*Glasgow Math. J.* **60** (2018) 487–493. © Glasgow Mathematical Journal Trust 2017.
doi:10.1017/S0017089517000222.

# MULTIPLICATIVE ORDERS IN ORBITS OF POLYNOMIALS OVER FINITE FIELDS

IGOR E. SHPARLINSKI

*School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia*
*e-mail: igor.shparlinski@unsw.edu.au*

(Received 26 March 2017; accepted 7 August 2017; first published online 23 October 2017)

**Abstract.** We show, under some natural restrictions, that orbits of polynomials cannot contain too many elements of small multiplicative order modulo a large prime $p$. We also show that for all but finitely many initial points either the multiplicative order of this point or the length of the orbit it generates (both modulo a large prime $p$) is large. The approach is based on the results of Dvornicich and Zannier (*Duke Math. J.* **139** (2007), 527–554) and Ostafe (2017) on roots of unity in polynomial orbits over the algebraic closure of the field of rational numbers.

2010 *Mathematics Subject Classification.* Primary 11T06, 37P05, 37P25.

## 1. Introduction.

**1.1. Background.** Let $f(X) \in \mathbb{K}[X]$ be a polynomial of degree $d \geq 2$ over a field $\mathbb{K}$.

We set $f^{(0)} = X$ and then define the $n$th iterate of $f$ recursively as $f^{(n)}(X) = f\left(f^{(n-1)}(X)\right)$, $n = 1, 2, \ldots$.

Given $w \in \mathbb{K}$, we define its orbit $\mathrm{Orb}(w)$ with respect to the polynomial $f$ as the set

$$\mathrm{Orb}(w) = \{f^{(n)}(w) \ : \ n = 0, 1, \ldots\}. \tag{1}$$

We call $w \in \mathbb{K}$ the *initial value* of $\mathrm{Orb}(w)$.

For a prime $p$ and an integer $k \geq 1$, let $\mathbb{F}_{p^k}$ denote the finite field of $p^k$ elements. Clearly, if $\mathbb{K} = \overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$, then for any $w \in \overline{\mathbb{F}}_p$, the sequence $f^{(n)}(w)$, $n = 0, 1, \ldots$, is eventually periodic and if $w \in \mathbb{F}_{p^k}$ and $f(X) \in \mathbb{F}_{p^k}[X]$, then $\mathrm{Orb}(w)$ is a finite of cardinality

$$T(w) = \#\mathrm{Orb}(w) \leq p^k.$$

The orbit lengths of the reductions of polynomials have recently being studied by different methods and from various points of view, see **[1, 3–6, 14]** and references therein.

Furthermore, for each $u \in \overline{\mathbb{F}}_p^*$, we define the *multiplicative order* $\tau(u)$ as the smallest integer $\ell \geq 1$ with $u^\ell = 1$ (we also set $\tau(0) = 0$).

Several results about the distribution of multiplicative orders of elements in orbits $\mathrm{Orb}(w)$ have been studied in **[13]**. In particular, in **[13]**, for a fixed polynomial

$f(X) \in \mathbb{Z}[X]$ and $w \in \mathbb{F}_p$, various lower bounds are given on the size of the smallest subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ that contains all non-zero values of the sequence $f^{(n)}(w)$, $n = 0, \ldots, N-1$, for $N \le T(w)$.

Here, we consider the interplay between the period length and the multiplicative order of points $w \in \overline{\mathbb{F}}_p$, and obtain several new results in this direction.

Namely, given a positive integer $N \le T(w)$), we define by $M_w(t; N)$ the number of elements amongst the first $N$ elements of the orbit $\mathrm{Orb}(w)$ or multiplicative order at most $t$, that is,

$$M_w(t; N) = \#\{n \le N-1 \ : \ \tau(\left(f^{(n)}(w)\right) \le t\}.$$

Using recent results of Ostafe [**10**] about roots of unity in polynomial orbits over algebraic number fields, we obtain a lower bound on $M_w(t; N)$ when the polynomial $f$ is defined over $\mathbb{Q}$, and then reduced modulo $p$ (for a sufficiently large prime $p$). In fact, using the results of [**10**] in full generality, one can extend this to polynomials over arbitrary algebraic number fields.

