Periodic points for good reduction maps on curves *

Manfred Einsiedler (manfred.einsiedler@univie.ac.at)
Institut für Mathematik, Universität Wien, Strudlhofgasse 4, A-1090 Vienna, Austria

Graham Everest (g.everest@uea.ac.uk) and Thomas Ward (t.ward@uea.ac.uk)
School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom

Abstract. The periodic points of a morphism of good reduction for a smooth projective curve with good reduction over $\overline{\mathbb{Q}}_p$ form a discrete set. This is used to give an interpretation of the morphic height in terms of asymptotic properties of periodic points, and a morphic analogue of Jensen's formula.

Keywords: Morphism of good reduction, Periodic points, Morphic heights

Mathematics Subject Classification (2000): 11S05, 37F10

1. Introduction and Results

In this paper we study the behaviour of periodic points for a morphism on a smooth curve over $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$, with p-adic norm $|\cdot|$ normalized to have $|p| = 1/p$. Under a regularity condition, we prove that the asymptotic distance of a given point to the periodic points is equal to one in a suitable metric. This result generalises the case of polynomial morphisms on the projective line in [4].

Let $O_p = \{z \in \overline{\mathbb{Q}}_p \mid |z| \leq 1\}$ be the ring of integers in $\overline{\mathbb{Q}}_p$, with maximal ideal $\mathfrak{p} = \{z \in \overline{\mathbb{Q}}_p \mid |z| < 1\}$. Identify the quotient $O_p/\mathfrak{p}$ with the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let $\mathbb{P}^n(\overline{\mathbb{Q}}_p)$ denote n-dimensional projective space over $\overline{\mathbb{Q}}_p$, and write $X = (X_0, \ldots, X_n) \in \overline{\mathbb{Q}}_p^{n+1}$ for the homogeneous coordinates of a point $[X] \in \mathbb{P}^n(\overline{\mathbb{Q}}_p)$. It will be useful always to choose the homogeneous coordinates to have

$$|X| = \max\{|X_0|, \ldots, |X_n|\} = 1. \tag{1}$$

Writing $x = [X], y = [Y]$, define a function on $\mathbb{P}^n(\overline{\mathbb{Q}}_p)$ by

$$\Delta(x, y) = \max_{i,j} |X_i Y_j - X_j Y_i|. \tag{2}$$

* The first author was supported by EPSRC Grant GR/M 49588, LMS Scheme 4 grant 4627 and FWF Project P14379; the authors thank two anonymous referees for their comments.

Then, just as in the one-dimensional case (see [3] for example), Δ is a metric. In this metric, projective space $\mathbb{P}^n(\overline{\mathbb{Q}}_p)$ has diameter one. The regularity property used here – *good reduction* – will be defined in the next section.

A point $x \in C$ is a *fixed point for* a map $\phi : C \to C$ if $\phi(x) = x$, is a *point of period* n if $\phi^n(x) = x$, and has *least period* n if x is periodic (of period n) and the orbit $\{x, \phi(x), \phi^2(x), \ldots\}$ has cardinality n.

THEOREM 1. *Let $C \subseteq \mathbb{P}^n(\overline{\mathbb{Q}}_p)$ be an irreducible smooth curve with good reduction, and let $\phi : C \to C$ be a morphism of good reduction with degree $d > 1$. Then for every point $x \in C$ there is a constant κ_x with*

$$\Delta(x, y) \geq (\kappa_x |n|)^{1/n}$$

for any ϕ-periodic point y with least period n.

COROLLARY 2. *For every point $x \in C$, and every $r < 1$, the number of points $y \in C$ that are periodic under ϕ and satisfy $\Delta(x, y) < r$ is finite.*

The Riemann–Hurwitz formula [5, Sect. IV.2] shows that

$$(2 - 2g)(d - 1) \geq 0$$

where g is the genus of the curve C, since the ramification divisor of ϕ is non-negative. In particular, the hypothesis of Theorem 1 implies that C has genus 0 or 1.

In the case of the projective line $C = \mathbb{P}^1(\overline{\mathbb{Q}}_p)$ there are infinitely many periodic points (see [1, Theorem 6.2.2]; it is enough to prove this over any field). The proof of Theorem 1 simplifies in this case. If the point at infinity of the projective line is fixed by ϕ, then the periodic points of the morphism are related to the *morphic height* associated to ϕ (cf. Theorem 3 below; the morphic height is defined in [3]).

A rational function ϕ has *good reduction* modulo p if it can be written in homogeneous coordinates in the form

$$\phi(X, Y) = (F(X, Y), G(X, Y)) \text{ with } F, G \in O_p[X, Y]$$

where F and G have no common root modulo $\mathfrak{p}$ (see [2], [3] and [14]). Write $\lambda_{\phi,p}$ for the local morphic height (sometimes called the canonical local height in the literature) as defined in [3].

