New York Journal of Mathematics

New York J. Math. **14** (2008) 601–616.

Variation of periods modulo p in arithmetic dynamics

Joseph H. Silverman

Abstract. Let $\varphi : V \to V$ 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 φ. For each prime $\mathfrak{p}$ of good reduction, let $m_{\mathfrak{p}}(\varphi, P)$ be the size of the φ-orbit of the reduction of P modulo $\mathfrak{p}$. Fix any $\epsilon > 0$. We show that for almost all primes $\mathfrak{p}$ in the sense of analytic density, the orbit size $m_{\mathfrak{p}}(\varphi, P)$ is larger than $(\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p})^{1-\epsilon}$.

Contents

Introduction

Let

$$\varphi : \mathbb{P}^N_{\mathbb{Q}} \longrightarrow \mathbb{P}^N_{\mathbb{Q}}$$

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

$$\mathcal{O}_\varphi(P) = \{P, \varphi(P), \varphi^2(P), \dots\}.$$

Received June 19, 2008.

Mathematics Subject Classification. Primary: 11G35; Secondary: 11B37, 14G40, 37F10.

Key words and phrases. Arithmetic dynamical systems, orbit modulo p.

The author's research supported by NSF grant DMS-0650017.

ISSN 1076-9803/08

For all but finitely many primes p, we can reduce φ to obtain a morphism

$$\widetilde{\varphi}_p : \mathbb{P}^N_{\mathbb{F}_p} \longrightarrow \mathbb{P}^N_{\mathbb{F}_p}$$

whose degree is still d. We write $m_p(\varphi, P)$ for the size of the orbit of the reduced point $\widetilde{P} = P \bmod p$,

$$m_p(\varphi, P) = \#\mathcal{O}_{\widetilde{\varphi}_p}(\widetilde{P}).$$

(For the remaining primes we define $m_p(\varphi, P)$ to be ∞.)

Using an elementary height argument (see Corollary 12), one can show that

$$m_p(\varphi, P) \ge C_d \log\log p + O(1) \quad \text{for all } p,$$

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 $\boldsymbol{\delta}(\mathcal{P})$ for the logarithmic analytic density of a set of primes $\mathcal{P}$. (See Section 1 for the precise definition of $\boldsymbol{\delta}$ and the associated lower density $\underline{\boldsymbol{\delta}}$.)

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

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

$$\boldsymbol{\delta}\bigl\{p : m_p(\varphi, P) \ge (\log p)^\gamma\bigr\} = 1.$$

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

$$\underline{\boldsymbol{\delta}}\bigl\{p : m_p(\varphi, P) \ge \epsilon \log p\bigr\} \ge 1 - C\epsilon.$$

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 2 for the precise statement of our main result.

The proof of Theorem 1, and its generalization Theorem 2, 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

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

This is done using a height estimate for rational maps (Proposition 4) and a height estimate for arithmetic distances (Proposition 7). The second part of the proof uses the first part to prove an analytic estimate (Theorem 13) of the following form: for all $\lambda \ge 1$ there is a constant $C = C(\varphi, \lambda)$ so that

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

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 φ 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 present the results of some experiments using quadratic polynomials $\varphi_c(z) = z^2 + c$ which suggest that $m_p(\varphi_c, \alpha)$ is almost always larger than $\sqrt{p}^{1-\epsilon}$, and for $c \notin \{0, \frac{1}{2}\}$, it is seldom larger than $\sqrt{p}^{1+\epsilon}$.

Acknowledgements. The author would like the thank the referee for his careful reading of this paper and for suggesting a simplified proof of Proposition 7.

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. 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.

Definition. Let $\mathcal{V}/R_K$ be a scheme whose generic fiber is V/K and let Φ be a rational map $\Phi : \mathcal{V}/R_K \dashrightarrow \mathcal{V}/R_K$ whose restriction to the generic fiber is $\varphi : V/K \to V/K$. We say that φ has *good reduction at a prime* $\mathfrak{p}$ if the rational map

$$\Phi : \mathcal{V} \times_{R_K} R_\mathfrak{p} \dashrightarrow \mathcal{V} \times_{R_K} R_\mathfrak{p}$$

over the local ring $R_\mathfrak{p}$ extends to a morphism; cf. [12, §2.5]. If this is the case, then we define the reduction of φ modulo $\mathfrak{p}$ to be the restriction of Φ to the special fiber over $\mathfrak{p}$,

$$\Phi|_\mathfrak{p} = \widetilde{\varphi} : \widetilde{V}/\mathbb{F}_\mathfrak{p} \longrightarrow \widetilde{V}/\mathbb{F}_\mathfrak{p}.$$

We note that reduction modulo $\mathfrak{p}$ commutes with φ in its action on points, i.e.,

$$\widetilde{\varphi(P)} = \widetilde{\varphi}(\widetilde{P}).$$

We observe that different choices of model $\Phi : \mathcal{V} \dashrightarrow \mathcal{V}$ affect only finitely many of the reduced maps $\Phi|_\mathfrak{p}$, and thus have no effect on the density results proven in this paper. We will assume henceforth, without further comment, that a particular model has been fixed.