We also consider a related question and show that for a natural class of polynomials $f \in \mathbb{Z}[X]$, for all but $O(1)$ points $w \in \overline{\mathbb{F}}_p$, the dynamical or multiplicative order is large (where the implied constant in $O(1)$ depends only on $f$). This is based on the result of Dvornicich and Zannier [**7**, Theorem 2] on the finiteness of algebraic cyclotomic points $w \in \overline{\mathbb{Q}}$, which are preperiodic, that is, for which $\mathrm{Orb}(w)$ is finite.

**1.2. Notation, conventions and definitions.** We use $\mathbb{U}$ to denote the set of all roots of unity in $\mathbb{C}$.

We also use $T_d$ to denote the Chebyshev polynomial of degree $d$, which is uniquely determined by the equation $T_d(X + X^{-1}) = X^d + X^{-d}$.

We now define the following class of *exceptional polynomials*.

DEFINITION 1.1. We call a polynomial $f \in \mathbb{Z}[X]$ to be exceptional if for some linear polynomial $L(X) = aX + b \in \mathbb{Q}[X]$, the composition

$$L\left(f\left(L^{-1}(X)\right)\right) = af\left(a^{-1}(X-b)\right) + b$$

is either $(\pm X)^d$ or $T_d(\pm X)$.

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$. Throughout the paper, any implied constants in the symbols $O$, $\ll$ and $\gg$ may depend on the polynomial $f$ and the real positive parameter $\varepsilon$ but are uniform in the prime $p$ and the point $w \in \overline{\mathbb{F}}_p$.

**1.3. Main results.** We start with a bound on the largest multiplicative order amongst the first $N$ iterates.

THEOREM 1.2. *Assume that* $f(X) \in \mathbb{Z}[X]$ *is not exceptional with* $\deg f = d \ge 2$. *Then, for any fixed* $\varepsilon > 0$,

(*i*) *for any prime* $p$ *and* $t \le (\log p)^{1/2-\varepsilon}$ *for all initial values* $w \in \overline{\mathbb{F}}_p$, *we have*

$$M_w(t; N) \ll \max\{N^{1/2}, N/\log\log p\};$$

https://doi.org/10.1017/S0017089517000222 Published online by Cambridge University Press

(*ii*) *for any sufficiently large* $P \geq 1$ *and* $t \leq P^{1/2-\varepsilon}$ *for all but* $o(P/\log P)$ *primes* $p \leq P$ *for all initial values* $w \in \overline{\mathbb{F}}_p$, *we have*

$$M_w(t; N) \ll \max\{N^{1/2}, N/\log p\}.$$

We also show that for all but a bounded (only in terms of $f$) number of $w \in \overline{\mathbb{F}}_p$, either $T(w)$ or $\tau(w)$ is large.

THEOREM 1.3. *If* $f(X) \in \mathbb{Z}[X]$ *is not exceptional with* $\deg f = d \geq 2$. *Then,*
(*i*) *for any prime* $p$ *for all but* $O(1)$ *initial values* $w \in \overline{\mathbb{F}}_p$, *we have*

$$d^{T(w)}\tau(w) \gg \log p;$$

(*ii*) *for any sufficiently large* $P \geq 1$ *and any function* $\psi(z) \to 0$ *as* $z \to \infty$, *for all but* $o(P/\log P)$ *primes* $p \leq P$ *for all initial values* $w \in \overline{\mathbb{F}}_p$, *we have*

$$d^{T(w)}\tau(w) \gg P\psi(P).$$

## 2. Preliminaries.

**2.1. Orbits and roots of unity.** We now formulate two very special cases of the results of Dvornicich and Zannier [**7**] and Ostafe [**10**].

First, we recall that by [**7**, Theorem 2], we have the following.

LEMMA 2.1. *If* $f(X) \in \mathbb{Z}[X]$ *is not exceptional with* $\deg f = d \geq 2$, *then there are finitely many* $u \in \mathbb{U}$ *for which* $\mathrm{Orb}(u)$ *is finite.*

Furthermore, by [**10**] we also have the following.

LEMMA 2.2. *If* $f(X) \in \mathbb{Z}[X]$ *is not exceptional with* $\deg f = d \geq 2$, *then there are finitely many* $u \in \mathbb{U}$ *for which* $f^{(n)}(u) \in \mathbb{U}$ *for some integer* $n \geq 1$.

