PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 1, January 2014, Pages 85–92
S 0002-9939(2013)11740-5
Article electronically published on September 26, 2013

EXPANSIONS OF QUADRATIC MAPS IN PRIME FIELDS

MEI-CHU CHANG

(Communicated by Bryna Kra)

ABSTRACT. Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ be a quadratic polynomial with $a \not\equiv 0 \bmod p$. Take $z \in \mathbb{F}_p$ and let $\mathcal{O}_z = \{f_i(z)\}_{i\in\mathbb{Z}^+}$ be the orbit of z under f, where $f_i(z) = f(f_{i-1}(z))$ and $f_0(z) = z$. For $M < |\mathcal{O}_z|$, we study the diameter of the partial orbit $\mathcal{O}_M = \{z, f(z), f_2(z), \ldots, f_{M-1}(z)\}$ and prove that there exists $c_1 > 0$ such that

$$\operatorname{diam} \mathcal{O}_M \gtrsim \min\left\{Mp^{\,c_1}, \frac{1}{\log p} M^{\frac{4}{5}} p^{\frac{1}{5}}, M^{\,\frac{1}{13}\log\log M}\right\}.$$

For a complete orbit $\mathcal{C}$, we prove that

$$\operatorname{diam} \mathcal{C} \gtrsim \min\{p^{\,5c_1}, e^{\,T/4}\},$$

where T is the period of the orbit.

INTRODUCTION

This paper belongs to the general theme of dynamical systems over finite fields. Let p be a prime and $\mathbb{F}_p$ the finite field of p elements, represented by the set $\{0, 1, \ldots, p-1\}$. Let $f \in \mathbb{F}_p[x]$ be a polynomial, which we view as a transformation of $\mathbb{F}_p$. Thus if $z \in \mathbb{F}_p$ is some element, we consider its orbit

$$z_0 = z,\ z_{n+1} = f(z_n), \quad n = 0, 1, \ldots, \tag{0.1}$$

which eventually becomes periodic. The *period* $T_z = T$ is the smallest integer satisfying

$$\{z_n : n = 0, 1, \ldots, T-1\} = \{z_n : n \in \mathbb{N}\}. \tag{0.2}$$

We are interested in the metrical properties of orbits and partial orbits. More precisely, for $M < T_z$, we define

$$\operatorname{diam} \mathcal{O}_M = \max_{0\le n<M} |z_n - z|. \tag{0.3}$$

Following the papers [GS] and [CGOS], we study the expansion properties of f, in the sense of establishing lower bounds on diam $\mathcal{O}_M$. Obviously, if $M \le T$, then diam $\mathcal{O}_M \ge M$. But, assuming that f is nonlinear and $M = o(p)$, one reasonably expects that the diameter of the partial orbit is much larger. Results along these lines were obtained in [GS] under the additional assumption that $M > p^{\frac{1}{2}+\epsilon}$. In this situation, Weil's theorem on exponential sums permits proving equidistribution of the partial orbit. For $M \le p^{1/2}$, Weil's theorem becomes inapplicable and

Received by the editors October 10, 2011 and, in revised form, March 2, 2012.
2010 *Mathematics Subject Classification.* Primary 11B50, 37A45, 11B75; Secondary 11T23, 37F10, 11G99.
Key words and phrases. Dynamical system, orbits, additive combinatorics, exponential sums.
The author's research was partially financed by the National Science Foundation.

lower bounds on diam $\mathcal{O}_M$ based on Vinogradov's theorem were established in [CGOS]. Our paper is a contribution of this line of research. We restrict ourselves to quadratic polynomials, though certainly the methods can be generalized. (See [CCGHSZ] for a generalization of Proposition 2 and Theorem 2 to higher degree polynomials and rational maps.)

Our first result is the following.