THEOREM 3. *Let $\phi : \mathbb{P}^1(\overline{\mathbb{Q}}_p) \to \mathbb{P}^1(\overline{\mathbb{Q}}_p)$ be a rational function of good reduction and degree $d > 1$. Assume that the point $(0, 1)$ at infinity is* *fixed under* ϕ. *Fix a point* $x \in \overline{\mathbb{Q}}_p$, *and a sequence* $y_n \in \overline{\mathbb{Q}}_p$ *of points of least period* n *under* ϕ. *Then*

$$\frac{|x - y_n|}{\max(1, |x|)\max(1, |y_n|)} \to 1 \text{ for } n \to \infty.$$

Moreover,

$$\log|x - y_n| \to \lambda_{\phi,p}(x) = \log^+ |x|_p$$

and, if x *is not a periodic point, then*

$$\frac{1}{d^n} \log|f_n(x) - x g_n(x)| \to \lambda_{\phi,p}(x) = \log^+ |x|$$

where $\phi^n = \frac{f_n}{g_n}$, *so* $f_n(t) - t g_n(t)$ *is the polynomial whose roots are exactly the periodic points of period* n.

Notice that there are infinitely many points whose least period exceeds 1 (cf. Remark 6). Theorem 3 is a morphic analogue of Jensen's classical formula (see Section 3). We should point out that a paper of Lubin [10] contains results closely related to those presented here, and Hua–Chieh Li has made an extensive study [7], [8], [9], of periodic points for p-adic power series, mainly aimed at counting the points of given period. Finally, Morton and Silverman [12] studied the multiplicities of periodic points and used this to construct algebraic units in number fields.

2. Proofs of theorems

In this section we prove Theorems 1 and 3 assuming some results on good reduction curves and uniformizers that will be proved later. Recall that $X = (X_1, \dots, X_n)$ always denotes the homogeneous coordinates of a point $x = [X] \in C$ chosen so that Equation (1) holds.

Let $\pi : \mathbb{P}^n(\overline{\mathbb{Q}}_p) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$ be the reduction map, defined by

$$\pi(x) = [X_0 + \mathfrak{p}, X_1 + \mathfrak{p}, \dots, X_n + \mathfrak{p}],$$

which is well-defined by (1). Let C be an irreducible projective curve in $\mathbb{P}^n(\overline{\mathbb{Q}}_p)$, with ideal of relations $I = I(C)$. Let $J = I \cap O_p[T_0, \dots, T_n]$ be generated by the forms $f_1, \dots, f_t$. Fix a point $y \in C$, and assume without loss of generality that $Y_0 \neq 0$. The curve is *non-singular at* y if

$$\operatorname{rank}\left(\frac{\partial g_i}{\partial U_j}(y)\right)_{i,j} = n - 1, \tag{3}$$

where $g_i(U_1, \ldots, U_n) = f_i(1, U_1, \ldots, U_n)$. The curve C is *smooth* if it is non-singular at every point.

Define $\overline{J} = J \bmod \mathfrak{p} \subset \overline{\mathbb{F}}_p[T_0, \ldots, T_n]$, and let $\overline{C} \subset \mathbb{P}^n(\overline{\mathbb{F}}_p)$ be the variety defined by the ideal $\overline{J}$ (which of course may not in general coincide with the ideal of relations of the algebraic set $\overline{C}$). The curve C has *good reduction* if (3) holds mod $\mathfrak{p}$ for every $\bar{y} \in \overline{C}$. From now on we will assume that the curve C is smooth with good reduction.

The metric (2) on an integral affine piece simplifies as follows: for $x = [X], y = [Y] \in \mathbb{P}^n(\overline{\mathbb{Q}}_p)$ with $X_0 = 1, Y_0 = 1$ and $X_i, Y_i \in O_p$,

$$\Delta(x, y) = \max_i |Y_i - X_i|.$$

A rational function $f = F/G$ on C is defined by two forms F and G in $\overline{\mathbb{Q}}_p[T_0, \ldots, T_n]$ of the same degree with $G \notin I(C)$. A rational function is *regular at* $x \in C$ if there are two forms F', G' with $G'(X) \neq 0$ and $FG' - F'G \in I$ (in other words $f = F'/G'$). Moreover, f is *regular at* $\bar{x} \in \overline{C} \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_p)$ if there are two forms $F', G' \in O_p[T_0, \ldots, T_n]$ such that $G'(\bar{X}) \neq 0$, $FG' - F'G \in I$, and $\bar{X} \in \overline{\mathbb{F}}_p^{n+1}$ is a homogeneous coordinate of $\bar{x}$. In that case $\overline{f} = \overline{F}/\overline{G}$ defines a rational function on $\overline{C}$ which is regular at $\bar{x} \in \overline{C}$.

