Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
23 (2007), 115–123
www.emis.de/journals
ISSN 1786-0091

ON THE MAPPINGS OF ELLIPTIC CURVES DEFINED OVER $\mathbb{Q}$ INTO $[0,1)^2$

ZOLTÁN CSAJBÓK

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ given by an affine Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z}, x, y \in \mathbb{Q}). \tag{1}$$

Reducing the elliptic curve (1) modulo a sufficiently large prime p, we obtain an elliptic curve $\widetilde{E}_p$ over $\mathbb{F}_p$. Considering an infinite sequence of elliptic curves $\widetilde{E}_p$, we map the point (x, y) of them into the unit square $[0, 1)^2$ via the mapping $(x, y) \mapsto \left(\frac{x}{p}, \frac{y}{p}\right)$.

We prove that the obtained cumulative point set contains a point sequence aligning a line when $E/\mathbb{Q}$ has an integral point, and point sequences aligning lines of well defined number when $E/\mathbb{Q}$ has a rational point. In both cases, these lines contain infinitely many points being strictly monotone increasing or decreasing according to the L_∞ norm, and these monotone point sequences converge to well defined points.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ given in Weierstrass normal form

$$y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z}, x, y \in \mathbb{Q},\, 4a^3 \neq 27b^2).$$

If the prime p is sufficiently large, then its reduction modulo p

$$y^2 = x^3 + \tilde{a}x + \tilde{b} \quad (\tilde{a}, \tilde{b}, x, y \in \mathbb{F}_p)$$

is also an elliptic curve $\widetilde{E}_p$ defined over the finite field $\mathbb{F}_p$ with p elements.

The finite abelian group $\widetilde{E}_p(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\widetilde{E}_p$ has size

$$\#\widetilde{E}_p(\mathbb{F}_p) = p + 1 - a_p$$

where $|a_p| < 2\sqrt{p}$ according to the Hasse-Weil theorem ([4], Chap. V, Theorem 1.1).

2000 *Mathematics Subject Classification.* 14H52.
Key words and phrases. Elliptic curves, reduction of elliptic curves, normalization of elliptic curves.

The elliptic curve group $\widetilde{E}(\mathbb{F}_p)$ can be studied at fixed p and varying E, or conversely, at fixed E and varying p. If we fix p and vary E, then there are only finitely many curves E over $\mathbb{F}_p$ up to equivalence, and Deuring's theorems contain detailed information of these curves [2].

It is much less known, however, the converse case, i.e., when E is fixed and p varies.

Our approach to this problem is that we normalize the $\mathbb{F}_p$-rational points of $\widetilde{E}_p$ simultaneously for all sufficiently large primes p, mapping them into the unit square. In this paper we will study this normalized cumulative point set.

We prove that

- if $E/\mathbb{Q}$ has an integral point, then there is a line corresponding to that point, which contains infinitely many points of the cumulative point set (Theorem 6.1 (ii));
- if $E/\mathbb{Q}$ has a rational point, then there are lines of well defined number corresponding to that point, and each of them also contains infinitely many points of the cumulative point set (Theorem 7.1 (i) and (ii)).

Furthermore, in both cases, the point sequences lying on these lines are strictly monotone increasing or decreasing according to the L_∞ norm, and they converge to well defined points (Theorem 6.1 (iii) and Theorem 7.1 (iii)).

2. Basic notation

Considering a fixed modulus $m > 1$, the finite residue ring $\mathbb{Z}/m\mathbb{Z}$ is identified with the set $\{0, 1, \ldots, m-1\}$.

Note that if $m = p$ is a prime, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field of p elements. Throughout the paper, if $u, v \in \mathbb{Z}$ with $\gcd(v, m) = 1$ then $u/v \pmod{m}$ denotes that (unique) $w \in \{0, 1, \ldots, m-1\}$ for which $u \equiv vw \pmod{m}$ holds.

Let r_p denote the natural reduction map of the p-integral elements $\mathbb{Z}_{v_p}$ of $\mathbb{Q}$ onto $\mathbb{F}_p$, i.e., $r_p(u/v) := u/v \pmod{p}$, where $u, v \in \mathbb{Z}$ with $\gcd(v, p) = 1$. Note that if $a, m \in \mathbb{Z}$ with $m > 1, 0 < |a| < m$, then $a \pmod{m} = a$ if $a > 0$, and $a \pmod{m} = m + a$ if $a < 0$.