Theorem 1. *There is a constant $c_1 > 0$ such that if $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ with $(a, p) = 1$, then with the above notation, for any $z \in \mathbb{F}_p$ and $M \leq T_z$,*

$$\text{diam } \mathcal{O}_M \gtrsim^{1} \min\left\{Mp^{\,c_1}, \frac{1}{\log p} M^{\frac{4}{5}} p^{\frac{1}{5}}, M^{\,\frac{1}{13}\log\log M}\right\}. \tag{0.4}$$

In view of Theorem 2, one could at least expect that diam $\mathcal{O}_M \gtrsim \min(p^{\,c}, e^{cM})$ as is the case when $M = T_z$.

In the proof, we distinguish the cases diam $\mathcal{O}_M > p^{\,c_0}$ and diam $\mathcal{O}_M \leq p^{\,c_0}$, where $c_0 > 0$ is a suitable constant. First, we again exploit exponential sum techniques (though, from the analytical side, our approach differs from [CGOS] and exploits a specific multilinear setup of the problem). More precisely, Proposition 1 in §1 states that (for $M \leq T$ large enough)

$$\text{diam } \mathcal{O}_M \gtrsim \frac{1}{\log p} \min\left(M^{\frac{5}{4}}, M^{\frac{4}{5}} p^{\frac{1}{5}}\right). \tag{0.5}$$

(Note that (0.5) is a clear improvement over Theorem 8 from [CGOS] for the case $d = 2$.)

When diam $\mathcal{O}_M \leq p^{\,c_0}$, a different approach becomes available as explained in Proposition 2. In this situation, we are able to replace the (mod p) iteration by a similar problem in the field $\mathbb{C}$ of complex numbers, for an appropriate quadratic polynomial $F(z) \in \mathbb{Q}[z]$. Elementary arithmetic permits us to then prove that $\log \text{diam } \mathcal{O}_M$ is at least as large as $\frac{1}{13} \log M \log\log M$.

Interestingly, assuming $\mathcal{C}$ is a complete periodic cycle and diam $\mathcal{C} < p^{\,c_0}$, the transfer argument from Proposition 2 enables us to invoke bounds on the number of rational preperiodic points of a quadratic map, for instance the results from R. Benedetto [B]. The conclusion is the following.

Theorem 2. *There is a constant $c_0 > 0$ such that if $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ with $(a, p) = 1$ and $\mathcal{C} \subset \mathbb{F}_p$ is a periodic cycle for f of length T, then*

$$\text{diam } \mathcal{C} \gtrsim \min\{p^{\,c_0}, e^{\,T/4}\}. \tag{0.6}$$

1. Diameter of partial orbits

Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$, where $a \not\equiv 0 \pmod p$. Fix $x_0 \in \mathbb{F}_p$ and denote the *orbit* of x_0 by

$$\mathcal{O}_{x_0} = \{f_j(x_0)\}_{j \in \mathbb{Z}^+},$$

where $f_j(x_0) = f(f_{j-1}(x_0))$ and $f_0(x_0) = x_0$. The *period* of the orbit of x_0 under f is denoted $T = T_{x_0} = |\mathcal{O}_{x_0}|$. For $A \subset \mathbb{F}_p$, we denote the *diameter* of A by

$$\text{diam } A = \max_{x,y \in A} p \left\| \frac{x-y}{p} \right\|,$$

[1] $h \lesssim g$ if there exist constants C, M such that $|h(x)| \leq Cg(x)$ for all $x > M$.

where $\|a\|$ is the distance from a to the nearest integer. We are interested in the expansion of part of an orbit.

Proposition 1. *For $1 \ll M < T$, consider a partial orbit*

$$\mathcal{O}_M = \{x_0, f(x_0), f_2(x_0), \dots, f_{M-1}(x_0)\}.$$

Then

$$\operatorname{diam} \mathcal{O}_M \gtrsim \frac{1}{\sqrt{\log p}} \min(M^{5/4}, M^{4/5}p^{1/5}). \tag{1.1}$$

Proof. Let $M_1 = \operatorname{diam} \mathcal{O}_M$. Take $I \subset \mathbb{F}_p$ with $|I| = M_1$ and $\mathcal{O}_M \subset I$; then

$$|f(I) \cap I| \geq M - 1. \tag{1.2}$$

We will express (1.2) using exponential sums.

