COMPUTING IN COMPONENT GROUPS OF ELLIPTIC CURVES

J. E. CREMONA

ABSTRACT. Let K be a p-adic local field and E an elliptic curve defined over K. The component group of E is the group $E(K)/E^0(K)$, where $E^0(K)$ denotes the subgroup of points of good reduction; this is known to be finite, cyclic if E has multiplicative reduction, and of order at most 4 if E has additive reduction. We show how to compute explicitly an isomorphism $E(K)/E^0(K) \cong \mathbb{Z}/N\mathbb{Z}$ or $E(K)/E^0(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1. INTRODUCTION

Let K be a p-adic local field (that is, a finite extension of $\mathbb{Q}_p$ for some prime p), with ring of integers R, uniformizer π, residue field $k = R/(\pi)$ and valuation function v. Let E be an elliptic curve defined over K. The component group of E is the group $\Phi = E(K)/E^0(K)$, where $E^0(K)$ denotes the subgroup of points of good reduction; this is known to be a finite abelian group.

When E has split multiplicative reduction, we have $\Phi \cong \mathbb{Z}/N\mathbb{Z}$ where $N = v(\Delta)$ and Δ is the discriminant of a minimal model for E. In all other cases, Φ has order at most 4, so is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ with $n \in \{1, 2, 3, 4\}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The order of Φ is called the Tamagawa number of E/K, usually denoted c or c_p.

In this note we will show how to make the isomorphism $\kappa\colon E(K)/E^0(K) \to A$ explicit, where A is the one of the above standard abelian groups.

The most interesting case is that of split multiplicative reduction. Here the map κ is almost determined by a formula for the (local) height in [2]. Specifically, if the minimal Weierstrass equation for E has coefficients a_1, a_2, a_3, a_4, a_6 as usual, for a point $P = (x, y) \in E(K) \setminus E^0(K)$ we have $\kappa(P) = \pm n \pmod N$ where $n = \min\{v(2y + a_1x + a_3), N/2\}$, and $0 < n \leq N/2$. In computing heights, of course, one need not distinguish between P and $-P$, but for our purposes this is essential. We show how to determine the appropriate sign in a consistent way to give an isomorphism $\kappa\colon E(K)/E^0(K) \cong \mathbb{Z}/N\mathbb{Z}$. (Note that for an individual point this is not a well-defined question since negation gives an automorphism of $\mathbb{Z}/N\mathbb{Z}$; but when comparing the values of κ at two or more points it is important.) We first establish the formula for Tate curves, and then see how to apply it to a general minimal Weierstrass model.

We also make some remarks about the other reduction types, which are much simpler to deal with, and also the real case.

One application for this, which was our motivation, occurs in the determination of the full Mordell-Weil group $E(K)$ where E is an elliptic curve defined over a number field K. Given a subgroup B of $E(K)$ of full rank, generated by r independent points P_i for $1 \leq i \leq r$, one method for extending this to a $\mathbb{Z}$-basis for $E(K)$ requires determining the index in B of $B \cap \bigcap_{p \leq \infty} E^0(\mathbb{Q}_p)$. The component group maps κ for each prime p may be used here.

We use standard notation for Weierstrass equations of elliptic curves throughout.

2000 *Mathematics Subject Classification.* Primary: 11G07; Secondary: 11Y99.
Key words and phrases. Elliptic curves, component groups, local fields.

2. The split multiplicative case

We refer to [3, Chapter V] for the theory of the Tate parametrization of elliptic curves with split multiplicative reduction.

2.1. **The case of Tate curves.** For each $q \in K^*$ with $|q| < 1$ we define the Tate curve E_q by its Weierstrass equation

$$Y^2 + XY = X^3 + a_4X + a_6$$

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

Reducing modulo π^N, the equation becomes $Y(Y + X) \equiv X^3$; the linear factors Y, $Y + X$ give the distinct tangents at the node $(0, 0)$ on the reduced curve over k.

Theorem. *The map $\kappa\colon E(K) \to \mathbb{Z}/N\mathbb{Z}$ given by*

$$\kappa(P) = \begin{cases} 0 & \text{if } P \in E^0(K) \\ +n & \text{if } P = (x, y) \notin E^0(K) \text{ and } n = v(x + y) < v(y) \\ -n & \text{if } P = (x, y) \notin E^0(K) \text{ and } n = v(y) < v(x + y) \\ N/2 & \text{if } P = (x, y) \notin E^0(K) \text{ and } v(y) = v(x + y) \end{cases}$$

induces an isomorphism $E(K)/E^0(K) \cong \mathbb{Z}/N\mathbb{Z}$. The integer n here always satisfies $0 < n < N/2$. The last case only occurs when N is even, and then $v(y) \geq N/2$.