For integers $n \geq 1$ let $\varphi(n)$ denote the Euler phi function, i.e.

$$\varphi(n) = \#\{x \in \mathbb{Z} \mid 1 \leq x \leq n, \gcd(x, n) = 1\}.$$

For $(x_1, x_2) \in \mathbb{R}^2$ let $\|(x_1, x_2)\|$ denote the L_∞ norm of (x_1, x_2), i.e. $\|(x_1, x_2)\| := \max\{|x_1|, |x_2|\}$.

3. Reduction of an elliptic curve over $\mathbb{Q}$ modulo p

Consider an elliptic curve E defined over $\mathbb{Q}$ given by an affine Weierstrass equation of the form

$$E/\mathbb{Q} : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z}, x, y \in \mathbb{Q}) \tag{2}$$

with discriminant Δ. Put

$$p_{min} := \max\{3, |a|, |b|, P(\Delta)\},$$

where $P(\Delta)$ is the greatest prime divisor of Δ.

Reducing the elliptic curve (2) modulo a prime $p > p_{min}$, we obtain an elliptic curve $\widetilde{E}_p$ over $\mathbb{F}_p$ of the form

$$\widetilde{E}_p : y^2 = x^3 + \tilde{a}x + \tilde{b} \quad (\tilde{a}, \tilde{b}, x, y \in \mathbb{F}_p), \tag{3}$$

where $\tilde{a} = r_p(a), \tilde{b} = r_p(b)$.

The elliptic curve $\widetilde{E}_p$ is nonsingular for all primes $p > p_{min}$.

4. Reduction of the points of an elliptic curve over $\mathbb{Q}$ modulo p

An elliptic curve $E(\mathbb{Q})$ can be written as a union of its affine part and the point at infinity. A reduction modulo p, however, cannot map each point of $\mathbb{A}^2(\mathbb{Q})$ into $\mathbb{A}^2(\mathbb{F}_p)$. Namely, if $P = (x, y) \in \mathbb{A}^2(\mathbb{Q})$, then its reduction modulo p is in $\mathbb{A}^2(\mathbb{F}_p)$ if and only if the rational numbers x and y are p-integral.

For the rational points of the curve (2) we have the following statement.

Proposition 4.1 ([5], pp. 68-69)**.** *Let (x, y) be a $\mathbb{Q}$-rational point on the curve $E/\mathbb{Q}$ of the form (2). Then*

$$x = \frac{x_0}{e^2}, \quad y = \frac{y_0}{e^3} \tag{4}$$

for some integers x_0, y_0, e with $e > 0$ and $gcd(x_0, e) = gcd(y_0, e) = 1$.

Hence, if P is a rational point, then either both coordinates are p-integral $(v_p(x), v_p(y) \geq 0)$, or p divides the denominators of both x and y $(v_p(x), v_p(y) < 0)$. Thus we can construct the reduction homomorphism as follows:

$$R_p^{aff} \colon E(\mathbb{Q}) \to \widetilde{E}_p(\mathbb{F}_p) \tag{5}$$

$$P = (x, y) \mapsto \begin{cases} (r_p(x), r_p(y)), & \text{if } P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}, v_p(x), v_p(y) \geq 0; \\ \mathcal{O}, & \text{if } P = \mathcal{O}, \text{ or } P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}, \\ & v_p(x), v_p(y) < 0. \end{cases}$$

where $E/\mathbb{Q}$ and $P = (x, y)$ are in the form (1) and (4) respectively.

5. Mappings of the points of $E(\mathbb{Q})$ and $\widetilde{E}_p(\mathbb{F}_p)$ into $[0,1)^2$

Consider an infinite sequence of elliptic curves $\widetilde{E}_p$ of the form (3) for primes $p > p_{min}$, and define the following sets:

$$\widehat{E}_p := \left\{ \left(\frac{x}{p}, \frac{y}{p} \right) \mid (x, y) \in \widetilde{E}_p(\mathbb{F}_p) \setminus \{\mathcal{O}\}, p > p_{min} \right\},$$

$$\widehat{E} := \bigcup_{p > p_{min}} \widehat{E}_p,$$

and the natural mappings

$$\Omega_p \colon \widetilde{E}_p(\mathbb{F}_p) \setminus \{\mathcal{O}\} \to \widehat{E}_p \subset \widehat{E} \subset [0,1)^2, \quad (x, y) \mapsto \left(\frac{x}{p}, \frac{y}{p} \right).$$

Some basic elementary properties of the mappings Ω_p, and the sets $\widehat{E}_p, \widehat{E}$ are summarized in the following proposition.

