ellnflocalred

François Brunault (ÉNS Lyon)
francois.brunault@ens-lyon.fr

17 janvier 2013

K : field with a discrete valuation v.
R : ring of integers of K
E : elliptic curve defined over K.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K).$$

K : field with a discrete valuation v.
R : ring of integers of K
E : elliptic curve defined over K.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K).$$

Recall that a Weierstrass equation of E is said to be

- *v-integral* if all $a_i \in R$;
- *v-minimal* if it is v-integral, and $v(\Delta)$ is minimal among all possible v-integral Weierstrass equations of E.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K).$$

Remind that

- v-integral equations always exist (clear denominators) ;

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K).$$

Remind that

- v-integral equations always exist (clear denominators) ;
- v-minimal equations always exist, and are unique up to

$$[u, r, s, t] : \begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases} \qquad (u \in R^\times; r, s, t \in R).$$

We have $\Delta = u^{12}\Delta'$.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K).$$

Remind that

- v-integral equations always exist (clear denominators) ;
- v-minimal equations always exist, and are unique up to

$$[u, r, s, t] : \begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases} \qquad (u \in R^\times; r, s, t \in R).$$

We have $\Delta = u^{12}\Delta'$.

Remark

If the equation is v-integral and $v(\Delta) < 12$, then it is v-minimal.

Why do we need to compute minimal equations ?

Why do we need to compute minimal equations ?

E : elliptic curve defined over a number field K

- Compute the L-function

$$L(E,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(E,s).$$

$L_{\mathfrak{p}}(E,s)$ is defined using a minimal equation of E at $\mathfrak{p}$.

Why do we need to compute minimal equations ?

E : elliptic curve defined over a number field K

- Compute the L-function

$$L(E,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(E,s).$$

  $L_{\mathfrak{p}}(E,s)$ is defined using a minimal equation of E at $\mathfrak{p}$.
- Compute the local height functions

$$h_{\mathfrak{p}} : E(K_{\mathfrak{p}}) \backslash \{0\} \to \mathbf{R}.$$

Further local informations

K : number field
E : elliptic curve over K

Further local informations

K : number field
E : elliptic curve over K

$\mathfrak{p}$: prime ideal of $\mathcal{O}_K$
$k_{\mathfrak{p}}$: residue field of $\mathfrak{p}$
$\overline{E}/k_{\mathfrak{p}}$: reduction of a $\mathfrak{p}$-minimal equation of E

Further local informations

K : number field
E : elliptic curve over K

$\mathfrak{p}$: prime ideal of $\mathcal{O}_K$
$k_{\mathfrak{p}}$: residue field of $\mathfrak{p}$
$\overline{E}/k_{\mathfrak{p}}$: reduction of a $\mathfrak{p}$-minimal equation of E

If $\overline{E}$ is singular, we may need a refined model of E at $\mathfrak{p}$, the *minimal (proper) regular* model of E at $\mathfrak{p}$.

Further local informations

K : number field
E : elliptic curve over K

$\mathfrak{p}$: prime ideal of $\mathcal{O}_K$
$k_{\mathfrak{p}}$: residue field of $\mathfrak{p}$
$\overline{E}/k_{\mathfrak{p}}$: reduction of a $\mathfrak{p}$-minimal equation of E

If $\overline{E}$ is singular, we may need a refined model of E at $\mathfrak{p}$, the *minimal (proper) regular* model of E at $\mathfrak{p}$.

The possible reduction types of minimal regular models have been classified by Kodaira, Néron.

Further local informations

K : number field
E : elliptic curve over K

Further local informations

K : number field
E : elliptic curve over K

- N_E conductor of E (ideal of $\mathcal{O}_K$)
  (enters into the functional equation of $L(E,s)$)

  $N_E = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}}$
  $f_{\mathfrak{p}}$: conductor exponent of E at $\mathfrak{p}$

Further local informations

K : number field
E : elliptic curve over K

- N_E conductor of E (ideal of $\mathcal{O}_K$)
  (enters into the functional equation of $L(E,s)$)

  $N_E = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}}$
  $f_{\mathfrak{p}}$: conductor exponent of E at $\mathfrak{p}$

- $c_{\mathfrak{p}}$: Tamagawa number of E at $\mathfrak{p}$
  $c_{\mathfrak{p}} = \#(E(K_{\mathfrak{p}})/E_0(K_{\mathfrak{p}}))$
  (enters into the BSD conjecture for E)

Tate's algorithm

Input :

- $E = [a_1, a_2, a_3, a_4, a_6]$: elliptic curve over K
- $\mathfrak{p}$: prime ideal of $\mathcal{O}_K$

Tate's algorithm

Input :

- $E = [a_1, a_2, a_3, a_4, a_6]$: elliptic curve over K
- $\mathfrak{p}$: prime ideal of $\mathcal{O}_K$

Output :

- $[u, r, s, t]$: change of variables to a $\mathfrak{p}$-minimal equation
- reduction type of E at $\mathfrak{p}$ (Kodaira symbol)
- $f_{\mathfrak{p}}$: conductor exponent of E at $\mathfrak{p}$
- $c_{\mathfrak{p}}$: Tamagawa number of E at $\mathfrak{p}$

PARI/GP has an implementation of Tate's algorithm for elliptic curves over $\mathbf{Q}$:

PARI/GP has an implementation of Tate's algorithm for elliptic curves over $\mathbf{Q}$:

`elllocalred(E,p)`: E being an elliptic curve, returns `[f,kod,[u,r,s,t],c]`, where f is the conductor's exponent, kod is the Kodaira type for E at p, `[u,r,s,t]` is the change of variable needed to make E minimal at p, and c is the local Tamagawa number c_p.

