C. R. Acad. Sci. Paris, Ser. I 353 (2015) 283–285

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory/Dynamical systems

On periods modulo p in arithmetic dynamics

Sur les périodes modulo p des systèmes dynamiques arithmétiques

Mei-Chu Chang [1]

Department of Mathematics, University of California, Riverside, CA 92521, USA

A R T I C L E   I N F O

Article history:
Received 18 August 2014
Accepted after revision 20 January 2015
Available online 2 February 2015

Presented by the Editorial Board

A B S T R A C T

We prove the following analogue of Silverman's results [9] for pairs of maps.
Let $d \ge 2$ be an integer, $K/\mathbb{Q}$ a number field, and $N = N_{K/\mathbb{Q}}(\mathcal{P})$ the norm of an ideal $\mathcal{P} \subset \mathcal{O}_K$. Let $h(z) \in K[z]$ be non-constant and not of the form $h(z) = \xi z$, $\xi^{d-1} = 1$. Denote $f_t(z) = z^d + t$, $g_t(z) = z^d + h(t)$, and $F^{(\ell)}$ the ℓ-th iteration of F. There are constants c_1, c_2 depending on d and h such that the following holds.
For almost all prime ideals $\mathcal{P} \subset \mathcal{O}_K$, there is a finite subset $T \subset \bar{\mathbb{F}}_{\mathcal{P}}$, $|T| \le c_1$ such that if $t \in \bar{\mathbb{F}}_{\mathcal{P}} \setminus T$ at least one of the sets

$$\left\{f_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\right\}, \qquad \left\{g_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\right\} \tag{1}$$

consists of distinct elements.

R É S U M É

Nous prouvons l'analogue suivant des résultats de Silverman [9] pour les paires d'applications.
Soit $d \ge 2$ un entier, $K/\mathbb{Q}$ un corps de nombres, et $N = N_{K/\mathbb{Q}}(\mathcal{P})$ la norme d'un idéal $\mathcal{P} \subset \mathcal{O}_K$. Soit $h(z) \in K[z]$ un polynôme non constant qui n'est pas de la forme $h(z) = \xi z$, $\xi^{d-1} = 1$. Posons $f_t(z) = z^d + t$, $g_t(z) = z^d + h(t)$ et $F^{(\ell)}$ les itérés de F. Il existe des constantes c_1, c_2, dépendant de d et h, possédant la propriété suivante : pour presque tout idéal premier $\mathcal{P} \subset \mathcal{O}_K$, il y a un sous-ensemble $T \subset \bar{\mathbb{F}}_{\mathcal{P}}$, $|T| \le c_1$ tel que si $t \in \bar{\mathbb{F}}_{\mathcal{P}} \setminus T$, au moins un des ensembles

$$\left\{f_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\right\}, \qquad \left\{g_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\right\}$$

se compose d'éléments distincts.

E-mail address: mcc@math.ucr.edu.

[1] Research partially financed by the National Science Foundation.

http://dx.doi.org/10.1016/j.crma.2015.01.007

Version française abrégée

Soit $d \geq 2$ un entier, $K/\mathbb{Q}$ un corps de nombres, et $N = N_{K/\mathbb{Q}}(\mathcal{P})$ la norme d'un idéal $\mathcal{P} \subset \mathcal{O}_K$. Soit $h(z) \in K[z]$ un polynôme non constant qui n'est pas de la forme $h(z) = \xi z$, $\xi^{d-1} = 1$. Soit $\mathcal{P} \subset \mathcal{O}_K$ un idéal premier de bonne réduction et considérons $h(z) \in \mathbb{F}_{\mathcal{P}}[z]$. Posons $f_t(z) = z^d + t$, $g_t(z) = z^d + h(t)$ et $F^{(\ell)}$ les itérés de F.

Théorème 1. *Il existe des constantes c_1, c_2 dépendant de d et h avec la propriété suivante. Pour presque tout idéal premier $\mathcal{P}$, il y a un sous-ensemble $T \subset \bar{\mathbb{F}}_{\mathcal{P}}$, $|T| \leq c_1$ tel que, si $t \in \bar{\mathbb{F}}_{\mathcal{P}} \setminus T$, au moins un des ensembles*

$$\{f_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\}, \qquad \{g_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\}$$

se compose d'éléments distincts.