Remark. This is compatible with the result from [2] quoted in the introduction, which here says that $\kappa(P) = \pm n$ where $n = \min\{v(2y + x), N/2\}$. What we have done is decompose $2y + x$ as $y + (y + x)$, where the summands come from the tangent lines at the singular point, and consider the valuations of each summand separately.

Proof. Recall that the Tate parametrization gives an isomorphism $\varphi\colon K^*/q^{\mathbb{Z}}R^* \cong E(K)/E^0(K)$, and that κ is determined by $\kappa(\varphi(u)) = v(u) \pmod N$ for $u \in K^*$.

Let $P = \varphi(u) = (x, y)$. Then $x = X(u, q)$ and $y = Y(u, q)$ where $X(u, q)$ and $Y(u, q)$ are power series given in [3, §V.3, Theorem 5.1(c)]:

$$x = \frac{u}{(1-u)^2} + \sum_{n\geq 1}\left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n/u}{(q^n/u-1)^2} - 2\frac{q^n}{(1-q^n)^2}\right);$$

$$y = \frac{u^2}{(1-u)^2} + \sum_{n\geq 1}\left(\frac{(q^n u)^2}{(1-q^n u)^3} + \frac{q^n/u}{(q^n/u-1)^3} + \frac{q^n}{(1-q^n)^2}\right).$$

First suppose that $v(u) = e$ with $0 < e < N/2$. The first series shows that $v(x) = e$, since the term outside the sum has valuation e while all those in the sum have strictly greater valuation. Regarding y, the term outside the sum has valuation $2e$ and all those in the sum have strictly greater valuation, except possibly the term $\frac{q^n/u}{(q^n/u-1)^3}$ for $n = 1$, which has valuation $N - e > e$. Considering the three cases $N - e > 2e$, $N - e = 2e$, $e < N - e < 2e$, we find that

$$\begin{aligned} v(y) &= 2e && \text{if } 0 < e < N/3; \\ v(y) &\geq 2e && \text{if } e = N/3; \\ e < v(y) &= N - e < 2e && \text{if } N/3 < e < N/2. \end{aligned}$$

It follows that $\kappa(P) = e$ with $e = v(y + x) = v(x) < v(y)$ as required. (We have $P \in V_e$ in the notation of [3, p.434].)

Next suppose that $v(u) = -e$ with $0 < e < N/2$. Now $v(u^{-1}) = e$ and $\varphi(u^{-1}) = -P = (x, -y - x)$, so by the first case we have $\kappa(P) = -\kappa(-P) = -e$ where

$e = v(y) = v(x) < v(x+y)$ as required. (We have $P \in U_e$ in the notation of [3, p.434].)

Finally suppose that N is even and $v(u) = N/2$. Now we have $v(y) = e$ while $v(x) \geq e$ and $v(x+y) \geq e$, so $N/2 = e = v(y) \leq v(x+y)$. (We have $P \in W$ in the notation of [3, p.434].) □

2.2. **The general case.** Let E with split multiplicative reduction be given by the minimal Weierstrass equation $F(X,Y) = 0$ where

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

Thus $a_i \in R$, $v(\Delta) = N > 0$ and $v(c_4) = 0$. Define

$$\begin{aligned} x_0 &= c_4^{-1}(18b_6 - b_2b_4); \\ y_0 &= c_4^{-1}(a_1^3a_4 - 2a_1^2a_2a_3 + 4a_1a_2a_4 + 3a_1a_3^2 - 36a_1a_6 - 8a_2^2a_3 + 24a_3a_4) \\ &= -\frac{1}{2}(a_1x_0 + a_3). \end{aligned}$$

Our result is as follows.

Theorem. *Let α_1, α_2 be the roots of $T^2 + a_1T - (a_2 + 3x_0)$; these lie in R and are distinct. For $P = (x,y) \in E(K) \setminus E^0(K)$, set*

$$e_i = v((y - y_0) - \alpha_i(x - x_0))$$

for $i = 1, 2$. Then $\kappa(P) \in \mathbb{Z}/N\mathbb{Z}$ is given by

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

where in the first two cases $0 < e < N/2$, and the last case can only occur when N is even.