**2.2. Heights of polynomials and their iterates.** For a polynomial $F \in \mathbb{Z}[X]$, we define its *height*, denoted by $\mathrm{h}(F)$, as the logarithm of the maximum of the absolute values of its coefficients.

We recall the well-known bound for the height of the composition of polynomials, see, for instance, [**8**, Lemma 1.2(1.c)], where it is given in a much larger generality for multivariate polynomials.

LEMMA 2.3. *Let* $F, G \in \mathbb{Z}[X]$. *Then,*

$$\mathrm{h}(F(G)) \leq \mathrm{h}(F) + \deg F\,(\mathrm{h}(G) + (\deg G + 1)\log 2)\,.$$

Hence, by induction on $n$, we now immediately derive from Lemma 2.3 the following bound on the height of iterations of polynomials (see also [**6**] for a fully explicit bound in the multivariate case)

LEMMA 2.4. *Let* $f \in \mathbb{Z}[X]$. *be of degree* $d \geq 2$. *Then,*

$$\mathrm{h}\left(f^{(n)}\right) = O(d^n).$$

https://doi.org/10.1017/S0017089517000222 Published online by Cambridge University Press

Let $\Phi_k$ denote the $k$th cyclotomic polynomial.

We now recall the following very simplified version of the classical result of Bateman, Pomerance and Vaughan [**2**].

LEMMA 2.5. *For $k \to \infty$,*

$$\mathrm{h}(\Phi_k) = k^{o(1)}.$$

Combining Lemmas 2.3 and 2.5 with the trivial upper bound on the Sylvester determinant formula for the resultant $\mathrm{Res}(F, G)$ of two polynomials $F, G \in \mathbb{Z}[X]$, we derive.

LEMMA 2.6. *For any integers $r, s \geq 1$ and $F \in \mathbb{Z}[U]$, we have*

$$\mathrm{Res}(\Phi_r, \Phi_s(F)) = \exp(O(rs(\mathrm{h}(F) + \deg F))).$$

**2.3. Combinatorial result.** We also need the following combinatorial statement that in different forms has been used in a number of works, see [**6, 9, 12**]. In the form below it is given in [**11**].

LEMMA 2.7. *Let $\mathcal{S} \subseteq \mathbb{K}$ be an arbitrary subset of a field $\mathbb{K}$ and let $w \in \mathbb{K}$. If for some $\vartheta > 0$, we have*

$$\#\{0 \leq n \leq N-1 \ : \ f^{(n)}(w) \in \mathcal{S}\} \geq \vartheta N,$$

*then there is a non-negative integer $m \leq 2\vartheta^{-1}$ such that*

$$\#\{f^{(m)}(u) = v \ : \ u, v \in \mathcal{S}\} \geq \frac{\vartheta^2 N}{8}.$$

## 3. Proofs of main results.

**3.1. Proof of Theorem 1.2.** As before we use $\Phi_k$ to denote the $k$th cyclotomic polynomial. We fix some positive parameter $\rho < 1$ and consider some $w \in \overline{\mathbb{F}}_p$ with

$$M_w(t; N) \geq \rho N. \tag{2}$$

Then there are at least $\rho N$ values of $n < N$ with

$$\Phi_\ell\left(f^{(n)}(w)\right) = 0$$

for some positive integer $\ell \leq t$. (where the equations are in $\overline{\mathbb{F}}_p$). Hence, by Lemma 2.7, there is some positive integer $m \leq 2\rho^{-1}$ such that for at least $\rho^2 N/8$ distinct values $u \in \overline{\mathbb{F}}_p$, we have

$$\Phi_k(u) = \Phi_\ell\left(f^{(m)}(u)\right) = 0 \tag{3}$$

for some pair $(k, \ell) \in [1, t]^2$. Denote by $R_{k,\ell,m}$ the resultant of the polynomials $\Phi_k(U)$ and $\Phi_\ell\left(f^{(m)}(U)\right)$ (considered over $\mathbb{Z}$, so we have $R_{k,\ell,m} \in \mathbb{Z}$).

https://doi.org/10.1017/S0017089517000222 Published online by Cambridge University Press

