Variation of Periods Modulo $p$ in Arithmetic Dynamics

JOSEPH H. SILVERMAN

Abstract. Let $\varphi : V \rightarrow V$ be a self-morphism of a quasiprojective variety defined over a number field $K$ and let $P \in V(K)$ be a point with infinite orbit under iteration of $\varphi$. For each prime $p$ of good reduction, let $m_p(\varphi, P)$ be the size of the $\varphi$-orbit of the reduction of $P$ modulo $p$. Fix any $\epsilon > 0$. We show that for almost all primes $p$ in the sense of analytic density, the orbit size $m_p(\varphi, P)$ is larger than $(\log N_{K/Q})^{1-\epsilon}$.

Introduction

Let
$$\varphi : \mathbb{P}^N_Q \longrightarrow \mathbb{P}^N_Q$$
be a morphism of degree $d$ defined over $\mathbb{Q}$ and let $P \in \mathbb{P}^N(\mathbb{Q})$ be a point with infinite forward orbit
$$\mathcal{O}_\varphi(P) = \{ P, \varphi(P), \varphi^2(P), \ldots \}.$$ 
For all but finitely many primes $p$, we can reduce $\varphi$ to obtain a morphism
$$\tilde{\varphi}_p : \mathbb{P}^N_{\mathbb{F}_p} \longrightarrow \mathbb{P}^N_{\mathbb{F}_p}$$
whose degree is still $d$. We write $m_p(\varphi, P)$ for the size of the orbit of the reduced point $\tilde{P} = P \mod p$,
$$m_p(\varphi, P) = \#\mathcal{O}_{\tilde{\varphi}_p}(\tilde{P}).$$ (For the remaining primes we define $m_p(\varphi, P)$ to be $\infty$.)

Using an elementary height argument (see Corollary 10), one can show that
$$m_p(\varphi, P) \geq d \log \log p + O(1) \quad \text{for all } p,$$
but this is a very weak lower bound for the size of the mod $p$ orbits. Our principal results say that for most primes $p$, we can do (almost) exponentially better. In the following result, we write $\delta(P)$ for the...
logarithmic analytic density of a set of primes $\mathcal{P}$. (See Section 1 for the precise definition of $\delta$ and the associated lower density $\hat{\delta}$.)

**Theorem 1.** With notation as above, we have the following:

(a) For all $\gamma < 1$,

$$\delta \{ p : m_p(\varphi, P) \geq (\log p)^\gamma \} = 1.$$ 

(b) There is a constant $C = C(N, \varphi, P)$ so that for all $\epsilon > 0$,

$$\hat{\delta} \{ p : m_p(\varphi, P) \geq \epsilon \log p \} \geq 1 - C\epsilon.$$ 

More generally, we prove analogous results for any self-morphism $\varphi : V \to V$ of a quasiprojective variety $V$ defined over a number field $K$. See Section 1 for the basic setup and Theorem 3 for the precise statement of our main result.

The proof of Theorem 1, and its generalization Theorem 3, proceeds in two steps. In the first step we prove that there is an integer $D(m)$ satisfying $\log \log D(m) \ll m$ with the property that

$$m_p(\varphi, P) \leq m \quad \text{if and only if} \quad p|D(m).$$

This is done using a height estimate for rational maps (Proposition 4) and a height estimate for arithmetic distances (Proposition 6). The second part of the proof uses the first part to prove an analytic estimate (Theorem 11) of the following form: for all $\lambda \geq 1$ there is a constant $C = C(\varphi, \lambda)$ so that

$$\sum_{p \text{ prime}} \frac{\log p}{p e^{m_p(\varphi, P)_s}} \leq \frac{C}{s^{1/\lambda}} \quad \text{for all} \quad s > 0. \quad (1)$$

The inequality (1) is a dynamical analogue of the results in [9], which treated the case of periods modulo $p$ of points in algebraic groups.

Theorem 1 says that for most $p$, the mod $p$ orbit of $P$ has size (almost) as large as $\log p$. If $\varphi$ were a random map, we would expect most orbits to have size on the order of $\sqrt{\# \mathbb{P}^N(\mathbb{F}_p)} \approx p^{N/2}$. In Section 6 we do some experiments using quadratic polynomials $\varphi_c(z) = z^2 + c$ which seem to suggest that $m_p(\varphi_c, \alpha)$ grows slightly slower than $\sqrt{p}$.

1. **Notation and Statement of Main Result**

In this section we set notation for our basic objects of study, give some basic definitions, and state our main result. We start with the dynamical setup.