Remarks. Note that in order to determine $\kappa(P)$ we need to compute the quantities x_0, y_0, α_i only modulo π^N (or even $\pi^{\lceil N/2 \rceil}$), and that these depend only on E, not on P. Also, if we interchange the order of the roots α_i the only effect is to replace $\kappa(P)$ by $-\kappa(P)$ consistently, which is harmless since negation is an automorphism of $\mathbb{Z}/N\mathbb{Z}$. Finally note that

$$\begin{aligned} [(y - y_0) - \alpha_i(x - x_0)] + [(y - y_0) - \alpha_2(x - x_0)] &= 2y + a_1x - (2y_0 + a_1x_0) \\ &= 2y + a_1x + a_3, \end{aligned}$$

so this result is compatible with the formula from [2] quoted in the introduction.

Proof. With x_0, y_0 as given we may check that $F(x_0, y_0) \equiv F_X(x_0, y_0) \equiv F_Y(x_0, y_0) \equiv 0 \pmod{\pi^N}$. (Here the subscripts denote derivatives.) In other words, (x_0, y_0) reduces to a singular point, not just modulo π but modulo π^N. As in the first step of Tate's algorithm (where normally one only requires x_0 and y_0 modulo π), we shift the origin by setting $X = X' + x_0$ and $Y = Y' + y_0$. This results in a new Weierstrass equation with coefficients a_i' satisfying $a_1' = a_1$, $a_2' = a_2 + 3x_0$, $b_2' = b_2 + 12x_0 \in R^*$, and

$$a_3' \equiv a_4' \equiv a_6' \equiv b_4' \equiv b_6' \equiv b_8' \equiv 0 \pmod{\pi^N}.$$

Since we have split multiplicative reduction, the quadratic $T^2 + a_1'T - a_2'$, whose discriminant is b_2', splits modulo π and hence by Hensel's Lemma splits over K. The roots α_1, α_2 lie in R, and $\alpha_1 - \alpha_2 \in R^*$ since $(\alpha_1 - \alpha_2)^2 = b_2'$.

Now set $\beta_i = (\alpha_1 - \alpha_2)^{-1}(a'_4 - \alpha_i a'_3)$ for $i = 1, 2$. Then $\beta_i \equiv 0 \pmod{\pi^N}$ and we may check that

$$\begin{aligned} F &= (Y' - \alpha_1 X' - \beta_1)(Y' - \alpha_2 X' + \beta_2) - (X'^3 + b'_8/b'_2) \\ &\equiv (Y' - \alpha_1 X')(Y' - \alpha_2 X') - X'^3 \\ &\equiv Y''(Y'' + a''_1 X') - X'^3 \pmod{\pi^N}, \end{aligned}$$

where we have set $Y' = Y'' + \alpha_1 X' + \beta_1$ and $a''_1 = \alpha_1 - \alpha_2$. (Here we have used: $\beta_1 - \beta_2 = -a'_3$, $\alpha_1\beta_2 - \alpha_2\beta_1 = a'_4$, and $b'_2(a'_6 - \beta_1\beta_2) = b'_8$.) After a further scaling by the unit a''_1, this has the form of a Tate curve.

Applying the result of the previous section, we see that $\kappa(P)$ is given in terms of the valuations of y'' and $y'' + a''_1 x''$. Now

$$y'' \equiv y' - \alpha_1 x' \equiv (y - y_0) - \alpha_1(x - x_0) \pmod{\pi^N}$$

and

$$y'' + a''_1 x'' \equiv y' - \alpha_2 x' \equiv (y - y_0) - \alpha_2(x - x_0) \pmod{\pi^N},$$

which implies the result as stated.

□

2.3. **Example.** Let E be the elliptic curve defined over $\mathbb{Q}$ denoted 8025j1 in the tables [1], whose Weierstrass equation is

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

Take $P = (335021/4, 224570633/8)$, a generator of the Mordell-Weil group $E(\mathbb{Q})$ which is isomorphic to $\mathbb{Z}$.

We consider E over $K = \mathbb{Q}_3$ where it has split multiplicative reduction of type I_{31}. We compute $x_0 = 556930682563112$ and $y_0 = 308836698141973$ modulo 3^{31}, and $\alpha_1 \equiv -\alpha_2 \equiv 256142918648120$. Now for the point P we find

$$\begin{aligned} (y - y_0) - \alpha_1(x - x_0) &\equiv 446797736663247 \pmod{3^{31}}, \\ (y - y_0) - \alpha_2(x - x_0) &\equiv 325294064834346 \pmod{3^{31}}, \end{aligned}$$

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

To test our implementation of the computation of κ, 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

3. Other reduction types

For completeness we will now discuss the other reduction types, as well as $K = \mathbb{R}$.

3.1. **Types where Φ is trivial.** When the reduction type is I_1 (good reduction), II or II*, the component group Φ is trivial, i.e. $c = 1$. This is also the case for non-split multiplicative reduction of type I_m when m is odd, and in the "non-split" cases for types IV, IV*, and I_0^*. Here there is nothing to be done.