A *uniformizer* of C at $x \in C$ is a rational function z which is regular at x, such that the vector $(\frac{\partial z}{\partial U_i})_i$ is not in the image of the matrix in (3).

PROPOSITION 9 (cf. Section 4.) *Fix a point $x \in C$. Then there exists a uniformizer z of C at x such that z is regular at $\pi(x)$ and $\overline{z}$ is a uniformizer at $\pi(x)$. The restriction $z : U \to \mathfrak{p}$ of z to $U = \{y \in C \mid \Delta(y, x) < 1\}$ is a bijection and its inverse, in each affine coordinate, is a convergent power series with coefficients in O_p. Hence $\Delta(y, y') = |z(y) - z(y')|$ for all $y, y' \in U$.*

For example, if the curve is $\mathbb{P}^1(\overline{\mathbb{Q}}_p)$ and $X = (1, 0)$, one may choose $z(y) = \frac{Y_1}{Y_0}$ for the uniformizer in Proposition 9.

Now let $\phi : C \to C$ be a morphism, defined by forms

$$(F_0, \ldots, F_n) \in \overline{\mathbb{Q}}_p[T_0, \ldots, T_n]^{n+1}$$

of the same degree, with $F_j \notin I(C)$ for some j. Since ϕ is a map from C to C, $f(F_0, \ldots, F_n) \in I(C)$ for every $f \in I(C)$. In order for ϕ to be defined on all of C, at each $x = [X] \in C$ there must be a representation

$$(G_0, \ldots, G_n) \in \overline{\mathbb{Q}}_p[T_0, \ldots, T_n]^{n+1} \tag{4}$$

of the morphism, with

$$F_i G_j - F_j G_i \in I(C) \text{ for } 0 \leq i, j \leq n \tag{5}$$

and

$$(G_0(X), \ldots, G_n(X)) \neq (0, \ldots, 0). \tag{6}$$

Here (5) means that the forms $(G_0, \ldots, G_n)$ define the same map as the forms $(F_0, \ldots, F_n)$ do, and (6) means that ϕ is well defined at x.

The morphism $\phi : C \to C$ has *good reduction* if for every $\bar{x} \in \overline{C}$, there is a representation

$$(G_0, \ldots, G_n) \in O_p[T_0, \ldots, T_n]^{n+1}$$

of ϕ satisfying (5) such that

$$(G_0(\bar{X}), \ldots, G_n(\bar{X})) \notin \mathfrak{p}^{n+1}.$$

Here $\mathfrak{p}^{n+1}$ denotes the $(n+1)$-fold Cartesian product of $\mathfrak{p}$ and $\bar{X}$ is a homogeneous coordinate for $\bar{x} \in \overline{C} \subseteq \overline{\mathbb{F}}_p^{n+1}$.

In the case of $C = \mathbb{P}^1(\overline{\mathbb{Q}}_p)$, there exists a canonical representation (F_0, F_1) satisfying (6) for all $x \in \mathbb{P}^1(\overline{\mathbb{Q}}_p)$. We can assume that $F_0, F_1 \in O_p[T_0, T_1]$ and at least one of the two polynomials has a coefficient in $O_p^\times$. Then the morphism ϕ has good reduction if and only if the two forms $\overline{F_0}, \overline{F_1}$ do not have a common zero on $\mathbb{P}^1(\overline{\mathbb{F}}_p)$ – they define a rational function on $\mathbb{P}^1(\overline{\mathbb{F}}_p)$.

REMARK 4. *A morphism $\phi : C \to C$ has good reduction in the above sense if and only if it extends to a morphism over the scheme Spec(O_p).*

From now on we will assume that ϕ is a morphism of good reduction.

Let K denote the field of rational functions on C. The degree of the morphism ϕ is defined as the degree of the field extension $[K : \phi^*(K)]$, where

$$\begin{aligned} \phi^* \ : \ & K \to K \\ & f \mapsto f \circ \phi \end{aligned}$$

is the map induced by ϕ. Alternatively, one can define the degree as the common number of pre-images (counted with multiplicities) of points under the map ϕ.

In the case of a rational function ϕ on $\mathbb{P}^1(\overline{\mathbb{Q}}_p)$ this is again obvious since the degree d of ϕ coincides with the degree of the forms in the canonical representation (F_0, F_1).