**Definition.** Let $K/\mathbb{Q}$ be a number field, let $V \subset \mathbb{P}^N_K$ be a quasiprojective variety defined over $K$, and let 

$$\varphi : V \longrightarrow V$$
be a morphism defined over $K$. Fix a point $P \in V(K)$ whose forward $\varphi$-orbit
$$O_\varphi(P) = \{ P, \varphi(P), \varphi^2(P), \ldots \}$$
is infinite. For each prime ideal $\mathfrak{p}$ of $K$ at which $V$ and $\varphi$ have good reduction, let
$$m_\mathfrak{p} = m_\mathfrak{p}(\varphi, P) = \text{size of the } \tilde{\varphi}\text{-orbit of } \tilde{P} \text{ in } \tilde{V}(\mathbb{F}_p).$$
If $V$ has bad reduction at $\mathfrak{p}$, we set $m_\mathfrak{p} = \infty$.

**Remark 2.** The question of good versus bad reduction requires choosing models for $V$ and $\varphi$ over the ring of integers of $K$. However, different choices affect only finitely many of the $m_\mathfrak{p}(\varphi, P)$ values, and thus have no effect on our density results. We thus assume throughout that a particular model has been fixed.

We next define the analytic density that will be used in the statement of our main result.

**Definition.** Let $K/\mathbb{Q}$ be a number field with ring of integers $R_K$. For any set of primes $\mathcal{P} \subseteq \text{Spec}(R_K)$, define the partial $\zeta$-function for $\mathcal{P}$ by
$$\zeta_K(\mathcal{P}, s) = \prod_{\mathfrak{p} \in \mathcal{P}} \left( 1 - \frac{1}{N_{K/\mathbb{Q}} \mathfrak{p}^s} \right)^{-1}.$$ This Euler product defines an analytic function on $\text{Re}(s) > 1$. As usual, we write $\zeta_K(s)$ for the $\zeta$-function of the field $K$. Then the (logarithmic analytic) density of $\mathcal{P}$ is given by the following limit, assuming that the limit exists:
$$\delta(\mathcal{P}) = \lim_{s \to 1^+} \frac{d \log \zeta_K(\mathcal{P}, s)}{d \log \zeta_K(s)} = \lim_{s \to 1^+} \frac{\zeta'_K(\mathcal{P}, s)/\zeta_K(\mathcal{P}, s)}{\zeta'_K(s)/\zeta_K(s)}.$$ Expanding the logarithm before differentiating and using the fact that $\zeta_K(s)$ has a simple pole at $s = 1$, it is easy to check that the density is also given by the formula
$$\delta(\mathcal{P}) = \lim_{s \to 1^+} (s - 1) \sum_{\mathfrak{p} \in \mathcal{P}} \frac{\log N_{K/\mathbb{Q}} \mathfrak{p}}{N_{K/\mathbb{Q}} \mathfrak{p}^s}.$$ We similarly define upper and lower densities $\delta(\mathcal{P})$ and $\bar{\delta}(\mathcal{P})$ by replacing the limit with the limsup or the liminf, respectively.

With this notation, we can now state our main result.

**Theorem 3.** Let $K/\mathbb{Q}$ be a number field and let $\varphi : V/K \to V/K$, and $P \in V(K)$ be as described in this section. Further, let $m_\mathfrak{p}(\varphi, P)$ denote the size of the $\tilde{\varphi}$-orbit of $\tilde{P}$ in $\tilde{V}(\mathbb{F}_p)$. 

(a) For all $\gamma < 1$ we have
$$\delta \{ p \in \text{Spec } R_K : m_p(\varphi, P) \geq (\log Np)^\gamma \} = 1.$$ 

(b) There is a constant $C = C(K, V, \varphi, P)$ so that for all $\epsilon > 0$,
$$\delta \{ p \in \text{Spec } R_K : m_p(\varphi, P) \geq \epsilon \log Np \} \geq 1 - C\epsilon.
$$

2. HEIGHT AND NORM ESTIMATES

In this section we prove various estimates for heights and norms that will be needed for the proof of our main result. To ease notation, for the remainder of this paper we fix the number field $K/\mathbb{Q}$ and write $N_a$ for the $K/\mathbb{Q}$ norm of a fractional ideal $a$ of $K$.

**Proposition 4.** With notation as in Section 1 and Theorem 3, there are constants
$$d = d(V, \varphi) \geq 2 \quad \text{and} \quad C = C(V, \varphi) \geq 0$$
so that
$$h(\varphi^n(Q)) \leq d^n(h(Q) + C) \quad \text{for all } n \geq 0 \text{ and all } Q \in V(K).$$

*Proof.* We are given that $\varphi$ is a morphism on $V$, but note that $V$ is only quasiprojective, i.e., $V$ is a Zariski open subset of a Zariski closed subset of $\mathbb{P}^N$. We write $V$ as a union of open subsets $V_1, \ldots, V_t$ such that on each $V_i$ we can write
$$\varphi_i = \varphi|_{V_i} = [F_{i0}, F_{i1}, \ldots, F_{IN}],$$
where the $F_{ij}$ are homogeneous polynomials and such that
$$F_{i0}, F_{i1}, \ldots, F_{iN} \quad \text{do not simultaneously vanish on } V_i.$$ 

