On periods modulo p in arithmetic dynamics *†

Mei-Chu Chang‡
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

We prove the following mod p version of a case of the dynamical André-Oort conjecture obtained in [GKN].

Theorem. *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 $T \subset \bar{\mathbb{F}}_{\mathcal{P}}$, $|T| \le c_1$ such that if $t \in \bar{\mathbb{F}}_{\mathcal{P}} \setminus T$ at least one of the sets*

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

consists of distinct elements. Here $N = N_{K/\mathbb{Q}}(\mathcal{P})$.

§1. Introduction

Let $d \ge 2$ be an integer and $K/\mathbb{Q}$ a number field. 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

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

*2000 *Mathematics Subject Classification.* Primary 11A07, 11B50, 11B75; Secondary 37F10 11G50.
† *Key words.* dynamical system, orbits, Effective Nullstellensatz.
‡Research partially financed by the National Science Foundation.

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

We prove the following theorem, which may be seen as a mod p version of [GKN].

Theorem. *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*

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

consists of distinct elements. Here $N = N_{K/\mathbb{Q}}(\mathcal{P})$.

This result is a sample of other work in similar spirit that will appear in a forthcoming publication.

§2. The Proof

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

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

is finite.

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

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

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, the Effective Nullstellensatz [BY] (particularly, the first remark after the proof of Theorem 5.1) 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 $c_3^{\ell+m}$, the Effective Nullstellensatz 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, $\mathcal{P}$ of good reduction 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 both sets

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

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

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

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 reminisent of the work of Silverman [S], which was improved by Akbary and Ghioca [AG] 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 [S] 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 argument (cf [C]) 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

[AG] A. Akbary, D. Ghioca *Periods of orbits modulo primes*, J. Number Theory, 129 (2009), 2831 - 2842.

[BY] C. Berenstein, A. Yger *Effective Bezout identities in* $\mathbb{Q}[Z1, ..., Zn]$, Acta Math., 166 (1991), 69 - 120.

[C] M.-C. Chang *Elments of Large Order in Prime Finite Fields*, Bull. Aust. Math. Soc., 88 (2013) 169 - 176.

[GKN] D. Ghioca, H. Krieger, K. Nguyen *A case of the dynamical Andre-Oort conjecture*, (preprint)

[S] J. J. Silverman *Variation of periods modulo p in arithmetic dynamics*, New York J. Math. 14 (2008), 601 - 616.