COROLLARY 11 (cf. Section 4.) *Let $\phi : C \to C$ be a morphism of good reduction, and let $x \in C$ be a fixed point. Then there exists a uniformizer z, also satisfying Proposition 9, such that*

$$\phi^* z = z \circ \phi = \sum_{i=1}^{\infty} a_i z^i \text{ with } a_i \in O_p.$$

Again if $C = \mathbb{P}^1(\overline{\mathbb{Q}}_p)$ and ϕ is a rational function on $\mathbb{P}^1(\overline{\mathbb{Q}}_p)$ with good reduction, it is easy to see that Corollary 11 holds: Assume $X = (1, 0)$, then $z(y) = \frac{Y_1}{Y_0}$ is a uniformizer at x, and

$$\phi^* z(y) = \frac{F_1(Y)}{F_0(Y)}.$$

Since x is a fixed point, $F_1(X) = 0$ and $F_0(X) \neq 0$. Moreover, ϕ has good reduction and therefore $F_0(X) \notin \mathfrak{p}$. Changing to the affine coordinate z, write $\phi^* z = \frac{f_1(z)}{f_0(z)}$ with $f_1(0) = 0$ and $|f_0(0)| = 1$. Since the constant term of f_0 is a unit in O_p, the polynomial f_0 is a unit in $O_p[[z]]$. So the rational function $\phi^* z \in O_p[[z]]$ satisfies Corollary 11.

LEMMA 5. *Let $f(z) = \sum_{i=1}^{\infty} a_i z^i$ be a power series with coefficients $a_i \in O_p$. Then, for any $n > 1$,*

$$f^n(z) = a_1^n z + z^2 g_n,$$

where $g_n \in O_p[[z]]$. Assume now that $a_1 = 1$ and let e be the first index $e > 1$ with $a_e \neq 0$, so that $f(z) = z + z^e g$ for some $g \in O_p[[z]]$. For any $n > 1$ there exists a power series $h_n \in O_p[[z]]$ with

$$f^n(z) = z + nz^e g + z^{2e-1} h_n.$$

This may be seen by a simple induction argument. For the proof of the second statement, notice that $g(z + z^e F(z)) = g(z) + z^e G(z)$ for some G depending on g and F. Note also that Lemma 5 played an important role in [12].

REMARK 6. *Some rather general properties of periodic points in the setting are needed later and assembled here.*

1. *The second statement in Lemma 5 can be used to show that if a point x is a multiple root of $f^n(z) - z = 0$, then it is never a higher multiplicity root of any other equation of the form $f^m(z) - z = 0$ (notice this is only true for multiplicity two or higher). In particular, if $x \in C$ is a point of period n for ϕ with multiplicity two or higher, then that multiplicity cannot increase when x is viewed as a point with period $m > n$.*

2. *If the curve is $\mathbb{P}^1(\overline{\mathbb{Q}}_p)$ then many of the roots of $\phi^n(z) - z = 0$ are genuine points with least period n, and in particular there are infinitely many points whose least period exceeds any given number.*

3. *Any map for which the number of points of period n grows exponentially fast will have the same exponential rate of growth in the number of points of least period n (cf. [13]). In fact if p_n is the number of periodic points of period n and p_n^* is the number of periodic points of least period n, then $p_n^*/p_n \to 1$ for $n \to \infty$.*

LEMMA 7. *Let $f(z) = \sum_{i=1}^{\infty} a_i z^i$ be a power series with coefficients $a_i \in O_p$ such that $|a_1 - 1| < p^{-1/(p-1)}$. Then every periodic point $y \in \mathfrak{p} \setminus \{0\}$ of f of least period $n \geq 1$ satisfies*

$$|y| \geq (\kappa |n|)^{1/n},$$

where the constant $\kappa > 0$ does not depend on n.

Proof. The assumptions on f imply that $|f(y)| \leq |y|$ for any $y \in \mathfrak{p}$. So if $y \in \mathfrak{p}$ is a periodic point of least period n, then the points $y_1 = y, y_2 = f(y), \ldots, y_n = f^n(y)$ along the orbit of y all have the same norm.

Suppose first that $a_1 \neq 1$. From the p-adic logarithm (see [6, Sect. IV.1]) it follows that for every integer $n \geq 1$, $|a_1^n - 1| \geq \kappa |n|$, where $\kappa = |\log_p a_1|$. Consider the power series

$$F_n(z) = f^n(z) - z = \sum_{i=1}^{\infty} b_i z^i \in O_p[[z]]; \tag{7}$$

the first nontrivial term for this series is $b_1 = a_1^n - 1$. If y is a periodic point in $\mathfrak{p} \setminus \{0\}$ of least period n, then all the points y_i on the orbit of y are roots of the equation $F_n(z) = 0$. From the usual Newton polygon arguments (see for example [6, Sect. IV.4]) we see that $\log |y| = \log |y_i| < 0$ equals one of the slopes of the Newton polygon of F, say the slope between the points P_k and P_ℓ defined by the coefficients b_k and b_ℓ with $k < \ell$ (cf. Figure 1). Since $\ell - k$ is exactly the number