We may view $\varphi_i$ as a rational map $\varphi_i : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$ of degree $d_i = \deg F_{ij}$. Letting $Z_i \subset \mathbb{P}^N$ be the locus of indeterminacy for the rational map $\varphi_i$, we have the elementary height estimate
$$h(\varphi_i(Q)) \leq d_i h(Q) + C(\varphi_i), \quad \text{valid for all } Q \in \mathbb{P}^N(\overline{K}) \setminus Z_i. \quad (2)$$
(See [6, Theorem B.2.5(a)].) By construction,
$$V \cap Z_1 \cap Z_2 \cap \cdots \cap Z_t = \emptyset,$$
so for all $Q \in V(\overline{K})$ we obtain the inequality
$$h(\varphi(Q)) = h(\varphi_i(Q)) \leq \max_{i \text{ with } Q \not\in Z_i} d_i h(Q) + C(\varphi_i) \quad \text{from (2)},$$
$$\leq \max_{1 \leq i \leq n} d_i h(Q) + \max_{1 \leq i \leq n} C(\varphi_i).$$
Setting
\[ d = \max\{2, d_1, \ldots, d_t\} \quad \text{and} \quad C = \max\{C(\varphi_1), \ldots, C(\varphi_t)\}, \]
we have
\[ h(\varphi(Q)) \leq dh(Q) + C \quad \text{for all} \quad Q \in V(\overline{K}). \]
Applying this iteratively yields
\[ h(\varphi^n(Q)) \leq d^n h(Q) + C, \quad (3) \]
(note that \( d \geq 2 \) by assumption) which is the desired result. \( \square \)

**Remark 5.** If \( \varphi : \mathbb{P}^N \to \mathbb{P}^N \) is a finite morphism, then in the statement of Proposition 4 we can take \( d = \max\{\deg \varphi, 2\} \). More precisely, in this situation a standard property of height functions [6, B.2.5(b)] gives upper and lower bounds,
\[ h(\varphi^n(Q)) = d^n (h(Q) + O(1)). \]
For maps of degree 1, the middle inequality in (3) yields the stronger estimate
\[ h(\varphi^n(Q)) \leq h(Q) + Cn. \]
Tracing through the proofs in this paper, this would give an exponential improvement in our results. For example, consider a linear map \( \varphi(z) = az \) with \( a \in \mathbb{Q}^\ast \), so \( m_p(\varphi, 1) \) is the order of \( a \) in the multiplicative group \( \mathbb{F}_p^\ast \). Then in place of (1) we would obtain
\[ \sum_{p \text{ prime}} \frac{\log p}{pm_p(\varphi, 1)^s} \leq \frac{2}{s} + O(1), \quad (4) \]
and this would allow us to replace Theorem 1(b) with
\[ \delta\{p : m_p(\varphi, 1) \geq p^\epsilon\} \geq 1 - 2\varepsilon. \quad (5) \]
However, we will not pursue the degree 1 case, because both (4) and (5) are special cases of the general results on algebraic groups proven in [9], see in particular [9, equation (3)] and the remark following [9, Theorem 4.2].

**Proposition 6.** Let \( K/\mathbb{Q} \) be a number field and let
\[ \alpha_0, \ldots, \alpha_N, \beta_0, \ldots, \beta_N \in K \]
be elements of \( K \) with at least one \( \alpha_i \) and at least one \( \beta_i \) nonzero. Define fractional ideals
\[ \mathfrak{A} = (\alpha_0, \ldots, \alpha_N), \quad \mathfrak{B} = (\beta_0, \ldots, \beta_N), \quad \mathfrak{D} = (\alpha_i \beta_j - \alpha_j \beta_i)_{0 \leq i < j \leq N}. \]
Also let $A = [\alpha_0, \ldots, \alpha_N] \in \mathbb{P}^N(K)$ and $B = [\beta_0, \ldots, \beta_N] \in \mathbb{P}^N(K)$, and assume that $A \neq B$. Then
\[
\frac{1}{[K:Q]} \log \left( \frac{N\mathcal{D}}{N\mathcal{A} \cdot N\mathcal{B}} \right) \leq h(A) + h(B) + O(1),
\]
where the $O(1)$ depends only on $N$. (Here $h$ is the absolute logarithm height on $\mathbb{P}^N(\overline{\mathbb{Q}})$.)

Proof. We give a proof using the machinery of heights relative to closed subschemes developed in [11], although for the specific result that we need, some readers may prefer to write down a direct proof. We assume that the absolute values on $K$ have been normalized so as to obtain the absolute height, i.e., the height of a point $P = [x_0, \ldots, x_N]$ is given by $h(P) = \sum_{v \in M_K} \max_i \{-v(x_i)\}$.