Proposition 5.1. *(i) The points of $\widehat{E}_p$ are symmetric to the line $y = \frac{1}{2}$ for all primes $p > p_{min}$.*

(ii) If $x_0y_0 \neq 0, p_1 \neq p_2$ are different primes, $p_1, p_2 > p_{min}$, and $P = (x_0, y_0) \in E(\mathbb{F}_{p_1}) \cap E(\mathbb{F}_{p_2})$, then

$$\Omega_{p_1}(x_0, y_0) \neq \Omega_{p_2}(x_0, y_0).$$

Moreover, the points $\Omega_{p_1}(x_0, y_0), \Omega_{p_2}(x_0, y_0)$ are not on a line parallel either to the x-axis, or to the y-axis.

(iii) If $x_0y_0 \neq 0$, then for each $P \in \widehat{E}$ there is exactly one prime p that $P \in \widehat{E}_p$.

(iv) If $x_0y_0 \neq 0$ then the cardinality of the preimage of $P \in \widehat{E}$ is exactly one, i.e, $\#\Omega_p^{-1}(P) = 1$.

(v) If a rational point $Q = \left(\frac{x_0}{p}, \frac{y_0}{p}\right) \in [0,1)^2$ with $x_0y_0 \neq 0$ does not belong to the image of the mapping Ω_p, i.e., $Q \notin \widehat{E}_p$ for the prime p, then $Q \notin \widehat{E}$.

Proof. *(i)* It follows from the fact that $(x, y) \in E$ implies $(x, -y) \in E$.

(ii) If $P = (x_0, y_0) \in E(\mathbb{F}_{p_1}) \cap E(\mathbb{F}_{p_2})$, then $x, y <\min\{p_1, p_2\}$, thus

$$\Omega_{p_1}(x_0, y_0) = \left(\frac{x_0}{p_1}, \frac{y_0}{p_1}\right) \neq \left(\frac{x_0}{p_2}, \frac{y_0}{p_2}\right) = \Omega_{p_2}(x_0, y_0),$$

since $p_1 \neq p_2$, especially $\frac{x_0}{p_1} \neq \frac{x_0}{p_2}$ and $\frac{y_0}{p_1} \neq \frac{y_0}{p_2}$.

(iii) If p_1, p_2 are primes, then there are not exist integers $0 < x_0 < p_1$ and $0 < x_0' < p_2$ such that $\frac{x_0}{p_1} = \frac{x_0'}{p_2}$, because $x_0 \cdot p_2 = x_0' \cdot p_1$ implies, e.g., $p_1 \mid x_0$ which is, however, contradicts the assumption that $0 < x_0 < p_1$.

(iv) It follows from part *(iii)*.

(v) If $Q = \left(\frac{x_0}{p}, \frac{y_0}{p}\right) \notin \widehat{E}_p$ for the prime p, then, by definition, $Q \notin \widehat{E}_{p'}$ for any other primes p' as well. $\square$

Let $E(\mathbb{Q})_{v_p}$ denote the subset of $E(\mathbb{Q})$ which consists of all points of $E(\mathbb{Q})$ whose both coordinates are p-integral, that is

$$E(\mathbb{Q})_{v_p} := \{(x, y) \mid (x, y) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}, v_p(x), v_p(y) \geq 0, p > p_{min}\}.$$

Restricting the reduction map R_p^{aff} to the subset $E(\mathbb{Q})_{v_p}$

$$R_p^{aff}|_{E(\mathbb{Q})_{v_p}} \colon E(\mathbb{Q})_{v_p} \to \widetilde{E}_p(\mathbb{F}_p), \quad (x, y) \mapsto (r_p(x), r_p(y)),$$

we get the map

$$R_p := \Omega_p \circ R_p^{aff} \colon E(\mathbb{Q})_{v_p} \to \widehat{E}, \quad (x, y) \mapsto \left(\frac{r_p(x)}{p}, \frac{r_p(y)}{p}\right),$$

with $R_p(E(\mathbb{Q})_{v_p}) = \Omega_p(R_p^{aff}(E(\mathbb{Q})_{v_p})) \subset \widehat{E}_p \subset \widehat{E} \subset [0,1)^2$.