3.2. **Types where $\Phi \cong \mathbb{Z}/2\mathbb{Z}$.** When the reduction type is non-split multiplicative of type I_m when m is even, III or III*, and some cases of type I_m, we have $\Phi \cong \mathbb{Z}/2\mathbb{Z}$. Here all we need do is define $\kappa(P) = 0$ if P has good reduction and 1 otherwise.

3.3. **Types where $\Phi \cong \mathbb{Z}/3\mathbb{Z}$.** When the reduction type is IV or IV* we may have $\Phi \cong \mathbb{Z}/3\mathbb{Z}$ in the "split" case. Our task is to see how to distinguish the two nontrivial components or cosets of $E^0(K)$ in $E(K)$.

First consider Type IV. After translating the model so that the singular point is $(0,0) \pmod{\pi}$, as in the first step of Tate's algorithm, the quadratic $h(T) = T^2 + \pi^{-1}a_3T - \pi^{-2}a_6$ has distinct roots in the residue field k (since if the roots only lie in a quadratic extension of k then $c = 1$ and Φ is trivial: the "non-split" case). Let α_1, α_2 be the roots of $h(T)$. Then any point $P = (x, y)$ of bad reduction has $y \equiv \alpha_i\pi \pmod{\pi^2}$ for $i \in \{1, 2\}$, as may be seen by reducing the Weierstrass equation modulo π^2. These two cases distinguish the two components, and we may define $\kappa(P) = i \pmod 3$.

We may translate this condition to apply to the original coordinates of the point: if the singular point is $(x_0, y_0) \pmod{\pi}$ then for $P = (x, y) \in E(K) \setminus E^0(K)$ the value of $y - y_0$ lies in one of two distinct residue classes modulo π^2, which we may label arbitrarily and use to distinguish the nonzero values of κ. However, this is hardly worth while in practice: instead we may simply define $\kappa(P_1) = 1 \pmod 3$ for the first point P_1 of bad reduction we encounter, and then for subsequent such points P we have $\kappa(P) = \pm 1$ according as $P - P_1$ does or does not have good reduction.

This latter strategy is certainly to be preferred for the case IV*, where (referring to Tate's algorithm) a second change of variables may be required. Otherwise we would need to determine $y_0 \pmod{\pi^2}$ and use the value of $y - y_0 \pmod{\pi^3}$ to distinguish the cases.

3.4. **Types where $\Phi \cong \mathbb{Z}/4\mathbb{Z}$.** This can only occur with Type I_m^* when m is odd. Since this route in Tate's algorithm is the most subtle, rather than analyze the situation in more detail we can proceed as follows.

Set $\kappa(P) = 0$ if P has good reduction; otherwise set $\kappa(P) = 2$ if $2P$ has good reduction; otherwise $\kappa(P) = \pm 1$. A simple strategy, similar to that used for the $\mathbb{Z}/3\mathbb{Z}$ case, may be used to distinguish the latter in practice.

3.5. **Types where $\Phi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.** This can occur with Type I_m^* when m is even (including $m = 0$). Noting that the automorphism group of Φ includes all permutations of its nontrivial elements, we may proceed as follows:

Set $\kappa(P) = (0,0)$ if P has good reduction; otherwise set $\kappa(P_1) = (1,0)$ for the first point P_1 of bad reduction and $\kappa(P_2) = (0,1)$ for the first point P_2 such that neither P_2 nor $P_1 + P_2$ has good reduction. Now we can determine $\kappa(P)$ for all P simply by testing P, $P + P_1$ and $P + P_2$ for good reduction.

In case of Type I_0^*, the nonzero values of $\kappa(P)$ may also be distinguished by the residue of $x - x_0 \pmod{\pi^2}$ where as usual $(x_0, y_0) \pmod{\pi}$ is the singular point on the reduction; but we have not attempted to extend this to a criterion for $m > 0$.

3.6. **The real case.** For completeness we finish by mentioning the case $K = \mathbb{R}$, where the component group is trivial if $\Delta < 0$ and has order 2 when $\Delta > 0$. In the latter case we may test whether a given point $P = (x, y)$ lies in $E^0(\mathbb{R})$ by checking that $g'(x) > 0$ and $g''(x) > 0$ where $g(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$; note that this may be done using exact arithmetic when E is defined over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$, and so does not rely on approximating the real 2-torsion points.

References

[1] J. E. Cremona. Tables of elliptic curves. `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`.
[2] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.
[3] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, UK.
E-mail address: `John.Cremona@nottingham.ac.uk`