Since $A \neq B$, there are indices $i$ and $j$ such that $\alpha_i \beta_j \neq \alpha_j \beta_i$. Relabeling the coordinates, we may assume without loss of generality that $\alpha_0 \beta_1 \neq \alpha_1 \beta_0$. We define subvarieties $D$ and $\Delta$ of $\mathbb{P}^N \times \mathbb{P}^N$ by
\[
D = \{x_0 y_1 = x_1 y_0\} \quad \text{and} \quad \Delta = \{x_i y_j = x_j y_i \text{ for all } i \text{ and } j\}.
\]
Thus $\Delta$ is the diagonal of $\mathbb{P}^N \times \mathbb{P}^N$, while $D$ is a divisor of type $(1,1)$. In particular, if we let $\pi_1$ and $\pi_2$ be the projections $\mathbb{P}^N \times \mathbb{P}^N \to \mathbb{P}^N$ and let $H$ be a hyperplane in $\mathbb{P}^N$, then $D$ is linearly equivalent to $\pi_1^*H + \pi_2^*H$.

We also observe that $\Delta \subset D$. It follows from [11] that
\[
\lambda_\Delta(P, v) \leq \lambda_D(P, v) + O_v(1) \quad \text{for all } P \in ((\mathbb{P}^N \times \mathbb{P}^N) \setminus |D|)(K). \tag{6}
\]
Here $O_v(1)$ denotes an $M_K$-bounded function (i.e., it is bounded by an $M_K$-constant) in the sense of Lang [8]. Note that our assumption on $A$ and $B$ ensures that $(A, B)$ is not in the support of $D$. We also note that since $D$ is an effective divisor, the local height $\lambda_D$ is bounded below by an $M_K$-constant for all $P$ not in the support of $D$. Hence evaluating (6) at $P = (A, B)$ and summing over all nonarchimedean $v$ yields
\[
\sum_{v \in M_K^0} \lambda_\Delta((A, B), v) \leq \sum_{v \in M_K^0} (\lambda_D((A, B), v) + O_v(1))
\leq \sum_{v \in M_K} \lambda_D((A, B), v) + O(1)
= h_D((A, B)) + O(1)
= h_{\pi_1^*H + \pi_2^*H}((A, B)) + O(1)
= h(A) + h(B) + O(1). \tag{7}
\]
It remains to compute the local height relative to the diagonal. (In [11], \( \lambda_\Delta \) is called an arithmetic distance function.) From [11] and knowledge of the generators of the ideal defining \( \Delta \), we see that a representative local height function for \( \Delta \) is given by

\[
\lambda_\Delta((A, B), v) = \min_{0 \leq i < j \leq N} v(\alpha_i \beta_j - \alpha_j \beta_i) - \min_{0 \leq i \leq N} v(\alpha_i) - \min_{0 \leq i \leq N} v(\beta_i).
\] (8)

Next we observe that for any nonzero ideal \( \mathfrak{C} = (\gamma_1, \ldots, \gamma_n) \), we have

\[
\frac{1}{[K : \mathbb{Q}]} \log |\mathfrak{C}| = \sum_{v \in M^0_K} \min_{1 \leq i \leq n} v(\gamma_i).
\]

(The \( 1/[K : \mathbb{Q}] \) in front comes from the way that we have normalized the valuations in order to simplify the formula for the absolute height.) Hence when we sum (8) over all nonarchimedean places of \( K \), we obtain

\[
\sum_{v \in M^0_K} \lambda_\Delta((A, B), v) = \frac{1}{[K : \mathbb{Q}]} (\log N\mathfrak{D} - \log N\mathfrak{A} - \log N\mathfrak{B}).
\]

Substituting this into (7) yields the desired result. \( \square \)

We conclude this section with an elementary result saying that every point in \( \mathbb{P}^N(K) \) has integral homogeneous coordinates that are almost relatively prime.

**Lemma 7.** Let \( K/\mathbb{Q} \) be a number field and let \( R_K \) be the ring of integers of \( K \). There is an integral ideal \( \mathfrak{C} = \mathfrak{C}(K) \) so that every \( P \in \mathbb{P}^N(K) \) can be written using homogeneous coordinates

\[
P = [\alpha_0, \alpha_1, \ldots, \alpha_N]
\]

satisfying

\[
\alpha_0, \ldots, \alpha_N \in R_K \quad \text{and} \quad (\alpha_0, \ldots, \alpha_N) \mid \mathfrak{C}.
\]

**Proof.** Fix integral ideals \( \mathfrak{a}_1, \ldots, \mathfrak{a}_h \) that are representatives for the ideal class group of \( R_K \). Given a point \( P \in \mathbb{P}^N(K) \), choose any homogeneous coordinates \( P = [\beta_0, \ldots, \beta_N] \). Multiplying the coordinates by a constant, we may assume that \( \beta_0, \ldots, \beta_N \in R_K \). The ideal generated by \( \beta_0, \ldots, \beta_N \) differs by a principal ideal from one of the representative ideals, say

\[(\gamma)(\beta_0, \ldots, \beta_N) = \mathfrak{a}_j \quad \text{for some} \quad \gamma \in K^*.
\]