PARI/GP has an implementation of Tate's algorithm for elliptic curves over $\mathbf{Q}$:

`elllocalred(E,p)`: E being an elliptic curve, returns [f,kod,[u,r,s,t],c], where f is the conductor's exponent, kod is the Kodaira type for E at p, [u,r,s,t] is the change of variable needed to make E minimal at p, and c is the local Tamagawa number c_p.

We would like an analogous function `ellnflocalred(E,nf,P)`.
`E` : elliptic curve as output by `ellinit`
`nf` : number field as output by `nfinit`
`P` : prime ideal of `nf`

Currently I implemented `ellnflocalred(E,nf,P)` only in the "easy" case where the residual characteristic of `P` is $\geqslant 5$.

Assume $\mathrm{char}(k_{\mathfrak{p}}) \geqslant 5$. There are basically two steps in Tate's algorithm :

Assume $\mathrm{char}(k_{\mathfrak{p}}) \geqslant 5$. There are basically two steps in Tate's algorithm :

1. Find a $\mathfrak{p}$-minimal equation ;

Assume $\mathrm{char}(k_{\mathfrak{p}}) \geqslant 5$. There are basically two steps in Tate's algorithm :

1. Find a $\mathfrak{p}$-minimal equation ;
2. Compute the local invariants.

Assume $\mathrm{char}(k_{\mathfrak{p}}) \geqslant 5$. There are basically two steps in Tate's algorithm :

1. Find a $\mathfrak{p}$-minimal equation ;
2. Compute the local invariants.

Step 1 is easy since E admits a reduced equation

$$E : y^2 = x^3 - 27c_4x - 54c_6 \qquad (c_4, c_6 \in \mathcal{O}_K).$$

- If $v_{\mathfrak{p}}(c_4) < 4$ or $v_{\mathfrak{p}}(c_6) < 6$, then this equation is $\mathfrak{p}$-minimal.
- Otherwise, put $k = \min(\lfloor \frac{v_{\mathfrak{p}}(c_4)}{4} \rfloor, \lfloor \frac{v_{\mathfrak{p}}(c_6)}{6} \rfloor)$ and let $(c_4, c_6) \leftarrow \left(\frac{c_4}{\pi^{4k}}, \frac{c_6}{\pi^{6k}}\right)$ where π is a uniformizer at $\mathfrak{p}$. Then the resulting equation is $\mathfrak{p}$-minimal.

Remarks

- When doing $(c_4, c_6) \leftarrow \left(\frac{c_4}{\pi^{4k}}, \frac{c_6}{\pi^{6k}}\right)$, we don't want to lose integrality. So instead of taking an arbitrary uniformizer π, we compute an element $\pi' = \frac{1}{\pi}$ such that $v_{\mathfrak{p}}(\pi') = -1$ and $v_{\mathfrak{q}}(\pi') \geqslant 0$ for any $\mathfrak{q} \neq \mathfrak{p}$. For this we use `idealappr`.

Remarks

- When doing $(c_4, c_6) \leftarrow \left(\frac{c_4}{\pi^{4k}}, \frac{c_6}{\pi^{6k}}\right)$, we don't want to lose integrality. So instead of taking an arbitrary uniformizer π, we compute an element $\pi' = \frac{1}{\pi}$ such that $v_{\mathfrak{p}}(\pi') = -1$ and $v_{\mathfrak{q}}(\pi') \geqslant 0$ for any $\mathfrak{q} \neq \mathfrak{p}$. For this we use `idealappr`.
- If $\mathfrak{p}$ is principal, the function takes a generator π of $\mathfrak{p}$ as optional argument.

Remarks

- When doing $(c_4, c_6) \leftarrow \left(\frac{c_4}{\pi^{4k}}, \frac{c_6}{\pi^{6k}}\right)$, we don't want to lose integrality. So instead of taking an arbitrary uniformizer π, we compute an element $\pi' = \frac{1}{\pi}$ such that $v_{\mathfrak{p}}(\pi') = -1$ and $v_{\mathfrak{q}}(\pi') \geqslant 0$ for any $\mathfrak{q} \neq \mathfrak{p}$. For this we use `idealappr`.
- If $\mathfrak{p}$ is principal, the function takes a generator π of $\mathfrak{p}$ as optional argument.
- We may well have $v_{\mathfrak{q}}(\pi') > 0$ for some $\mathfrak{q} \neq \mathfrak{p}$. In this case, multiplying by (π'^{4k}, π'^{6k}) does not preserve $\mathfrak{q}$-minimality. We cannot avoid this since $\mathfrak{p}$ need not be principal.

What remains to be done :

- Case of residual characteristic 2 and 3 ;

What remains to be done :

- Case of residual characteristic 2 and 3 ;
- Compute the local root number of E at $\mathfrak{p}$
(Halberstadt, Kobayashi, Dokchitser-Dokchitser, Whitehouse)

What remains to be done :

- Case of residual characteristic 2 and 3 ;
- Compute the local root number of E at $\mathfrak{p}$ (Halberstadt, Kobayashi, Dokchitser-Dokchitser, Whitehouse)
- Compute a global minimal equation (when it exists) : Kraus-Laska-Connell's algorithm

What remains to be done :

- Case of residual characteristic 2 and 3 ;
- Compute the local root number of E at $\mathfrak{p}$ (Halberstadt, Kobayashi, Dokchitser-Dokchitser, Whitehouse)
- Compute a global minimal equation (when it exists) : Kraus-Laska-Connell's algorithm

Question :
How to encode the local Galois representation of E at $\mathfrak{p}$

$$\rho_{E,\mathfrak{p}} : \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})?$$