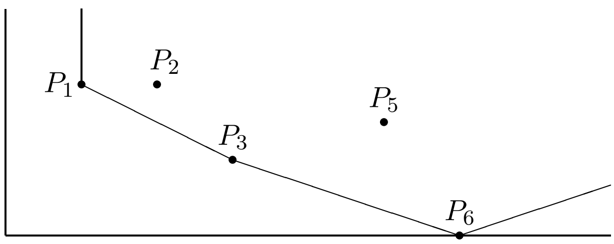

Figure 1. The Newton polygon of F is defined by the points $P_i = (i, -\log |b_i|)$. The slopes determine the norms of the roots.

of roots whose norm equals the slope, we get $\ell - k \geq n$. Furthermore $|b_1| \leq |b_k|$, because otherwise the point defined by b_k is higher in the

Newton polygon and the slope between the points P_k and P_ℓ is positive – contradicting $|y| < 1$. Furthermore, $|b_\ell| \leq 1$ and

$$\frac{\log|b_1|}{n} \leq \frac{\log|b_1| - 0}{\ell - k} \leq \frac{\log|b_k| - \log|b_\ell|}{\ell - k} = \log|y|.$$

Together with the estimate on $b_1 = a_1^n - 1$, this proves the lemma in the case $a_1 \neq 1$.

If $a_1 = 1$, choose $\kappa = |b_e|$, where b_e is the first non-zero coefficient in (7), use the second equation in Lemma 5, and deduce in a similar fashion the same inequality.

We are grateful to a referee for pointing out that the condition

$$|a_1 - 1| < p^{-1/(p-1)}$$

in the hypotheses of Lemma 7 can be removed entirely by arguing as follows. Let $m \geq 1$ be the smallest integer with $|a_1^m - 1| < p^{-1/(p-1)}$. If $a_1^m \neq 1$, then choose $\kappa = |\log_p(a_1^m)|$. For $n \geq 1$,

$$|a_1^n - 1| \geq |a_1^{mn/d} - 1| \geq \kappa|n/d| \geq \kappa|n|$$

where $d = \gcd(m, n)$; the second inequality being arrived at as in the proof above. If $a_1^m = 1$, then choose $\kappa = |a_{m,e}|$, where $a_{m,e}$ is the coefficient of z^e in the expansion of $F_m(z) = f^m(z) - z$ and $e \geq 2$ is the smallest integer for which this is non-zero. Let b_e be the coefficient of the z^e term of $F_{mn/d}$ ($d = \gcd(m, n)$ as before). By Lemma 7, $b_e = \frac{n}{d} a_{m,e}$, so $|b_e| \geq \kappa|n|$. The equation $F_{mn/d}(z) = 0$ has at least n distinct roots of norm $|y|$ for any point y with least period n under ϕ; the rest of the argument proceeds as before.

Proof of Theorem 1. We begin the proof with the case where x itself is a periodic point. Clearly every periodic point for ϕ is also a periodic point for a power of ϕ. So it is enough to consider the case where x is a fixed point.

By Proposition 9 and Corollary 11 the action of ϕ in the open unit disk U with centre x with respect to the metric Δ is conjugate to the action of a power series $f(z) = \sum_{i=1}^{\infty} a_i z^i$ on $\mathfrak{p}$. If $|a_1| < 1$, then it is easy to see that $|f(y)| < |y|$ for any $y \in \mathfrak{p} \setminus \{0\}$. So there cannot be any periodic points in $\mathfrak{p}$ other than 0. For ϕ this means that there is no periodic point $y \in C$ with $\Delta(y, x) < 1$.

Assume now $|a_1| = 1$. Then, for some n, $|a_1^n - 1| < 1/p$. As before, without loss of generality replace ϕ by ϕ^n and assume $|a_1 - 1| < 1/p$. Lemma 7 shows that there are only finitely many periodic points $y \in \mathfrak{p}$ for f with $|y| < r$. This shows the theorem for periodic points.

Assume now x is an arbitrary point. If there is no periodic point y with $\Delta(x,y) < 1$, the statement is trivial. So assume that for some periodic point y, $R = \Delta(x,y) < 1$. By the above we know $\Delta(y,y') < r$ holds for only finitely many periodic points y'. If $R < r < 1$, then the ultrametric inequality shows that the discs around the centre points x resp. y with radius r agree; the theorem follows.

Proof of Theorem 3. The first statement simply specializes Theorem 1. For the second, notice that Theorem 1 applied to the point at infinity implies that $\log^+|y_n| \to 0$, so $\log|x - y_n| - \log^+|x| \to 0$. The third follows by factorizing the polynomial $f_n(t) - tg_n(t)$ and noting that most roots of $f_n(t) - tg_n(t) = 0$ are points with least period n (cf. Remark 6).

3. Examples

In this section, we are going to present several examples to exhibit our main conclusions. The first example explains the earlier remark that Theorem 3 is a version of Jensen's Formula.