Then each \( \gamma \beta_i \in \mathfrak{a}_j \subset R_K \), so if we set \( \alpha_i = \gamma \beta_i \), then

\[
P = [\alpha_0, \ldots, \alpha_N] \quad \text{with} \quad \alpha_0, \ldots, \alpha_N \in R_K \quad \text{and} \quad (\alpha_0, \ldots, \alpha_N) = \mathfrak{a}_j.
\]

Hence if we let \( \mathfrak{C} \) be the integral ideal \( \mathfrak{C} = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_h \), then \( \mathfrak{C} \) depends only on \( K \), and for any point \( P \) we have shown how to find homogeneous
coordinates in \( R_K \) such that the ideal generated by the coordinates divides \( \mathcal{C} \).

\[ \square \]

3. An Ideal Characterization of Orbit Size

In this section we estimate the size of a certain ideal having the property that its prime divisors are the primes with \( m_p \leq m \).

**Proposition 8.** With notation as in Section 1 and Theorem 3, there are a constant \( C = C(K, V, \varphi) \) and a finite set of exceptional primes \( S = S(K, V, \varphi) \) so that for every \( m \geq 1 \) there exists a nonzero integral ideal \( \mathcal{D}(m) \) satisfying the following two conditions:

(i) For \( p \notin S \) we have \( m_p \leq m \) if and only if \( p \mid \mathcal{D}(m) \).

(ii) \( \log \log N_{\mathcal{D}(m)} \leq Cm \).

**Remark 9.** If \( V \) is projective and \( \varphi \) is finite of degree \( d \geq 2 \), then the following more precise version of (ii) holds:

\[ \log \log N_{\mathcal{D}(m)} \leq (\log d)m + C \log m. \]

**Proof.** By definition, \( m_p(\varphi, P) \) is the smallest value of \( m \) such that there exist \( r \geq 1 \) and \( s \geq 0 \) satisfying

\[ r + s = m \quad \text{and} \quad \varphi^{r+s}(P) \equiv \varphi^s(P) \pmod{p}. \]

Notice that \( s \) is the length of the tail and \( r \) is the length of the cycle in the orbit \( O_{\varphi_p}(\tilde{P} \pmod{p}) \).

We let \( \mathcal{C} \) be the ideal described in Lemma 7. Then for each \( n \geq 0 \) we can write

\[ \varphi^n(P) = [A_0(n), A_1(n), \ldots, A_N(n)] \]

with \( A_i(n) \in R_K \) and such that the ideal

\[ \mathfrak{A}(n) := (A_0(n), \ldots, A_N(n)) \]

divides the ideal \( \mathcal{C} \).

It follows that for all primes \( p \nmid \mathcal{C} \) we have

\[ \varphi^{r+s}(P) \equiv \varphi^s(P) \pmod{p} \]

\[ \iff A_i(r+s)A_j(s) \equiv A_i(s)A_j(r+s) \pmod{p} \]

for all \( 0 \leq i < j \leq N \).

Hence if we define ideals \( \mathfrak{B}(r, s) \) by

\[ \mathfrak{B}(r, s) = (A_i(r+s)A_j(s) - A_i(s)A_j(r+s))_{0 \leq i < j \leq N} \]

and define \( \mathcal{D}(m) \) to be the product

\[ \mathcal{D}(m) = \prod_{r \geq 1, s \geq 0 \atop r+s=m} \mathfrak{B}(r, s), \]
then for all primes $p \nmid C$ we have
\[ m_p(\varphi, P) \leq m \iff p \mid \mathfrak{D}(m). \]
Thus that $\mathfrak{D}(m)$ has property (i). Further, the assumption that $P$ has
infinite $\varphi$-orbit tells us that
\[ \varphi^{r+s}(P) \neq \varphi^s(P) \quad \text{for all } r \geq 1 \text{ and } s \geq 0, \]
so $\mathfrak{D}(m) \neq 0$.

It remains to estimate the norm of $\mathfrak{D}(m)$. We apply Proposition 6, which with our notation says that
\[ \frac{1}{[K : \mathbb{Q}]} \log \frac{\mathfrak{N}\mathfrak{B}(r, s)}{\mathfrak{N}\mathfrak{B}(r + s) \mathfrak{N}\mathfrak{A}(s)} \leq h(\varphi^{r+s}(P)) + h(\varphi^s(P)) + O(1). \]
Using the fact that $\mathfrak{N}\mathfrak{B}(r + s)$ and $\mathfrak{N}\mathfrak{A}(s)$ are smaller than $\mathfrak{N}\mathfrak{C}$, which only depends on $K$, we find that
\[ \frac{1}{[K : \mathbb{Q}]} \log \mathfrak{N}\mathfrak{B}(r, s) \leq h(\varphi^{r+s}(P)) + h(\varphi^s(P)) + O(1). \]
Next we apply Proposition 4 to estimate the heights, which gives
\[ \log \mathfrak{N}\mathfrak{B}(r, s) \leq Cd^{r+s}, \]
where $C = C(K, V, \varphi, P)$ and $d = d(V, \varphi) \geq 2$. The key point is that
neither $C$ nor $d$ depends on $r$ or $s$.