By Lemma 2.2, we see that there are only finitely many values of $m$ for which $R_{k,\ell,m} = 0$ is possible for some $k$ and $\ell$. Thus, there are at most $c_1$ values of $u \in \overline{\mathbb{F}}_p$ which are solutions to (3), which correspond to such triples, where the constant $c_1$ depends only on $f$. Thus, if $\rho^2 N/8 > c_1$, then there is a triple $(k, \ell, m)$ with $R_{k,\ell,m} \neq 0$ and such that (3) has a solution and therefore

$$p \mid R_{k,\ell,m}. \tag{4}$$

Hence, we now assume that

$$\rho > \sqrt{8c_1/N} \tag{5}$$

and thus (4) holds. Using that by Lemmas 2.4 and 2.6 if $R_{k,\ell,m} \neq 0$, then

$$\log |R_{k,\ell,m}| \ll k\ell d^m \ll t^2 d^{2\rho^{-1}}.$$

We note that $R_{k,\ell,m}$ depends only on $k$, $\ell$, $m$ and $f$ but does not depend on $p$.

We now see that (4) implies

$$\log p \ll t^2 d^{2\rho^{-1}}.$$

Thus, using the condition $t \leq (\log p)^{1/2-\varepsilon}$, we derive

$$d^{2\rho^{-1}} \gg t^{-2} \log p \geq (\log p)^{2\varepsilon}$$

or

$$\rho \leq c_2 (\log \log p)^{-1}. \tag{6}$$

Hence, taking

$$\rho = \max\{3\sqrt{c_1/N}, 2c_2(\log \log p)^{-1}\}$$

for some constant $c_2$ that depends only on $f$ satisfies (5) but contradicts this condition (6). This means that the inequality (2) fails for the above value of $\rho$, which concludes the proof of Part (i).

For Part (ii), we see that if $R_{k,\ell,m} \neq 0$, then the number of primes with (4) is at most

$$\omega(R_{k,\ell,m}) \leq 2 \log |R_{k,\ell,m}| \ll t^2 d^{2\rho^{-1}} \leq P^{1-2\varepsilon} d^{2\rho^{-1}},$$

where, as usual, we use $\omega(r)$ to denote the number of distinct prime divisors of an integer $s \neq 0$. Hence, if

$$\rho \geq \frac{1}{\varepsilon \log d \log P}$$

then $\omega(R_{k,\ell,m}) = o(P/\log P)$, which implies the bound of Part (ii).

**3.2. Proof of Theorem 1.3.** Fix some parameter $t \geq 1$ and assume that for $w \in \overline{\mathbb{F}}_p$, we have

$$d^{T(w)} \tau(w) \leq t.$$

https://doi.org/10.1017/S0017089517000222 Published online by Cambridge University Press

Then, we see that for some integers $k, \ell, m$ with

$$T(w) = k > \ell \ge 0 \qquad \text{and} \qquad m = \tau(w), \tag{7}$$

we have

$$f^{(k)}(w) = f^{(\ell)}(w) \qquad \text{and} \qquad \Phi_m(w) = 0. \tag{8}$$

Denote by $Q_{k,\ell,m}$ the resultant of the polynomials $f^{(k)}(U) - f^{(\ell)}(U)$ and $\Phi_m(U)$ (considered over $\mathbb{Z}$, so we have $Q_{k,\ell,n} \in \mathbb{Z}$). We now conclude from (8) that

$$p \mid Q_{k,\ell,m}$$

and if

$$|Q_{k,\ell,m}| < p \tag{9}$$

then $Q_{k,\ell,m} = 0$ and thus the system of equations (8) has a root over $\mathbb{C}$. This implies that there are only $O(1)$ triples $(k, \ell, m)$ that satisfy this condition and so, there are only $O(1)$ values of $w \in \overline{\mathbb{F}}_p$ that satisfy (8) for some integers $k, \ell, m$ as in (7) (where the implied constants depend only on $f$).

We now use Lemma 2.6 with $r = m$, $s = 1$ and $F(U) = f^{(k)}(U) - f^{(\ell)}(U) + 1$. Recalling the bound $d^k m = d^{T(w)}\tau(w) \le t$, we derive

$$|Q_{k,\ell,m}| = \exp\left(O\left(d^k m\right)\right) = \exp\left(O\left(t\right)\right). \tag{10}$$

Hence, taking $t = c_0 \log p$ for an appropriate constant $c_0 > 0$ that depends only on $f$, we see that we have (9), which concludes the proof of Part (i).

