Computing in component groups of elliptic curves

John Cremona
University of Warwick, UK

ANTS VIII: Banff, 9 May 2008

Plan of the talk

- What are component groups?
- What does it mean to “compute in a component group”?
- Easy cases
- The split multiplicative case
- Example and application

Component groups 1

Let K be a p-adic local field and E an elliptic curve defined over K.
The component group of E is the group

$$\Phi(E/K) = E(K)/E^0(K),$$

where $E^0(K)$ denotes the subgroup of points of good reduction. This is:

- finite;
- cyclic if E has multiplicative reduction;
- of order at most 4 if E has additive reduction.

Aim: to compute an explicit isomorphism $E(K)/E^0(K) \cong \mathbb{Z}/m\mathbb{Z}$ or $E(K)/E^0(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Component groups 2

- The order of $\Phi(E/K)$ is the *Tamagawa number*, often denoted c.
- If E has good reduction then $\Phi(E/K)$ is trivial.

In applications we may have E defined over a number field K, and be interested in the component groups $\Phi(E/K_v)$ for *all* completions K_v.

For archimedean v, $E^0(K_v)$ is the connected component of the identity; so

- If v is complex: $\Phi(E/\mathbb{C}) = 0$;
- If v is real: $\Phi(E/\mathbb{R}) = 0$ if $\Delta_v < 0$, and has order 2 if $\Delta_v > 0$;

Component groups and reduction types 1

For p-adic local fields the component groups are as follows:

Reduction type	c	Φ
I_m (split, all m)	m	C_m
I_m (non-split, even m)	2	C_2
I_m (non-split, odd m)	1	C_1
$\mathrm{II}, \mathrm{II}^*$	1	C_1
$\mathrm{III}, \mathrm{III}^*$	2	C_2
$\mathrm{IV}, \mathrm{IV}^*$	$1, 3$	C_1, C_3
I_0^*	$1, 2, 4$	$C_1, C_2, C_2 \times C_2$
I_m^* (even $m > 0$)	$2, 4$	$C_2, C_2 \times C_2$
I_m^* (odd m)	$2, 4$	C_2, C_4

Component groups and reduction types 2

From the table we see that identifying the component group as an abstract abelian group is easy: Tate's algorithm gives both the reduction type (Kodaira symbol) and the Tamagawa number c to distinguish between split and non-split cases.

Recall that our goal is to make the following map (isomorphism) explicit:

$$\kappa\colon E(K)/E^0(K) \to G,$$

where $G \cong \Phi(E/K)$ and either $G = \mathbb{Z}/m\mathbb{Z}$ or $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
First we deal with some easy cases.

The easy cases

When $G = \mathbb{Z}/m\mathbb{Z}$ for small m, say $m \leq 4$, or $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ it suffices to be able to determine:

- for $P \in E(K)$, is $\kappa(P) = 0$?
- for $P, Q \in E(K)$, is $\kappa(P) = \kappa(Q)$?

which is simply a matter of checking whether P or $P - Q$ has good reduction.

We also need to do some book-keeping — to distinguish the two non-trivial elements of $\mathbb{Z}/3\mathbb{Z}$, for example.

When $G = \mathbb{Z}/m\mathbb{Z}$ for large m this would be tedious (at best), so we seek a more elegant solution.

The split multiplicative case

From now on we will assume that E has split multiplicative reduction of type I_m, so that $\kappa\colon E(K)/E^0(K) \cong \mathbb{Z}/m\mathbb{Z}$. Assume that E has minimal Weierstrass equation

$$E : F(X,Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6) = 0$$

with $a_i \in \mathcal{O}_K$; then $v(\Delta) = m > 0$ and $v(c_4) = 0$.

Theorem (Silverman) Let $P = (x,y) \in E(K) \setminus E^0(K)$. Then

$$\kappa(P) = \pm\min\{v(2y + a_1x + a_3), m/2\} \pmod{m} \in \mathbb{Z}/m\mathbb{Z}.$$

This result suffices to compute the local height of P (which only depends on the image of P in $\Phi(E/K)$), since it is the same for $\pm P$. But for our purposes, we need to define the sign ± 1 consistently. Since $n \mapsto -n$ is an automorphim of $\mathbb{Z}/m\mathbb{Z}$, this question only makes sense when we wish to compare the values of $\kappa(P)$ for several points P.

Split multiplicative case (continued)

Silverman's formula $\min\{v(2y + a_1x + a_3), m/2\} \pmod{m}$ gives the value of $\kappa((x, y))$ up to sign. We need to determine a consistent choice of sign.

Set

$$x_0 = (18b_6 - b_2b_4)/c_4; \qquad y_0 = -(a_1x_0 + a_3)/2.$$

Then $F(x_0, y_0) \equiv F_X(x_0, y_0) \equiv F_Y(x_0, y_0) \equiv 0 \pmod{\pi^m}$.