6. On the structure of $\widehat{E}$ when $E(\mathbb{Q})$ has an integral point

If $E(\mathbb{Q})$ has an integral point, then $\widehat{E}$ has the following properties. Note that if (x_0, y_0) is an integral point of $E(\mathbb{Q})$, then

$$R_p^{aff}(x_0, y_0) = (x_0(\operatorname{mod} p), y_0(\operatorname{mod} p)) \in \widetilde{E}_p(\mathbb{F}_p)$$

for all primes $p > p_{min}$.

Theorem 6.1. *Let (x_0, y_0) be a fixed integral point of $E(\mathbb{Q})$, where $x_0, y_0 \in \mathbb{Z}$, and $x_0 y_0 \neq 0$.*

(i) The points $R_p(x_0, y_0) = \left(\frac{x_0 \pmod p}{p}, \frac{y_0 \pmod p}{p}\right)$ are different for all primes $p > \max\{|x_0|, |y_0|, p_{\min}\}$.

(ii) The points $R_p(x_0, y_0) = \left(\frac{x_0 \pmod p}{p}, \frac{y_0 \pmod p}{p}\right)$ lie on the lines

$$\begin{array}{lll} y & = \frac{y_0}{x_0} x, & \text{if } x_0 > 0, y_0 > 0, \\ y - 1 & = \frac{y_0}{x_0} x, & \text{if } x_0 > 0, y_0 < 0, \\ y - 1 & = \frac{y_0}{x_0}(x-1), & \text{if } x_0 < 0, y_0 < 0, \\ y & = \frac{y_0}{x_0}(x-1), & \text{if } x_0 < 0, y_0 > 0, \end{array}$$

for primes $p > \max\{|x_0|, |y_0|, p_{\min}\}$.

(iii) The infinite sequence of points

$$\{R_p(x_0, y_0)\}_{p > \max\{|x_0|, |y_0|, p_{\min}\}}$$

is convergent, and $R_p(x_0, y_0) \to (x^*, y^*)$ with

$$(x^*, y^*) = \begin{cases} (0,0), & \text{if } x_0 > 0, y_0 > 0; \\ (0,1), & \text{if } x_0 > 0, y_0 < 0; \\ (1,0), & \text{if } x_0 < 0, y_0 > 0; \\ (1,1), & \text{if } x_0 < 0, y_0 < 0. \end{cases}$$

Furthermore, in each case

$$\|(x^*, y^*) - R_{p_2}(x_0, y_0)\| < \|(x^*, y^*) - R_{p_1}(x_0, y_0)\|$$

for $p_2 > p_1$.

Proof. Statements *(i), (ii), (iii)* will be proved only for the case when $x_0 > 0, y_0 < 0$. For other cases, the proof can be carried out similarly.

(i) For $x_0 > 0, y_0 < 0$, we have

$$R_{p_1}(x_0, y_0) = \left(\frac{x_0}{p_1}, 1 + \frac{y_0}{p_1}\right) \neq \left(\frac{x_0}{p_2}, 1 + \frac{y_0}{p_2}\right) = R_{p_2}(x_0, y_0).$$

(ii) For $x_0 > 0, y_0 < 0$, the point $R_p(x_0, y_0) = \left(\frac{x_0}{p}, 1 + \frac{y_0}{p}\right)$ is on the line $y = \frac{y_0}{x_0} x + 1$, because

$$1 + \frac{y_0}{p} = \frac{y_0}{x_0}\frac{x_0}{p} + 1.$$

(iii) For $x_0 > 0, y_0 < 0$ and $p > \max\{x_0, |y_0|, p_{\min}\}$, we have

$$\begin{aligned} \frac{x_0 \pmod p}{p} &= \frac{x_0}{p} \to 0 \ (p \to \infty), \\ \frac{y_0 \pmod p}{p} &= 1 + \frac{y_0}{p} \to 1 \ (p \to \infty). \end{aligned}$$

Furthermore, if $p_2 > p_1 > \max\{x_0, |y_0|, p_{\min}\}$, then

$$\|(0,1) - R_{p_2}(x_0, y_0)\| \quad < \quad \|(0,1) - R_{p_1}(x_0, y_0)\|$$

if and only if

$$\begin{aligned} &\left\| \left(\frac{x_0 \pmod{p_2}}{p_2}, 1 - \frac{y_0 \pmod{p_2}}{p_2} \right) \right\| \\ \leq &\left\| \left(\frac{x_0 \pmod{p_1}}{p_1}, 1 - \frac{y_0 \pmod{p_1}}{p_1} \right) \right\|. \end{aligned}$$