The ideal $\mathfrak{D}(m)$ is a product of various $\mathfrak{B}(r, s)$ ideals, so we obtain
\[ \log \mathfrak{N}\mathfrak{D}(m) = \sum_{r \geq 1, s \geq 0} \log \mathfrak{N}\mathfrak{B}(r, s) \leq \sum_{r \geq 1, s \geq 0} Cd^{r+s} \leq Cdm^{m+1} \leq Cd^m. \]
Taking one more logarithm yields
\[ \log \log \mathfrak{N}\mathfrak{D}(m) \ll m, \]
where the implied constant is independent of $m$. \hfill \Box

An immediate corollary of Proposition 8 is a weak lower bound for $m_p$.

**Corollary 10.** With notation as in Section 1, there is a constant $C = C(K, V, \varphi, P)$ so that
\[ m_p(\varphi, P) \geq C \log \log \mathfrak{N}p \quad \text{for all primes } p. \]

**Proof.** For each $m \geq 1$, let $\mathfrak{D}(m)$ be the nonzero the ideal described in
Proposition 8. Then for all but finitely many primes $p$ we have
\[ p \mid \mathfrak{D}(m_p) \quad \text{and} \quad \log \log \mathfrak{N}\mathfrak{D}(m_p) \leq Cm_p. \]
It follows that $N \mathfrak{D}(m_p) \geq N p$, which gives the desired result for $p$. Adjusting the constant to deal with the finitely many excluded primes completes the proof. \hfill \Box \\

4. AN ANALYTIC ESTIMATE

We now prove the key analytic estimate required for the proof of Theorem 3. This analytic result is a dynamical analog of a theorem of Romanoff [10], see also [2, 3, 7, 9]. The proof, especially insofar as we obtain an explicit dependence on $s$, follows the proof in [9].

**Theorem 11.** With notation as in Theorem 3, let $\lambda \geq 1$. Then there is a constant $C = C(K, V, \varphi, \lambda)$ so that

$$
\sum_{p \in \text{Spec} R_K} \frac{\log N p}{N p \cdot e^{sm_p^\lambda}} \leq \frac{C}{s^{1/\lambda}} \quad \text{for all } s > 0.
$$

(9)

**Proof.** To ease notation, define functions $g(t)$ and $G(t)$ by

$$
g(t) = \frac{\log t}{t} \quad \text{and} \quad G(t) = e^{-st^\lambda}.
$$

(10)

We use Abel summation to rewrite the series $S(\varphi, P, \lambda, s)$ in (9) as follows:

$$
S(\varphi, P, \lambda, s) = \sum_{p \in \text{Spec} R_K} \frac{\log N p}{N p \cdot e^{sm_p^\lambda}}
$$

$$
= \sum_{p \in \text{Spec} F_K} g(Np)G(m_p)
$$

$$
= \sum_{m \geq 1} \left( \sum_{p \in \text{Spec} R_K \atop m_p = m} g(Np)G(m) \right)
$$

$$
= \sum_{m \geq 1} G(m) \left( \sum_{p \in \text{Spec} R_K \atop m_p \leq m} g(Np) - \sum_{p \in \text{Spec} R_K \atop m_p \leq m-1} g(Np) \right)
$$

$$
= \sum_{m \geq 1} (G(m) - G(m + 1)) \sum_{p \in \text{Spec} R_K \atop m_p \leq m} g(Np). \quad (11)
$$

The mean value theorem gives

$$
G(m) - G(m + 1) \leq \sup_{m < \theta < m + 1} -G'(\theta) = \sup_{m < \theta < m + 1} s \lambda \theta^{\lambda - 1} e^{-s\theta^\lambda}
$$

$$
= s \lambda \mu^{\lambda - 1} e^{-sm^\lambda}.
$$
Substituting into (11) yields
\[ S(\varphi, \alpha, \lambda, s) \leq \sum_{m \geq 1} s \lambda m^{\lambda-1} e^{-s m^\lambda} \sum_{p \in \text{Spec } R_K \atop m_p \leq m} \frac{\log Np}{Np}. \] (12)

To deal with the inner sum, we use two results. The first, Proposition 8, was proven earlier. The second is as follows.