1. Introduction

Let $d \geq 2$ be an integer, $K/\mathbb{Q}$ a number field, and $N = N_{K/\mathbb{Q}}(\mathcal{P})$ the norm of an ideal $\mathcal{P} \subset \mathcal{O}_K$. Let $h(z) \in K[z]$ be non-constant and not of the form $h(z) = \xi z$, $\xi^{d-1} = 1$. For $\mathcal{P} \subset \mathcal{O}_K$ a prime ideal of good reduction, we consider $h(z) \in \mathbb{F}_{\mathcal{P}}[z]$, where $\mathbb{F}_{\mathcal{P}}$ is the residue field. Denote:

$$f_t(z) = z^d + t \tag{2}$$

and

$$g_t(z) = z^d + h(t). \tag{3}$$

The ℓ-th iteration of a polynomial map F is denoted by $F^{(\ell)}$.

We prove the following theorem.

Theorem 1. *There are constants c_1, c_2 depending on d and h such that the following holds. For almost all $\mathcal{P}$, there is a finite subset $T \subset \bar{\mathbb{F}}_{\mathcal{P}}$, $|T| \leq c_1$ such that if $t \in \bar{\mathbb{F}}_{\mathcal{P}} \setminus T$ at least one of the sets*

$$\{f_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\}, \qquad \{g_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log N]\} \tag{4}$$

consists of distinct elements.

Remark 1. Theorem 1 may be seen as a mod p version of Theorem 1.1 in [6], which falls into the theme of 'unlikely intersection in arithmetic dynamics' (see [2,7,8], formulated as a dynamical analogue of the André–Oort Conjecture by Baker and DeMarco [3]).

Remark 2. In Theorem 1, we take $f_t(z) = z^d + t$ and $g_t(z) = z^d + h(t)$ instead of $f_t(z) = z^d + k(t)$ with h and k unrelated, because the proof of Theorem 1.1 in [6] (which used a result in [8]) only works for pairs of polynomials of this form.

There are generalizations in different directions of our method that will be explored in a forthcoming paper. In particular, new developments in complex dynamics seem to allow results that are less restrictive for the iterated maps and those are expected to have a mod p counter part.

2. The proof

By Theorem 1.1 in [6], the subset of $\bar{\mathbb{Q}}$

$$S = \bigcup_{\ell' < \ell,\ m' < m} \{t : f_t^{(\ell)}(0) = f_t^{(\ell')}(0) \text{ and } g_t^{(m)}(0) = g_t^{(m')}(0)\} \tag{5}$$

is finite.

Let $F(t) \in \mathbb{Z}[t]$ be a nontrivial polynomial vanishing on S. For any $\ell' < \ell, m' < m$, let

$$B(t) = f_t^{(\ell)}(0) - f_t^{(\ell')}(0), \qquad C(t) = g_t^{(m)}(0) - g_t^{(m')}(0). \tag{6}$$

We note that $B(t) \in \mathbb{Z}[t]$ is a polynomial of degree d^ℓ and $C(t) \in K[t]$ of degree $\leq (\max(d, e))^m$, with $e = \deg h$. Since F vanishes on the common zero set of B and C, Theorem 5.1 in [4] asserts that there is some $A = A_{\ell,\ell',m,m'} \in \mathbb{Z} \setminus \{0\}$ and polynomials $P(t)$, $Q(t) \in \mathcal{O}[t]$, $\mathcal{O}$ being the ring of integers of K, such that

$$A\, F(t) = P(t)B(t) + Q(t)C(t). \tag{7}$$

Let c_3 refer to constants depending on d and h. Since the (logarithmic) heights of B and C may be bounded by $c_3^{\ell+m}$, Theorem 5.1 in [4] asserts that there exist P, Q of heights at most $c_3^{\ell+m}$ and $A \in \mathbb{N}$, $A < \exp c_3^{\ell+m}$ satisfying (7).