However,

$$\begin{aligned} &\max\left\{ \frac{x_0 \pmod{p_2}}{p_2}, 1 - \frac{y_0 \pmod{p_2}}{p_2} \right\} = \max\left\{ \frac{x_0}{p_2}, 1 - \frac{p_2 + y_0}{p_2} \right\} \\ < \; &\max\left\{ \frac{x_0}{p_1}, 1 - \frac{p_1 + y_0}{p_1} \right\} = \max\left\{ \frac{x_0 \pmod{p_1}}{p_1}, 1 - \frac{y_0 \pmod{p_1}}{p_1} \right\}. \end{aligned}$$

□

7. On the structure of $\widehat{E}$ when $E(\mathbb{Q})$ has a rational point

Throughout this section, let $(\frac{x_0}{e^2}, \frac{y_0}{e^3})$ be a fixed rational point of $E(\mathbb{Q})$, where $x_0, y_0, e \in \mathbb{Z}$ with $e > 1$, $\gcd(x_0, e) = \gcd(y_0, e) = 1$, $x_0 y_0 \neq 0$.

If $E(\mathbb{Q})$ has a rational point, then $\widehat{E}$ has the following properties.

Theorem 7.1. *(i) For all primes $p > \max\{|x_0|, |y_0|, e^3, p_{\min}\}$ the points $R_p\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right)$ lie on lines of the form*

$$l_i : \quad y - A_i \quad = \quad \frac{y_0}{e x_0}\left(x - B_i\right), \tag{6}$$

where $(A_i, B_i) = (\frac{i}{e^3}, \frac{i x_0 / y_0 \pmod{e^2}}{e^2})$ with $0 < i < e^3$, $gcd(i, e^3) = 1$.

(ii) The number of l_i is $\varphi(e^3)$, and each of them contains infinitely many points of the form $R_p(\frac{x_0}{e^2}, \frac{y_0}{e^3})$.

(iii) For all i the infinite sequence of the points

$$\left\{ R_p\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right) \right\}_{p > \max\{|x_0|, |y_0|, e^3, p_{\min}\}}$$

on the line l_i is convergent, and

$$R_p\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right) \to (B_i, A_i)\,(p \to \infty). \tag{7}$$

Furthermore, for primes $p_2 > p_1 > \max\{|x_0|, |y_0|, e^3, p_{\min}\}$ *with*

$$p_1 \equiv p_2 \equiv -y_0/i \pmod{e^3}$$

we have

$$\left\|(B_i, A_i) - R_{p_2}\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right)\right\| < \left\|(B_i, A_i) - R_{p_1}\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right)\right\|,$$

and the sequences $\left\{\frac{r_p(x_0/e^2)}{p}\right\}$ *and* $\left\{\frac{r_p(y_0/e^3)}{p}\right\}$ *are strictly monotone increasing or decreasing if* $x_0 < 0$ *or* $x_0 > 0$ *and* $y_0 < 0$ *or* $y_0 > 0$ *respectively.*

To prove the theorem, we need the following statement.

Lemma 7.2. *With the notation of Theorem 7.1, for* $p > \max\{|x_0|, |y_0|\}$ *with* $i = -y_0/p \pmod{e^3}$ *we have*

$$\frac{y_0}{e^3} \pmod{p} = pA_i + \frac{y_0}{e^3}, \quad \frac{x_0}{e^2} \pmod{p} = pB_i + \frac{x_0}{e^2}.$$

Proof. We are going to proof only the equation $\frac{x_0}{e^2} \pmod{p} = pB_i + \frac{x_0}{e^2}$, the other one can be proved similarly.

Since $i = -y_0/p \pmod{e^3}$, the congruence $i \equiv -y_0/p \pmod{e^2}$ holds, thus $B_i = \frac{-x_0/p \pmod{e^2}}{e^2}$. It only remains to show that

$$(x_0/e^2 \pmod{p}) \cdot e^2 \equiv (-x_0/p \pmod{e^2}) \cdot p + x_0 \pmod{p}, \text{ and}$$

$$0 \le (-x_0/p \pmod{e^2}) \cdot p + x_0 < pe^2.$$

The congruence obviously holds, and the inequalities follow from the facts that $1 \le -x_0/p \pmod{e^2} \le e^2 - 1$ and $-p < x_0 < p$.

$\square$

Proof of the theorem. We return to the proof of Theorem 7.1.