Let $0 \leq \varphi \leq 1$ be a smooth function on $\mathbb{F}_p$ such that $\varphi = 1$ on I and $\operatorname{supp} \varphi \subset \widetilde{I}$, where $\widetilde{I}$ is an interval with the same center and double the length of I. Equation (1.2) implies that

$$\sum_{x \in I} \varphi(f(x)) \geq M$$

and expanding φ in Fourier gives

$$\varphi(x) = \sum_{\xi \in \mathbb{F}_p} \widehat{\varphi}(\xi) e_p(x\xi), \quad \text{with} \quad \widehat{\varphi}(\xi) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} \varphi(x) e_p(-x\xi).$$

Combining these gives

$$\sum_{\xi \in \mathbb{F}_p} |\widehat{\varphi}(\xi)| \Big| \sum_{x \in I} e_p(\xi f(x)) \Big| \gtrsim M. \tag{1.3}$$

We will estimate $\sum_{x \in I} e_p(\xi f(x))$ using van der Corput-Weyl.

Take $M_0 = O(M)$, e.g. $M_0 = \frac{1}{100} M$. Then

(1.4)

$$\begin{aligned}
\Big| \sum_{x \in I} e_p(\xi f(x)) \Big| &\leq \frac{1}{M_0} \sum_{0 \leq y < M_0} \Big| \sum_{x \in I} e_p\Big(\xi\big(a(x+y)^2 + b(x+y)\big)\Big) \Big| + O(M_0) \\
&\leq \frac{1}{\sqrt{M_0}} \Big[\sum_{0 \leq y < M_0} \Big| \sum_{x \in I} e_p\big(\xi(ax^2 + 2axy + bx)\big) \Big|^2 \Big]^{1/2} + O(M_0) \\
&= \frac{1}{\sqrt{M_0}} \Big| \sum_{\substack{0 \leq y < M_0 \\ x_1, x_2 \in I}} e_p\Big(\xi(x_1 - x_2)(a(x_1 + x_2) + 2ay + b)\Big) \Big|^{1/2} + O(M_0).
\end{aligned}$$

(The second inequality is by Cauchy-Schwarz.)

Take φ sufficiently smooth so as to ensure that

$$\sum_{\xi \in \mathbb{F}_p} |\widehat{\varphi}(\xi)| = O(1). \tag{1.5}$$

Equations (1.3) and (1.4) imply

$$\sum_{\xi \in \mathbb{F}_p} |\widehat{\varphi}(\xi)| \Big| \sum_{\substack{0 \leq y < M_0 \\ x_1, x_2 \in I}} e_p\left(\xi(x_1 - x_2)(a(x_1 + x_2) + 2ay + b)\right) \Big|^{1/2} \gtrsim M^{3/2}.$$

Hence by Cauchy-Schwarz and (1.5),

$$\sum_{\xi\in\mathbb{F}_p}|\widehat{\varphi}(\xi)|\Bigg|\sum_{\substack{0\le y<M_0\\ x_1,x_2\in I}} e_p\left(\xi(x_1-x_2)(a(x_1+x_2)+2ay+b)\right)\Bigg|\gtrsim M^3. \tag{1.6}$$

Fix $x_1+x_2=s\le 2M_1$; then

$$\sum_{\xi\in\mathbb{F}_p}|\widehat{\varphi}(\xi)|\Bigg|\sum_{\substack{0\le y<M_0\\ x\in I}} e_p\left(\xi(2x-s)(as+2ay+b)\right)\Bigg|\gtrsim \frac{M^3}{2M_1}. \tag{1.7}$$