3.1. Jensen's formula and squaring

Assume that $p > 2$ and let $f(z) = z^2$. This map gives rise to a good reduction morphism on $\mathbb{P}^1(\overline{\mathbb{Q}}_p)$ with degree 2. Theorem 3 shows that

$$\lim_{n\to\infty} 2^{-n} \sum_{\zeta^{2^n}=\zeta} \log|\zeta - x|_p = \log^+|x|_p.$$

Working over $\mathbb{C}$ instead of $\overline{\mathbb{Q}}_p$ the sum on the left would tend to the integral over the unit circle, and the statement would be exactly Jensen's Formula. For more details on this point of view, see [4].

3.2. Local height on an elliptic curve

Let a and b denote elements of $\overline{\mathbb{Q}}_p$ with the property that $4a^3 + 27b^2$ does not reduce to zero. For $p > 2$, the morphism of degree 4 on $\mathbb{P}^1(\overline{\mathbb{Q}}_p)$ defined by

$$f(X,Y) = \Big(X^4 - 2aX^2Y^2 - 8bXY^3 + a^2Y^4, 4Y(X^3 + aXY^2 + bY^3)\Big)$$

has good reduction at p. If the underlying elliptic curve

$$y^2 = x^3 + ax + b$$

is in minimal form at the prime p, then our results show that the (unnormalized) local height of the point $Q = (x(Q), y(Q))$ can be expressed as a limit

$$\lim_{n\to\infty} 4^{-n} \sum_{2^n P=0} \log |x(P) - x(Q)|_p.$$

This example comes about from the duplication map on the elliptic curve. The reduction condition guarantees that the elliptic curve has non-singular reduction, and the condition $p > 2$ guarantees that the duplication morphism has good reduction. This can all be generalized to the multiplication by m map, and we can also handle the case of an elliptic curve embedded in projective space in a non-trivial way.

3.3. Segre embedding

Let E denote an elliptic curve defined over $\overline{\mathbb{Q}}_p$ with non-singular reduction. Initially, think of E embedded in $\mathbb{P}^2(\overline{\mathbb{Q}}_p)$. For any positive integers k and ℓ, map the curve $kE \times \ell E$ to $\mathbb{P}^8(\overline{\mathbb{Q}}_p)$ via the Segre embedding (this means we map $E \to E \times E$ using the map $P \mapsto (kP, \ell P) \in \mathbb{P}^2 \times \mathbb{P}^2$ and then embed the image in $\mathbb{P}^8$ via the Segre embedding; if $\gcd(k, \ell) = 1$ this is an embedding of E). The map $Q \mapsto mQ$, where m is co-prime to p, induces a morphism on this curve to which Theorem 1 applies.

Notice that this is not essentially different to Section 3.2, but gives an example of how curves can occur in higher-dimensional projective space.

4. Background results on the curve and the morphism

Let $C \subseteq \mathbb{P}^n(\overline{\mathbb{Q}}_p)$ be an irreducible projective smooth curve with good reduction. For $x \in C$, the ring of regular functions at x is defined by

$$\mathcal{O}_x = \{f \mid f \text{ is a rational regular function on } C \text{ at } x\}.$$

For $\pi(x) \in \overline{C}$, define similarly

$$\mathcal{O}_{\pi(x)} = \{f \mid f \text{ is a rational regular function on } C \text{ at } \pi(x)\}.$$

Notice that these two rings have quite different properties. For instance, for $x \in C$, $\mathcal{O}_x$ is an algebra over $\overline{\mathbb{Q}}_p$, and

$$\langle 0 \rangle \subseteq \{f \in \mathcal{O}_x \mid f(x) = 0\}$$

is a maximal chain of prime ideals in $\mathcal{O}_x$. On the other hand, $\mathcal{O}_{\pi(x)}$ is an algebra over O_p, and

$$\langle 0 \rangle \subseteq \{f \in \mathcal{O}_{\pi(x)} \mid f(x) = 0\} \subseteq \{f \in \mathcal{O}_{\pi(x)} \mid |f(x)| < 1\}$$

is a maximal chain of prime ideals in $\mathcal{O}_{\pi(x)}$. Hence, the Krull dimension of $\mathcal{O}_x$ is equal to 1, while that of $\mathcal{O}_{\pi(x)}$ is equal to 2.