For Part (ii), we note that if $Q_{k,\ell,m} \ne 0$, then $Q_{k,\ell,m}$ has at most

$$\omega\left(Q_{k,\ell,m}\right) \ll \frac{\log |Q_{k,\ell,m}|}{\log\log\left(|Q_{k,\ell,m}| + 2\right)}$$

prime divisors (which follows from the trivial inequality $\omega(s)! \le s$, that holds for any integer $s \ge 1$, and the Stirling formula). Using (10) and also the bound $d^k m = d^{T(w)}\tau(w) \le t$, we derive

$$\omega\left(Q_{k,\ell,m}\right) \ll t/\log t.$$

Taking $t = P\psi(P)$, we conclude the proof of Part (ii).

**4. Comments.** We note that by using the results of Dvornicich and Zannier [**7**] and Ostafe [**10**] in full generality one can easily extend our estimates to polynomials $f$ over algebraic number fields.

On the other hand, as long as multivariate analogues of [**7**] and [**10**] are not available we do not see any approaches to extending our results to multivariate polynomials. In fact, the lack of such extensions of [**7**] and [**10**] is the only essential obstacle for generalisations to multivariate polynomials as the results of [**6**] provide an adequate substitute to our resultant-based argument. Finding an alternative approach is also very desirable as it may lead to stronger bounds.

https://doi.org/10.1017/S0017089517000222 Published online by Cambridge University Press

Probably the most challenging question is to obtain versions of our results that are uniform in the polynomial $f$ in (1). In particular, it is important to allow $f$ to be defined over $\mathbb{F}_p$, or even $\overline{\mathbb{F}}_p$ rather than over $\mathbb{Z}$.

ACKNOWLEDGEMENTS. This work was supported by the Australian Research Council Grant DP170100786.

## REFERENCES

**1.** A. Akbary and D. Ghioca, Periods of orbits modulo primes, *J. Number Theory* **129** (2009), 2831–2842.

**2.** P. T. Bateman, C. Pomerance and R. C. Vaughan, On the size of the coefficients of the cyclotomic polynomial, in *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, Colloq. Math. Soc. János Bolyai, vol. 34 (North-Holland, Amsterdam, 1984), 171–202.

**3.** R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon and T. J. Tucker, Periods of rational maps modulo primes, *Math. Ann.* **355** (2013), 637–660.

**4.** M.-C. Chang, On periods modulo $p$ in arithmetic dynamics, *C. R. Acad. Sci. Paris, Ser. I* **353** (2015), 283–285.

**5.** M.-C. Chang, C. D'Andrea, A. Ostafe, I. E. Shparlinski and M. Sombra, Orbits of polynomial dynamical systems modulo primes, *Proc. Amer. Math. Soc.*, (to appear).

**6.** C. D'Andrea, A. Ostafe, I. E. Shparlinski and M. Sombra, Reduction modulo primes of systems of polynomial equations and algebraic dynamical systems, *Preprint*, 2015 (see `http://arxiv.org/abs/1505.05814`).

**7.** R. Dvornicich and U. Zannier, Cyclotomic diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps), *Duke Math. J.* **139** (2007), 527–554.

**8.** T. Krick, L. M. Pardo and M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, *Duke Math. J.* **109** (2001), 521–598.

**9.** A. Ostafe, Polynomial values in affine subspaces of finite fields, *J. d'Analyse Math.* (to appear).

**10.** A. Ostafe, On roots of unity in orbits of rational functions, *Proc. Amer. Math. Soc.* **145** (2017), 1927–1936.

**11.** A. Ostafe and I. E. Shparlinski, Orbits of algebraic dynamical systems in subfields and subgroups, in *Number theory – diophantine problems, uniform distribution and applications; festschrift in honour of Robert F. Tichy's 60th Birthday* (Elsholz C. and Grabner P., Editors) (Springer, 2017), 347–368.

**12.** O. Roche-Newton and I. E. Shparlinski, Polynomial values in subfields and affine subspaces of finite fields, *Quart. J. Math.* **66** (2015), 693–706.

**13.** I. E. Shparlinski, Groups generated by iterations of polynomials over finite fields, *Proc. Edinburgh Math. Soc.* **59** (2016), 235–245.

**14.** J. H. Silverman, Variation of periods modulo $p$ in arithmetic dynamics, *New York J. Math.* **14** (2008), 601–616.