Next, for $z\in\mathbb{F}_p$, denote

$$\eta(z)=\left|\{(x,y)\in I\times[1,M_0]:(2x-s)(2ay+b+as)\equiv z \pmod p\}\right|, \tag{1.8}$$

and write the left hand side of (1.7) as

$$\begin{aligned}
&\sum_{\xi\in\mathbb{F}_p}|\widehat{\varphi}(\xi)|\left|\sum_{z\in\mathbb{F}_p}\eta(z)\ e_p(\xi z)\right|\\
&\le\ \Big(\sum_{\xi\in\mathbb{F}_p}|\widehat{\varphi}(\xi)|^2\Big)^{1/2}\Big(\sum_{\xi\in\mathbb{F}_p}\Big|\sum_{z\in\mathbb{F}_p}\eta(z)e_p(\xi z)\Big|^2\Big)^{1/2}\\
&=\ \Big(\frac{1}{p}\sum_{x\in\mathbb{F}_p}|\varphi(x)|^2\Big)^{1/2}\sqrt{p}\ \Big(\sum_{z\in\mathbb{F}_p}\eta(z)^2\Big)^{1/2}\\
&<2M_1^{1/2}\Big(\sum_{z\in\mathbb{F}_p}\eta(z)^2\Big)^{1/2},
\end{aligned} \tag{1.9}$$

by Cauchy-Schwarz and Parseval.

Recall that $(a,p)=1$. Let $I'=I-\frac{s}{2},\ I''=[1,M_0]+\frac{b+as}{2a}\subset\mathbb{F}_p$ so that

$$\sum_{z\in\mathbb{F}_p}\eta(z)^2=E(I',I''),$$

the multiplicative energy of I' and I''.

It is well-known that

$$\begin{aligned}
E(I',I'')&\le\log p\ \max\left\{|I'||I''|,\frac{|I'|^2|I''|^2}{p}\right\}\\
&\le\log p\ \max\left\{M_1M,\frac{M_1^2M^2}{p}\right\}.
\end{aligned} \tag{1.10}$$

Thus, by (1.7), (1.9) and (1.10),

$$\frac{M^3}{M_1}\lesssim M_1^{1/2}(\log p)^{1/2}\max\left\{M_1^{1/2}M^{1/2},\frac{M_1M}{p^{1/2}}\right\}. \tag{1.11}$$

Distinguish the cases $M_1M\le p$ and $M_1M>p$, and then (1.11) implies

$$M_1\gtrsim\min\left\{\big(\log p\big)^{-1/4}M^{5/4},\big(\log p\big)^{-1/5}M^{4/5}p^{1/5}\right\}. \tag{1.12}$$

□

2. Partial orbits of small diameters

For $M < p^{c_0}$, one obtains the following stronger result. (Notation is as in Proposition 1.)

Proposition 2. *There exists $c_0 > 0$ such that*

$$\operatorname{diam} \mathcal{O}_M > \min\left(p^{c_0}, M^{\frac{1}{13}\log\log M}\right). \tag{2.1}$$

Consequently,

$$\operatorname{diam} \mathcal{O}_M \gtrsim \min\left\{Mp^{\frac{c_0}{5}}, \frac{1}{\log p} M^{\frac{4}{5}} p^{\frac{1}{5}}, M^{\frac{1}{13}\log\log M}\right\}. \tag{2.2}$$

Proof. Let $\mathcal{O}_M = \{x_0, x_1, \dots, x_{M-1}\}$ with $x_j = f(x_{j-1})$ as before, and let diam $\mathcal{O}_M = M_1$. Since $|x_j - x_0| \le M_1$, we can write $x_j = x_0 + z_j$ with $z_j \in [-M_1, M_1]$. Thus, a, b, c, x_0 satisfy the $M-1$ equations

$$a(x_0 + z_j)^2 + b(x_0 + z_j) + c \equiv x_0 + z_{j+1} \pmod p, \qquad j = 0, \dots, M-2,$$

and the $\mathbb{F}_p$-variety

$$\mathcal{V}_p = \bigcap_{j=0}^{M-2} \left[(r + z_j)^2 + v(r + z_j) + w = u(r + z_{j+1}) \pmod p\right.$$

in the variables $(u, v, w, r) \in \mathbb{F}_p^4$ is therefore nonempty. Note that the coefficients of the $M-1$ defining polynomials in $\mathbb{Z}[u, v, w, r]$ are $O(M_1^2)$.