PROPOSITION 8. *Let $x \in C$. Any function $z \in \mathcal{O}_{\pi(x)}$ which vanishes at x, and maps modulo $\mathfrak{p}$ to a uniformizer $\overline{z}$ at $\pi(x)$ for $\overline{C}$, is a uniformizer at x for C. If $f \in \mathcal{O}_{\pi(x)}$ vanishes at x, then there exists $g \in \mathcal{O}_{\pi(x)}$ such that $f = zg$. The local power series*

$$f(z) = \sum_{i=0}^{\infty} a_i z^i$$

satisfies $a_i \in O_p$. Let $y \in C$ with $\Delta(x, y) < 1$, then

$$f(y) = \sum_{i=0}^{\infty} a_i z(y)^i. \tag{8}$$

Proof. Let $x = [X] \in C$, $z \in \mathcal{O}_{\pi(x)}$ be as in the statement of Proposition 8. Assume that $X_0 = 1$, and work in affine coordinates. Let

$$I_0 \subseteq \overline{\mathbb{Q}}_p[U_1, \ldots, U_n] \text{ and } J_0 = I_0 \cap O_p[U_1, \ldots, U_n]$$

be the affine ideals corresponding to the homogeneous ideals I and J. Let

$$\mathfrak{m}_x = \langle U_1 - X_1, \ldots, U_n - X_n \rangle \subseteq \overline{\mathbb{Q}}_p[U_1, \ldots, U_n]$$

be the maximal ideal at x, and define a map

$$\theta : \mathfrak{m}_x/\mathfrak{m}_x^2 \to \overline{\mathbb{Q}}_p^n$$

by

$$\theta(f) = \left(\frac{\partial f}{\partial U_1}(X), \ldots, \frac{\partial f}{\partial U_n}(X) \right).$$

This is an isomorphism between $\mathfrak{m}_x/\mathfrak{m}_x^2$ and $\overline{\mathbb{Q}}_p^n$. Since C is smooth with good reduction,

$$\dim(\theta(J_0) + \mathfrak{p}^n) = n - 1, \tag{9}$$

where $\mathfrak{p}^n$ as before is the n-fold Cartesian product of $\mathfrak{p}$. Here $\theta(f) + \mathfrak{p}^n \in \overline{\mathbb{F}}_p^n$ for $f \in J_0$. Let

$$w_1, \ldots, w_{n-1} \in \theta(J_0)$$

and $w_n = \theta(z) \in O_p^n$ be elements such that $w_1 + \mathfrak{p}, \ldots, w_n + \mathfrak{p}$ are linearly independent over $\overline{\mathbb{F}}_p$. Then $w_1, \ldots, w_n \in O_p^n$ are linearly independent, and the determinant of the matrix formed by those vectors is a unit in O_p. Write $v \in \theta(J_0)$ as a linear combination $v = \sum_{i=1}^{n} a_i w_i$ with $a_i \in O_p$. Since $w_1, \ldots, w_{n-1}, v \in \theta(J_0)$ we must have $a_n = 0$, for otherwise

$\theta(I_0) = \overline{\mathbb{Q}}_p\theta(J_0)$ would be n-dimensional, contradicting the fact that C is a curve for which the rank condition (3) holds. This shows that $w_1, \dots, w_{n-1}$ is a basis for $\theta(J_0)$ over O_p. Therefore $\theta(z) \notin \theta(I_0)$, and z is a uniformizer at $x \in C$.

Now define the ideal

$$\mathfrak{q} = \{f \in \mathcal{O}_{\pi(x)} : f(x) = 0\} \subseteq \mathcal{O}_{\pi(x)}.$$

For any $f \in \mathfrak{q}$, there exists $a \in O_p$ such that $\theta(f) - a\theta(z) \in \theta(J_0)$. Since $f - az = \frac{h}{g}$ is a rational function which is regular at $\pi(x)$ we see that $h(x) = 0$ and so $\theta(h) = 0$ by the product formula for derivatives. It follows that $h \in \mathfrak{q}^2$, so

$$f - az \in \mathfrak{q}^2$$

and therefore

$$\mathfrak{q} = \mathcal{O}_{\pi(x)}z + \mathfrak{q}^2.$$

Using Nakayama's Lemma [11, Th. 2.2] this shows that

$$\mathfrak{q} = \mathcal{O}_{\pi(x)}z, \tag{10}$$

which is the first statement of the proposition.

For any $f \in \mathcal{O}_{\pi(x)}$ we can now find $a_0 \in O_p$ such that $f - a_0 \in \mathfrak{q}$. By (10) there exists $f_1 \in \mathcal{O}_{\pi(x)}$ with $f - a_0 = f_1 z$. For f_1 we can find $a_1 \in O_p$ and $f_2 \in \mathcal{O}_{\pi(x)}$ with $f_1 - a_1 = f_2 z$, and therefore

$$f - (a_0 + a_1 z) = f_2 z^2.$$

Continuing like this gives sequences $a_i \in O_p$ and $f_i \in \mathcal{O}_{\pi(x)}$ such that

$$f - \sum_{i=0}^{n} a_i z^i = f_{n+1} z^{n+1}. \tag{11}$$

Let $y \in C$ with $\Delta(x, y) < 1$, then $\pi(x) = \pi(y)$ and $|z(y)| = q < 1$. Equation (11) shows that

$$\left| f(y) - \sum_{i=0}^{n} a_i z(y)^i \right| \leq q^{-(n+1)},$$

which concludes the proof.