Let X be a large integer and consider the prime ideals $\mathcal{P}$, with $N(\mathcal{P}) < X$. Assume moreover that $\mathcal{P}$ is of good reduction for the polynomial $F(t)$ and $t \in \bar{\mathbb{F}}_{\mathcal{P}} \setminus T$, $T = T_{\mathcal{P}} =$ zero set of $F(t) \in \mathbb{F}_{\mathcal{P}}[t]$.

Assume that both sets

$$\left\{f_t^{(\ell)}(0) : \ell = 1, 2, \cdots, [c_2 \log X]\right\}, \qquad \left\{g_t^{(m)}(0) : m = 1, 2, \cdots, [c_2 \log X]\right\}$$

have repeated elements. Hence $B(t) = 0 = C(t)$ with B, C defined by (6), for some $\ell' < \ell < [c_2 \log X], m' < m < [c_2 \log X]$. Since $F(t) \neq 0$, (7) implies $\pi_{\mathcal{P}}(A_{\ell,\ell',m,m'}) = 0$, hence $p|\mathcal{A}$, where p is the rational prime dividing $N(\mathcal{P})$ and

$$\mathcal{A} = \prod_{\ell'<\ell<c_2 \log X,\ m'<m<c_2 \log X} A_{\ell,\ell',m,m'} < \exp\left(c_3^{c_2 \log X} \cdot (c_2 \log X)^4\right). \tag{8}$$

Choosing c_2 small enough will ensure $\mathcal{A} < e^{X^\tau}$ ($\tau > 0$ any fixed constant) and hence $\mathcal{A}$ with at most $O(X^\tau)$ prime divisors. It remains to exclude those primes $\mathcal{P}$ below divisors.

Remark 1. The proof gives $c_2 \log \log p$ instead of $c_2 \log p$ for any given $\mathcal{P}$ with $N(\mathcal{P})$ sufficiently large.

Remark 2. Our result is reminiscent of the work of Silverman [9], which was improved by Akbary and Ghioca [1] by removing the ε in the exponent. It should be noted that Silverman's result is a statement for individual maps and does not seem to apply directly to our problem. More specifically, the exceptional set of primes in [9] does depend on the map while here one has to deal with a family of pairs of maps $(f + a, f + b)$ with (a, b) on the curve V. As in other related arguments (cf. [5]), the main ingredients in passing to residue fields are height conditions and quantitative elimination theory.

Acknowledgements

During the preparation of this paper, the author was supported by the NSF Grants DMS 1301608 and by the NSF Grant 0932078000 while she was in residence at the Mathematical Science Research Institute in Berkeley, California, during the spring 2014 semester. This author would also like to thank the Mathematics Department of the University of California at Berkeley for its hospitality.

References

[1] A. Akbary, D. Ghioca, Periods of orbits modulo primes, J. Number Theory 129 (2009) 2831–2842.
[2] M. Baker, L. DeMarco, Preperiodic points and unlikely intersections, Duke Math. J. 159 (2011) 1–29.
[3] M. Baker, L. DeMarco, Special curves and postcritically-finite polynomials, Forum Math. Pi 1 (2013), e3 (35 p.).
[4] C. Berenstein, A. Yger, Effective Bezout identities in $\mathbb{Q}[Z1, \ldots, Zn]$, Acta Math. 166 (1991) 69–120.
[5] M.-C. Chang, Elements of large order in prime finite fields, Bull. Aust. Math. Soc. 88 (2013) 169–176.
[6] D. Ghioca, H. Krieger, K. Nguyen, A case of the dynamical Andre–Oort conjecture, Preprint.
[7] D. Ghioca, L.-C. Hsia, T.J. Tucker, Preperiodic points for families of polynomials, Algebra Number Theory 7 (2012) 701–732.
[8] D. Ghioca, L.-C. Hsia, T.J. Tucker, Preperiodic points for families of rational maps, Proc. Lond. Math. Soc. (2015), in press, arXiv:1210.7715.
[9] J.J. Silverman, Variation of periods modulo p in arithmetic dynamics, N.Y. J. Math. 14 (2008) 601–616.