Assume

$$M_1 < p^{c_0} \tag{2.3}$$

with $c_0 > 0$ small enough. Elimination theory[2] implies that $\mathcal{V}_p \neq \emptyset$ is a $\mathbb{C}$-variety. Hence there are $U, V, W, R \in \mathbb{C}$ such that for all j,

$$(R + z_j)^2 + V(R + z_j) + W = U(R + z_{j+1}), \quad j = 0, \dots, M-2.$$

Obviously, $U \neq 0$, since $z_1, \dots, z_{M-2}$ are distinct. We therefore have a quadratic polynomial

$$F(z) := \frac{1}{U}(R + z)^2 + \frac{V}{U}(R + z) + \frac{W}{U} - R =: Az^2 + Bz + C, \tag{2.4}$$

satisfying

$$F(z_j) = z_{j+1} \quad \text{in } \mathbb{C}, \quad \text{for } j = 0, \dots, M-2. \tag{2.5}$$

Since $z_0 = 0$, (2.4) and (2.5) imply $C = z_1 \in \mathbb{Z} \cap [-M_1, M_1]$, and the equations

$$z_1^2 A + z_1 B = z_2 - z_1,$$
$$z_2^2 A + z_2 B = z_3 - z_1$$

imply $A, B \in \mathbb{Q}$ with $A = \frac{a}{d}$, $B = \frac{b}{d}$, and $a, b, d \in \mathbb{Z}$ being $O(M_1^3)$. Equation (2.5) becomes

$$z_{j+1} = \frac{a}{d} z_j^2 + \frac{b}{d} z_j + C. \tag{2.6}$$

[2]See [C], where a similar elimination procedure was used in a combinatorial problem. In particular, see [C], Lemma 2.14 and its proof.

Hence

$$\frac{a}{d}z_{j+1}+\frac{b}{2d}=\left(\frac{a}{d}z_j+\frac{b}{2d}\right)^2+C\frac{a}{d}-\frac{b^2}{4d^2}+\frac{b}{2d}.$$

Putting

$$y_j=\frac{a}{d}z_j+\frac{b}{2d}\in\frac{1}{2d}\mathbb{Z},\quad j=0,\dots,M-1,$$

and

$$\frac{r}{s}=C\frac{a}{d}-\frac{b^2}{4d^2}+\frac{b}{2d}\quad\text{with } s>0,(r,s)=1,\ |r|,s=O(M_1^6),$$

gives

$$y_{j+1}=y_j^2+\frac{r}{s},\quad j=0,\dots,M-2. \tag{2.7}$$

Next, write $y_j=\alpha_j/\beta_j$, where $\beta_j|2d$ and $(\alpha_j,\beta_j)=1$; thus (2.7) gives

$$\frac{\alpha_{j+1}}{\beta_{j+1}}=\frac{\alpha_j^2}{\beta_j^2}+\frac{r}{s},\quad j=0,\dots,M-2. \tag{2.8}$$

Note also that

$$|\alpha_j|=O(M_1^4). \tag{2.9}$$

Write the prime factorizations

$$s=\prod_p p^{v(p)}\quad\text{and}\quad\beta_j=\prod_p p^{v_j(p)},\quad j=0,\dots,M-1.$$

Claim. $2v_j(p)\le v(p)$, for $j<M-O(\log\log M_1)$.

Proof. We may assume $v_j(p)>0$.

Case 1. $2v_j(p)>v_{j+1}(p)$.

Fact 2.1 (which will be stated at the end of this section) and (2.8) imply that $v(p)=2v_j(p)$.

Case 2. $2v_j(p)\le v_{j+1}(p)$.

Again, we separate two cases.

Case 2.1. $2v_{j+1}(p)>v_{j+2}(p)$. Reasoning as in Case 1, we have

$$v(p)=2v_{j+1}(p)\ge 2^2v_j(p)>2v_j(p).$$

Case 2.2. $2v_{j+1}(p)\le v_{j+2}(p)$. Therefore, $v_{j+2}(p)\ge 2^2v_j(p)$. We repeat the argument for Case 2 with $j=j+1$. Continuing this process, after τ steps, we obtain either $v(p)\ge 2v_j(p)$ or

$$v_{j+\tau}(p)\ge 2^\tau v_j(p), \tag{2.10}$$

when necessarily $\tau\lesssim\log v_{j+\tau}(p)\lesssim\log\log\beta_{j+\tau}\lesssim\log\log d\lesssim\log\log M_1$. Since $j+\tau\le M$, the claim is proved. □

