```
sage : eq.is_split()
```

True

The $p$-adic regulator is

```
sage : reg = eq.padic_regulator(3);reg
```

$$153 \cdot 223^2 + 125 \cdot 223^3 + 124 \cdot 223^4 + 69 \cdot 223^5 + O(223^6)$$

The $p$-adic regulator is

```
sage : reg = eq.padic_regulator(3);reg
```

$$153 \cdot 223^2 + 125 \cdot 223^3 + 124 \cdot 223^4 + 69 \cdot 223^5 + O(223^6)$$

The very first non-trivial appoximation to the $p$-adic $L$-series is

```
sage : lp = e.padic_lseries(p);lps =
lp.series(2,prec=4);lps
```

$$O(223^4) + O(223^1) \cdot T + O(223^1) \cdot T^2$$
$$+(139 + O(223)) \cdot T^3 + O(T^4)$$

The $p$-adic regulator is

```
sage : reg = eq.padic_regulator(3);reg
```

$$153 \cdot 223^2 + 125 \cdot 223^3 + 124 \cdot 223^4 + 69 \cdot 223^5 + O(223^6)$$

The very first non-trivial appoximation to the $p$-adic $L$-series is

```
sage : lp = e.padic_lseries(p);lps =
lp.series(2,prec=4);lps
```

$$O(223^4) + O(223^1) \cdot T + O(223^1) \cdot T^2$$
$$+(139 + O(223)) \cdot T^3 + O(T^4)$$

The $L$-invariant

```
sage : Li = eq.L_invariant(4); Li
```

$$179 \cdot 223 + 85 \cdot 223^2 + 30 \cdot 223^3 + O(223^4)$$

We find

```
sage : lpstar=lps(3); R=Qp(p,10);
lg=log(R(1+p)); tors=e.torsion_order();
tam=e.tamagawa_product()
lpstar/reg*lg^3/Li*tors^2/tam
```

$$1 + O(223)$$

We find

```
sage : lpstar=lps(3); R=Qp(p,10);
lg=log(R(1+p)); tors=e.torsion_order();
tam=e.tamagawa_product()
lpstar/reg*lg^3/Li*tors^2/tam
```

$$1 + O(223)$$

Hence $\text{Ш}(E/\mathbb{Q})(223)$ of this rank $2$ curve is trivial and the $p$-adic BSD predicts

We find

```
sage : lpstar=lps(3); R=Qp(p,10);
lg=log(R(1+p)); tors=e.torsion_order();
tam=e.tamagawa_product()
lpstar/reg*lg^3/Li*tors^2/tam
```

$$1 + O(223)$$

Hence $Ш(E/\mathbb{Q})(223)$ of this rank $2$ curve is trivial and the $p$-adic BSD predicts

$$\#Ш(E/\mathbb{Q}) \equiv \pm 1 \pmod{223}.$$