**Lemma 12.** Let \( K/\mathbb{Q} \) be a number field. There are constants \( c_1 \) and \( c_2 \), depending only on \( K \), so that for all integral ideals \( \mathfrak{D} \) we have
\[ \sum_{p \mid \mathfrak{D}} \frac{\log Np}{Np} \leq c_1 \log \log N\mathfrak{D} + c_2. \]

**Proof.** This is a standard result. See for example [9, Corollary 2.3] for a derivation and an explicit value for \( c_1 \). \( \square \)

Using the two lemmas, we obtain the bound
\[ S(\varphi, \alpha, \lambda, s) \]
\[ \leq \sum_{m \geq 1} s \lambda m^{\lambda-1} e^{-s m^\lambda} \sum_{p \in \text{Spec } R_K \atop m_p \leq m} \frac{\log Np}{Np} \text{ from (12)}, \]
\[ = \sum_{m \geq 1} s \lambda m^{\lambda-1} e^{-s m^\lambda} \sum_{p \in \text{Spec } R_K \atop p \mid \mathfrak{D}(m)} \frac{\log Np}{Np} \text{ from Proposition 8(i)}, \]
\[ \leq \sum_{m \geq 1} s \lambda m^{\lambda-1} e^{-s m^\lambda} \left( c_1 \log \log N\mathfrak{D}(m) + c_2 \right) \text{ from Lemma 12} \]
\[ \leq Cs\lambda \sum_{m \geq 1} m^\lambda e^{-s m^\lambda} \text{ from Proposition 8(ii)}. \]

It remains to deal with this last series. If \( \lambda = 1 \), then we can explicitly evaluate the series, but this is not possible for general values of \( \lambda \). (For example, if \( \lambda = 2 \), then it is more-or-less a theta function). Instead we use the following elementary estimate.

**Lemma 13.** Fix \( \lambda > 0 \) and \( \mu \geq 0 \). There is a constant \( C = C(\lambda, \mu) \) so that
\[ \sum_{m=1}^{\infty} m^\mu e^{-s m^\lambda} \leq Cs^{-(\mu+1)/\lambda} \text{ for all } s > 0. \]

**Proof.** We estimate
\[ \sum_{m=1}^{\infty} m^\mu e^{-s m^\lambda} \leq \int_0^{\infty} t^\mu e^{-st^\lambda} dt \]
\[ = s^{-(\mu+1)/\lambda} \int_0^\infty u^{\mu} e^{-u^\lambda} \, dt \text{ letting } u = s^{1/\lambda} t. \]

The integral converges and is independent of \( s \). \( \square \)

Applying Lemma 13 with \( \mu = \lambda \) and substituting in above yields
\[ S(\varphi, \alpha, \lambda, s) \leq C_1(K, V, \varphi) s \lambda \cdot C_2(\lambda) s^{-(\lambda+1)/\lambda} = C_3(K, V, \varphi, \lambda) s^{-1/\lambda}. \]
This is the desired result. \( \square \)

5. Proof of Theorem 3

We now use the analytic estimate provided by Theorem 11 to prove our main density results.

**Proof of Theorem 3.** (a) For any \( 0 < \gamma < 1 \) we let
\[ P_\gamma = \{ p \in \text{Spec}(R_K) : m_p \leq (\log N_p)^\gamma \}. \]

Then for all \( s > 0 \) we have
\[ \frac{C_s}{s^\gamma} \geq \sum_{p \in \text{Spec} R_K} \frac{\log N_p}{N_p \cdot e^{s m_p^\lambda}} \text{ from Theorem 11 with } \lambda = 1/\gamma, \]
\[ \geq \sum_{p \in P_\gamma} \frac{\log N_p}{N_p \cdot e^{s \log N_p}} \text{ by the definition of } P_\gamma, \]
\[ = \sum_{p \in P_\gamma} \frac{\log N_p}{(N_p)^{1+s}}. \tag{13} \]

Hence
\[ \overline{\delta}(P_\gamma) = \limsup_{s \to 1^+} (s - 1) \sum_{p \in P_\gamma} \frac{\log N_p}{(N_p)^s} \text{ by definition of upper density}, \]
\[ = \limsup_{s \to 0^+} s \sum_{p \in P_\gamma} \frac{\log N_p}{(N_p)^{s+1}} \text{ replacing } s \text{ by } s + 1, \]
\[ \leq \limsup_{s \to 0^+} C s^{1-\gamma} \text{ from (13)}, \]
\[ = 0 \text{ since } \gamma < 1. \]

Since the density is always nonnegative, this proves that \( \delta(P_\gamma) = 0 \). This is equivalent to Theorem 3 (a), which asserts that the complement of \( P_\gamma \) has density 1.