It follows from the claim that $\beta_j^2|s$ for $j<M-O(\log\log M_1)$. Back to (2.8), if $v(p)>2v_j(p)$ for some $j<M-O(\log\log M_1)$, then $v_{j+1}(p)=v(p)$. This contradicts the fact that $\beta_{j+1}^2|s$. So we conclude that

$$\beta_j^2=s=:s_1^2\quad\text{for } j<M-O(\log\log M_1). \tag{2.11}$$

Hence

$$\alpha_{j+1} = \frac{\alpha_j^2}{s_1} + \frac{r}{s_1}, \tag{2.12}$$

which implies

$$\alpha_j^2 + r \equiv 0 \mod s_1. \tag{2.13}$$

Let $s_1 = \prod p_i^{v_i}$. Then α_j satisfies (2.13) if and only if α_j satisfies $\alpha_j^2 + r \equiv 0 \mod p_i^{v_i}$ for all i. Since $-r$ is a quadratic residue modulo p^v if and only if it is a quadratic residue modulo p for odd prime p, we have

$$\left|\{\pi_{s_1}(\alpha_j)\}_j\right| \le 2 \cdot 2^{\omega(s_1)} < e^{\frac{\log s_1}{\log\log s_1}} < e^{\frac{4\log M_1}{\log\log M_1}}. \tag{2.14}$$

Here $\pi_{s_1}(\alpha_j)$ is the projection of α_j in $\mathbb{Z}_{s_1}$.

To show $M_1 > M^{\frac{1}{13}\log\log M}$, we assume

$$\log M_1 < \frac{1}{13}\log M \log\log M. \tag{2.15}$$

Then (2.14) implies there exists $\xi \in \mathbb{Z}_{s_1}$ such that

$$|\mathcal{J}| = \left|\left\{0 \le j \le \frac{M}{2} : \pi_{s_1}(\alpha_j) = \xi\right\}\right| > M^{1/2}. \tag{2.16}$$

Thus

$$\alpha_{j_1} - \alpha_{j_2} \in s_1\mathbb{Z}, \quad \text{for } \ j_1, j_2 \in \mathcal{J},$$

and

$$|\alpha_{j_1} - \alpha_{j_2}| \ge s_1, \quad \text{for } \ j_1 \ne j_2 \in \mathcal{J}.$$

In particular, there exists $j \in \mathcal{J}$ such that

$$|\alpha_j| \ge \frac{M^{1/2}}{8}s_1 \quad \text{and} \quad \left||\alpha_j| - |r|^{1/2}\right| > \frac{M^{1/2}}{8}s_1. \tag{2.17}$$

Claim. Either $|\alpha_j| > 10|r|^{1/2}$ or $|\alpha_{j+1}| > 10|r|^{1/2}$.

Proof. Assume

$$|\alpha_j|, |\alpha_{j+1}| < 10|r|^{1/2}. \tag{2.18}$$

Hence, $|r|^{1/2} \gtrsim M^{1/2}s_1$ by (2.17). From (2.12), (2.17) and (2.18),

$$\begin{aligned} 10|r|^{1/2}s_1 > |\alpha_{j+1}|s_1 &= |\alpha_j^2 + r| \\ &\ge (|\alpha_j| + |r|^{1/2})(|\alpha_j| - |r|^{1/2}) \\ &\ge |r|^{1/2} \cdot \frac{M^{1/2}}{8}s_1, \end{aligned}$$

a contradiction, proving the claim. □

Thus, there exists $j < M/2$ such that either

$$|\alpha_j| > 10s_1 \quad \text{and} \quad |\alpha_j| > 10|r|^{1/2} \tag{2.19}$$

or

$$|\alpha_j| > 10s_1 \quad \text{and} \quad |\alpha_{j+1}| > 10|r|^2. \tag{2.20}$$

Clearly, (2.19) implies (2.20). Indeed, by (2.12),

$$|\alpha_{j+1}| \ge \frac{1}{s_1}\left|\alpha_j^2 - |r|\ \right| \ge \frac{99}{100s_1}\alpha_j^2 > 2|\alpha_j|.$$

Iteration shows that

$$\left|\alpha_{j+\frac{M}{3}}\right| > 2^{\frac{M}{3}}|\alpha_j| > 2^{\frac{M}{3}},$$

contradicting (2.9). This proves (2.1).