Let α_1, α_2 be the roots of $T^2 + a_1T - (a_2 + 3x_0)$; these lie in $\mathcal{O}_K$ and are distinct.

Now the linear form $2y + a_1x + a_3$ may be written as a sum of two terms:

$$2y + a_1x + a_3 = [(y - y_0) - \alpha_1(x - x_0)] + [(y - y_0) - \alpha_2(x - x_0)].$$

We can now state our result.

Split multiplicative case: the formula

Theorem Let $P = (x, y) \in E(K) \setminus E^0(K)$. Set $e_i = v((y - y_0) - \alpha_i(x - x_0))$ for $i = 1, 2$. Then an isomorphism $\kappa\colon E(K)/E^0(K) \to \mathbb{Z}/m\mathbb{Z}$ is given by setting

$$\kappa(P) = \begin{cases} +e_2 & \text{if } e_2 < e_1; \\ -e_1 & \text{if } e_1 < e_2; \\ m/2 & \text{if } e_1 = e_2 \end{cases}$$

for $P \in E(K) \setminus E^0(K)$.

Sketch proof: We first prove the result when E is a "Tate curve", and then work out the explicit transformation between E and a Tate curve. The first step in transforming the original Weierstrass equation to a Tate curve equation consists of making the transformation $X = X' + x_0$ and $Y = Y' + y_0$.

Split multiplicative case: proof

A Tate curve E_q has equation

$$Y^2 + XY = X^3 + a_4 X + a_6,$$

where $a_4 = a_4(q)$ and $a_6 = a_6(q)$ are given by explicit power series in q. We have $v(\Delta) = v(a_6) = m$, where $m = v(q) > 0$, and $v(a_4) \geq m$. Also, $v(c_4) = v(c_6) = 0$.

The Tate curve has a parametrization

$$\varphi\colon K^*/q^{\mathbb{Z}}\mathcal{O}_K^* \cong E_q(K)/E_q^0(K).$$

The map κ is determined by $\kappa(\varphi(u)) = v(u) \pmod{m}$ for $u \in K^*$. The x- and y-coordinates of $\varphi(u)$ are given by explicit power series, using which we can relate $v(u)$ to the valuations of x, y and $x + y$.

Example

Let $E = 8025j1$, defined over $\mathbb{Q}$, with Weierstrass equation

$$Y^2 + Y = X^3 + X^2 + 2242417292X + 12640098293119.$$

$E(\mathbb{Q}) = \langle P \rangle$ where $P = (335021/4, 224570633/8)$ has infinite order.
Over $K = \mathbb{Q}_3$, E has split multiplicative reduction of type I_{31}.
We compute $x_0 = 556930682563112$ and $y_0 = 308836698141973$ modulo 3^{31}, and $\alpha_1 \equiv -\alpha_2 \equiv 256142918648120$. For the point P, we find

$$(y - y_0) - \alpha_1(x - x_0) \equiv 446797736663247 \pmod{3^{31}},$$

$$(y - y_0) - \alpha_2(x - x_0) \equiv 325294064834346 \pmod{3^{31}},$$

with valuations $e_1 = 12$ and $e_2 = 6$, so $\kappa(P) = +6 \pmod{31}$.

Example (continued)

As a test, we computed $\kappa(iP)$ independently for $1 \le i \le 30$, checking that $\kappa(iP) \equiv 6i \pmod{31}$. The results are given in the following table:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
e_1	12	19	13	7	1	10	20	14	8	2	8	20	15	9	3
e_2	6	12	18	14	2	5	11	17	16	4	4	10	16	18	6
$\kappa(iP)$	6	12	-13	-7	-1	5	11	-14	-8	-2	4	10	-15	-9	-3
i	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
e_1	6	12	18	14	2	5	11	17	16	4	4	10	16	18	6
e_2	12	19	13	7	1	10	20	14	8	2	8	20	15	9	3
$\kappa(iP)$	-6	-12	13	7	1	-5	-11	14	8	2	-4	-10	15	9	3

Application

- Given E, an elliptic curve defined over $\mathbb{Q}$
- Given a subgroup B of $E(\mathbb{Q})$ of full rank, generated by r independent points P_i
- Problem: "saturate" B: find a $\mathbb{Z}$-basis for the full group $E(\mathbb{Q})$
- Method: determine the index in B of $B_{\text{egr}} = B \cap \bigcap_{p\le\infty} E^0(\mathbb{Q}_p)$.

Working in B_{egr} instead of B allows us to use better height bounds to carry out the saturation.

The component group maps κ for each prime p may be used for this, and are accordingly implemented in our program `mwrank`.