(b) The proof is similar. Let \( \epsilon > 0 \) and define
\[ P_\epsilon = \{ p \in \text{Spec}(R_K) : m_p \leq \epsilon \log N_p \}. \]
Applying Theorem 11 with $\lambda = 1$ and using the definition of $P_\epsilon$, we estimate
\[ \frac{C}{s} \geq \sum_{p \in \text{Spec } R_K} \frac{\log N_p}{N_p \cdot e^{s m_p}} \geq \sum_{p \in P_\epsilon} \frac{\log N_p}{N_p \cdot e^{s m_p}} \geq \sum_{p \in P_\epsilon} \frac{\log N_p}{N_p \cdot e^{s \epsilon \log N_p}} = \sum_{p \in P_\epsilon} \frac{\log N_p}{(N_p)^{1+s \epsilon}}. \]
Replacing $s$ by $s/\epsilon$ yields
\[ \frac{C \epsilon}{s} \geq \sum_{p \in P_\epsilon} \frac{\log N_p}{(N_p)^{1+s}}. \]
Hence
\[ \delta(P_\epsilon) = \limsup_{s \to 0^+} s \sum_{p \in P_\epsilon} \frac{\log N_p}{(N_p)^{s+1}} \leq C \epsilon. \]
It follows that the complement of $P_\epsilon$ has lower density at least $1 - C \epsilon$. □

6. CONJECTURES AND EXPERIMENTS

The density estimate provided by Theorem 3 is probably far from the truth. If the $\varphi$-orbit of a point $P$ in $V(\mathbb{F}_p)$ is truly a “random map” from $V(\mathbb{F}_p)$ to itself, then the expected orbit length $m_p$ should be on the order of $\sqrt{\#V(\mathbb{F}_p)} \approx N_p^{\frac{1}{2} \dim V}$. (See [4, 5] for statistical properties of orbits of random maps and [1] for the analysis of orbits of certain polynomial maps.) Thus we might expect the quantity
\[ \frac{1}{\log X} \sum_{N_p \leq X} \frac{\log N_p}{m_p^{2 / \dim V}} \tag{14} \]
to be bounded as $X \to \infty$. (Note that $\frac{1}{\log X} \sum_{N_p \leq X} \frac{\log N_p}{N_p} \to 1$.)

We tested this guess numerically for the case of quadratic polynomial maps on $\mathbb{P}_Q^1$ by computing the value of (14) for various polynomials $\varphi(z) = z^2 + c$ and using values of $X$ encompassing every 200th rational prime up to 20000. The results are listed in Table 1.

The data in Table 1 is ambiguous; all five columns are increasing, but it is not clear whether they are approaching a finite bound. We extended the calculations for $z^2 + 1$ up to $X = 50000$, and the value of the sum (14) continues to grow as shown in Table 2. This suggests that $m_p$ grows somewhat slower than $\sqrt{N_p}$.

Emboldened by these few experiments, we are led to make the following plausible conjecture.
Conjecture 14. Let $K/\mathbb{Q}$ be a number field, let $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$, and let $P \in \mathbb{P}^N(K)$ be a point with infinite $\varphi$-orbit. Then for every $\epsilon > 0$ the set

$$ \{ p : m_p(\varphi, P) \geq Np^{\frac{N}{2} - \epsilon} \} $$

is a set of density 1.

It is reasonable to pose a stronger question. Is there some $\kappa > 0$ so that the conjecture is true for the set of $p$ satisfying

$$ m_p \geq Np^{\frac{N}{2}} (\log Np)^{-\kappa}? $$

And in the other direction, we ask whether for some constant $C > 0$, the set of $p$ satisfying $m_p \geq CNp^{N/2}$ is a set of density 0.

References

[1] E. Bach. Toward a theory of Pollard’s rho method. Inform. and Comput., 90(2):139–155, 1991.
[2] P. Erdös and P. Turan. Ein zahlentheoretischer Satz. Bull. de l’institut de Math. et Méc. a l’université Konybycheff de Tomsk, I:101–103, 1935.
[3] P. Erdös and P. Turan. Über die vereinfachung eines Landauschen Satzes. Bull. de l’institut de Math. et Méc. a l’université Konybycheff de Tomsk, I:144–147, 1935.
[4] P. Flajolet and A. M. Odlyzko. Random mapping statistics. In Advances in cryptology—EUROCRYPT ’89 (Houthalen, 1989), volume 434 of Lecture Notes in Comput. Sci., pages 329–354. Springer, Berlin, 1990.

[5] B. Harris. Probability distributions related to random mappings. Ann. Math. Statist., 31:1045–1062, 1960.

[6] M. Hindry and J. H. Silverman. Diophantine geometry, volume 201 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2000. An introduction.

[7] E. Landau. Verschärfung eines Romanoffschen Satzes. Acta Arith., 1:43–62, 1935.

[8] S. Lang. Fundamentals of Diophantine Geometry. Springer-Verlag, New York, 1983.

[9] M. R. Murty, M. Rosen, and J. H. Silverman. Variations on a theme of Romanoff. Internat. J. Math., 7(3):373–391, 1996.

[10] N. P. Romanoff. Über einige Sätze der additiven Zahlentheorie. Math. Ann., 109(1):668–678, 1934.

[11] J. H. Silverman. Arithmetic distance functions and height functions in Diophantine geometry. Math. Ann., 279(2):193–216, 1987.

E-mail address: jhs@math.brown.edu

MATHEMATICS DEPARTMENT, BOX 1917 BROWN UNIVERSITY, PROVIDENCE, RI 02912 USA