Combining Proposition 1 and (2.1), we have (2.2). □

Fact 2.1. Let $\frac{a_1}{d_1}, \frac{a_2}{d_2}, \frac{a_3}{d_3} \in \mathbb{Q}$ be rational numbers in lowest terms, and $p^{\,v_p(d_i)}||d_i$. If $\frac{a_1}{d_1} + \frac{a_2}{d_2} + \frac{a_3}{d_3} = 0$ and $v_p(d_1) \geq v_p(d_2) \geq v_p(d_3)$, then $v_p(d_1) = v_p(d_2)$.

3. Full cycles

In this section, we will prove Theorem 2.

Assume $M_1 = \operatorname{diam} \mathcal{C} < p^{\,c_0}$ with c_0 as in Proposition 2. The proof of Proposition 2 gives a quadratic polynomial (cf. (2.7))

$$F(z) = z^2 + \frac{r}{s} \quad \text{with } r, s \in \mathbb{Z}, |s| = O(M_1^6) \tag{3.1}$$

and a rational F-cycle $\{y_j\}_{0 \leq j < T}$, i.e.

$$y_{j+1} = F(y_j) \quad \text{for } 0 \leq j \leq T-2$$

and $F(y_{T-1}) = y_0$.

We now invoke a result of R. Benedetto [B], which gives quantitative bounds on the number of preperiodic points of a polynomial f in a number field $\big($$z$ is *preperiodic* if the set $\big\{z, f(z), f\big(f(z)\big), \dots\big\}$ is finite$\big)$. According to Theorem 7.1 in [B], the number of preperiodic points of F in $\mathbb{Q}$ is bounded by

$$(2\sigma+1)\left[\log_2(2\sigma+1) + \log_2(\log_2(2\sigma+1)-1) + 2\right] \tag{3.2}$$

with σ the number of primes where F has bad reduction. Hence $\sigma \leq \omega(s) \leq \frac{\log M_1}{\log\log M_1}$ and (3.2) implies

$$T < 4\log M_1 = 4\log \operatorname{diam} \mathcal{C}. \tag{3.3}$$

Acknowledgements

The author would like to thank the referee for many helpful comments and the mathematics department of the University of California at Berkeley for its hospitality.

References

[B] Robert L. Benedetto, *Preperiodic points of polynomials over global fields*, J. Reine Angew. Math. **608** (2007), 123–153, DOI 10.1515/CRELLE.2007.055. MR2339471 (2008j:11071)

[CCGHSZ] M.-C. Chang, J. Cilleruelo, M. Garaev, J. Hernandez, I. Shparlinski, A. Zumalacarregui, *Points on curves in small boxes and applications* (preprint).

[C] M. Chang, *Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems*, Geom. Funct. Anal. **13** (2003), no. 4, 720–736, DOI 10.1007/s00039-003-0428-5. MR2006555 (2004g:11007)

[CGOS] Javier Cilleruelo, Moubariz Z. Garaev, Alina Ostafe, and Igor E. Shparlinski, *On the concentration of points of polynomial maps and applications*, Math. Z. **272** (2012), no. 3-4, 825–837, DOI 10.1007/s00209-011-0959-7. MR2995141

[GS] Jaime Gutierrez and Igor E. Shparlinski, *Expansion of orbits of some dynamical systems over finite fields*, Bull. Aust. Math. Soc. **82** (2010), no. 2, 232–239, DOI 10.1017/S0004972709001270. MR2685147 (2011j:11153)

Department of Mathematics, University of California, Riverside, California 92521
E-mail address: mcc@math.ucr.edu