(i) Clearly, $R_p\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right) \in \widehat{E}_p \subset \widehat{E}$.

Substituting the number $\frac{\frac{y_0}{e^3} \pmod{p}}{p}$ for y in the left side of equation (6), and applying Lemma 7.2 we have:

$$\frac{\frac{y_0}{e^3} \pmod{p}}{p} - A_i = \frac{pA_i + \frac{y_0}{e^3}}{p} - A_i = \frac{y_0}{pe^3}.$$

Substituting the number $\frac{\frac{x_0}{e^2} \pmod{p}}{p}$ for x in the right side of equation (6), and applying Lemma 7.2 we have:

$$\frac{y_0}{ex_0}\left(\frac{\frac{x_0}{e^2} \pmod{p}}{p} - B_i\right) = \frac{y_0}{ex_0}\left(\frac{pB_i + \frac{x_0}{e^2}}{p} - B_i\right) = \frac{y_0}{pe^3}.$$

(ii) It is obvious that $\#\{l_i \mid 0 < i < e^3, \gcd(i, e^3) = 1\} = \varphi(e^3)$.

Furthermore, there are exist infinitely many primes for which $p \equiv -y_0/i \pmod{e^3}$ holds because of the Dirichlet's theorem on primes in arithmetical progressions ([1], Chap. 7).

(iii) It follows from the definition of R_p and Lemma 7.2, e.g., for $p > \max\{|x_0|, |y_0|\}$ with $i = -y_0/p \pmod{e^3}$ we have

$$\text{(8)}\quad \frac{r_p(\frac{x_0}{e^2})}{p} = \frac{\frac{x_0}{e^2} \pmod{p}}{p} = \frac{pB_i + \frac{x_0}{e^2}}{p} = B_i + \frac{x_0}{pe^2} \to B_i \quad (p \to \infty).$$

From (8) it follows immediately that the sequence $\left\{\frac{r_p(x_0/e^2)}{p}\right\}$ strictly monotone increase or decrease depending on $x_0 < 0$ or $x_0 > 0$.

By Lemma 7.2 we get

$$\begin{aligned}
&\left\|\left(B_i - \frac{\frac{x_0}{e^2} \pmod{p_2}}{p_2}, A_i - \frac{\frac{y_0}{e^3} \pmod{p_2}}{p_2}\right)\right\| \\
&= \left\|\left(-\frac{x_0}{p_2e^2}, -\frac{y_0}{p_2e^3}\right)\right\| = \max\left\{\left|-\frac{x_0}{p_2e^2}\right|, \left|-\frac{y_0}{p_2e^3}\right|\right\} \\
&< \max\left\{\left|-\frac{x_0}{p_1e^2}\right|, \left|-\frac{y_0}{p_1e^3}\right|\right\} = \left\|\left(-\frac{x_0}{p_1e^2}, -\frac{y_0}{p_1e^3}\right)\right\| \\
&= \left\|\left(B_i - \frac{\frac{x_0}{e^2} \pmod{p_1}}{p_1}, A_i - \frac{\frac{y_0}{e^3} \pmod{p_1}}{p_1}\right)\right\|.
\end{aligned}$$

$\square$

Remark 7.3. Theorem 7.1 is also true for primes $p < e^3$ with $\gcd(p, e) = 1$. However, we are interested in the asymptotic behavior of the sequence $R_p\left(\frac{x_0}{e^2}, \frac{y_0}{e^3}\right)$. Thus, for the sake of simplicity of the treatment, we can put aside finitely many primes.

Acknowledgements. I would like to thank Prof. Dr. A. Pethő for the basic idea of this article and helpful discussions and suggestions, and Dr. T. Herendi, Dr. T. Mihálydeák for effective help.

I also would like to thank the anonymous referee for careful reading of the manuscript and for many useful comments and suggestions.

References

[1] T. M. Apostol. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. New York-Heidelberg-Berlin: Springer-Verlag, 1976.

[2] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Semin. Hansische Univ.*, 14:197–272, 1941.

[3] A. W. Knapp. *Elliptic Curves.* Mathematical Notes (Princeton). 40. Princeton University Press, 1992.

[4] J. H. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, 1986.

[5] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

Received January 17, 2007.

Department of Health Informatics,
Health College Faculty,
University of Debrecen
Sóstói u. 2–4.,
H-4400 Nyíregyháza,
Hungary
E-mail address: csajzo@freemail.hu; csajzo@de-efk.hu