PROPOSITION 9. *Fix a point $x \in C$. There exists a uniformizer z of C at x such that z is regular at $\pi(x)$ and $\overline{z}$ is a uniformizer at $\pi(x)$. The restriction $z : U \to \mathfrak{p}$ of z to $U = \{y \in C \mid \Delta(y, x) < 1\}$ is a bijection and its inverse is, in each affine coordinate, a convergent power series with coefficients in O_p. Hence $\Delta(y, y') = |z(y) - z(y')|$ for all $y, y' \in U$.*

Proof. Choose z as in Proposition 8. Assume $X_0 = 1$ and work in the corresponding affine piece. The function $z \in \mathcal{O}_{\pi(x)}$ which vanishes at x maps U into $\mathfrak{p}$ and all the affine coordinate projections $U_i : C \to \overline{\mathbb{Q}}_p \cup \{\infty\}$ are elements of $\mathcal{O}_{\pi(x)}$. Applying Proposition 8 concludes the proof.

Finally, some information about the morphism is needed.

PROPOSITION 10. *Let C be an irreducible projective smooth curve with good reduction. Let $\phi : C \to \mathbb{P}^m(\overline{\mathbb{Q}}_p)$ be a morphism of good reduction and $x \in C$. Then ϕ induces a map*

$$\phi^* : \mathcal{O}_{\pi(\phi(x))} \to \mathcal{O}_{\pi(x)}$$
$$\phi^*(f) = f \circ \phi$$

Proof. By the definition of good reduction for maps, there are forms $F_0, \ldots, F_m$ such that ϕ is represented by $(F_0, \ldots, F_m)$ and for a homogeneous coordinate X for x

$$|X| = 1 = |F_0(X), \ldots, F_m(X)|.$$

Let $\frac{F}{G} \in \mathcal{O}_{\pi(\phi(x))}$ be chosen so that the homogeneous coordinate $Y = (F_0(X), \ldots, F_m(X))$ of the point $y = \phi(x)$ satisfies $|G(Y)| = 1$. Then

$$\phi^* z = \frac{F(F_0, \ldots, F_m)}{G(F_0, \ldots, F_m)} = \frac{F^*}{G^*}$$

with $|G^*(X)| = 1$, which means that $\phi^*\left(\frac{F}{G}\right) \in \mathcal{O}_{\pi(x)}$.

Proposition 8 and Proposition 10 together yield the next corollary.

COROLLARY 11. *Let $\phi : C \to C$ be a morphism of good reduction, and let $x \in C$ be a fixed point. Then there exists a uniformizer z, also satisfying Proposition 9, such that*

$$\phi^* z = z \circ \phi = \sum_{i=1}^{\infty} a_i z^i \text{ with } a_i \in O_p.$$

This completes the proof of the tools required for Theorem 1.

References

1. A. Beardon, *Iteration of Rational Functions*, Springer, New York, 1991.
2. R. Benedetto, *Reduction, dynamics, and Julia sets of rational functions*, J. Number Theory, **86** (2001), 175–195.

3. J. Call and J.H. Silverman, *Canonical heights on varieties with morphisms*, Compositio Math. **94** (1993), 163–205.
4. M. Einsiedler, G. Everest and T. Ward, *Morphic heights and periodic points*, New York Number Theory Seminar, to appear (2002). `arXiv:math.NT/0204179`
5. R. Hartshorne, *A*lgebraic Geometry, Springer-Verlag, New York, 1977.
6. N. Koblitz, *p*-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer-Verlag, New York, 1977.
7. Hua–Chieh Li, *C*ounting periodic points of *p*-adic power series, Compositio Math. **100** (1996), 351–364.
8. Hua–Chieh Li, *p*-adic dynamical systems and formal groups, Compositio Math. **104** (1996), 41–54.
9. Hua–Chieh Li, *p*-typical dynamical systems and formal groups, Compositio Math. **130** (2002), 75–88.
10. J. Lubin, *N*onarchimedean dynamical systems, Compositio Math. **94** (1993), 321–346.
11. H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986.
12. P. Morton and J.H. Silverman, *P*eriodic points, multiplicities, and dynamical units, J. Reine Angew. Math. **461** (1995), 81–122.
13. Y. Puri and T. Ward, *Arithmetic and growth of periodic orbits*, J. Integer Sequences **4**:01.2.1 (2001).
14. Juan Rivera Letelier, *Dynamique des Fonctions Rationelles sur des Corps Locaux*, PhD. thesis, Univ. Paris Sud, Orsay (2000).