Definition. With $K/\mathbb{Q}$ and $\varphi : V \to V$ as above, let $P \in V(K)$ be a point whose forward φ-orbit

$$\mathcal{O}_\varphi(P) = \bigl\{P, \varphi(P), \varphi^2(P), \dots\bigr\}$$

is infinite. For each prime ideal $\mathfrak{p}$ of K at which φ has good reduction, we let

$$m_\mathfrak{p} = m_\mathfrak{p}(\varphi, P) = \text{size of the } \widetilde{\varphi}\text{-orbit of } \widetilde{P} \text{ in } \widetilde{V}(\mathbb{F}_\mathfrak{p}).$$

If φ has bad reduction at $\mathfrak{p}$, we set $m_\mathfrak{p} = \infty$. As noted above, the choice of a model for $\varphi : V \to V$ affects only finitely many of the $m_\mathfrak{p}(\varphi, P)$ values.

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 $(0) \notin \mathcal{P} \subset \operatorname{Spec}(R_K)$, define the partial ζ-function for $\mathcal{P}$ by

$$\zeta_K(\mathcal{P}, s) = \prod_{\mathfrak{p}\in\mathcal{P}} \left(1 - \frac{1}{\mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}^s}\right)^{-1}.$$

This Euler product defines an analytic function on $\operatorname{Re}(s) > 1$. As usual, we write $\zeta_K(s)$ for the ζ-function of the field K. Then the (*logarithmic analytic*) *density* of $\mathcal{P}$ is given by the following limit, assuming that the limit exists:

$$\boldsymbol{\delta}(\mathcal{P}) = \lim_{s\to 1^+} \frac{d\log\zeta_K(\mathcal{P}, s)}{d\log\zeta_K(s)} = \lim_{s\to 1^+} \frac{\zeta_K'(\mathcal{P}, s)/\zeta_K(\mathcal{P}, s)}{\zeta_K'(s)/\zeta_K(s)}. \tag{2}$$

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

$$\boldsymbol{\delta}(\mathcal{P}) = \lim_{s\to 1^+} (s-1) \sum_{\mathfrak{p}\in\mathcal{P}} \frac{\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}}{\mathsf{N}_{K/\mathbb{Q}}\mathfrak{p}^s}. \tag{3}$$

We similarly define upper and lower densities $\overline{\boldsymbol{\delta}}(\mathcal{P})$ and $\underline{\boldsymbol{\delta}}(\mathcal{P})$ by replacing the limits in (2) with the limsup or the liminf, respectively; and then (3) is true with the appropriate limsup or liminf.

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

Theorem 2. *Let $K/\mathbb{Q}$ be a number field, let $\varphi : V/K \to V/K$, and let $P \in V(K)$ be as described in this section. Further, let $m_\mathfrak{p}(\varphi, P)$ denote the size of the $\widetilde{\varphi}$-orbit of $\widetilde{P}$ in $\widetilde{V}(\mathbb{F}_\mathfrak{p})$.*

(a) *For all $\gamma < 1$ we have*

$$\boldsymbol{\delta}\bigl\{\mathfrak{p} \in \operatorname{Spec} R_K : m_p(\varphi, P) \ge (\log \mathsf{N}\mathfrak{p})^\gamma\bigr\} = 1.$$

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

$$\underline{\boldsymbol{\delta}}\bigl\{\mathfrak{p} \in \operatorname{Spec} R_K : m_p(\varphi, P) \ge \epsilon \log \mathsf{N}\mathfrak{p}\bigr\} \ge 1 - C\epsilon.$$

Remark 3. Our results apply more generally to a map $\varphi : V \dashrightarrow V$, i.e., not necessarily a morphism, provided that we start with a point $P \in V(K)$ such that φ is well-defined at every point in the forward orbit of P. We need merely note that inequality (4) in Proposition 4 is valid away from the locus of indeterminacy of φ, so under our assumption, it may be applied to every point in $\mathcal{O}_\varphi(P)$. The rest of the proof remains unchanged. However, we feel that this situation is of somewhat less interest, since in general it is difficult to determine when the full orbit of a point $P \in V$ completely avoids hitting the indeterminacy locus of a rational map $\varphi : V \dashrightarrow V$.

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 $\mathsf{N}\mathfrak{a}$ for the $K/\mathbb{Q}$ norm of a fractional ideal $\mathfrak{a}$ of K.

We also fix a projective embedding of $V/K \subset \mathbb{P}^N$, and we use this to fix a height function

$$h : V(\overline{K}) \longrightarrow \mathbb{R}$$

on V as the restriction of the classical Weil height function on $\mathbb{P}^N(\overline{K})$. See, e.g., [6, Part B], [8, Chapter 3], or [12, §§3.1,3.2,7.3] for the theory of height functions.

Proposition 4. *With notation as in Section 1 and Theorem 2, there are constants*

$$d = d(V,\varphi) \ge 2 \quad \textit{and} \quad C = C(V,\varphi) \ge 0$$

so that

$$h\bigl(\varphi^n(Q)\bigr) \le d^n\bigl(h(Q)+C\bigr) \quad \textit{for all } n \ge 0 \textit{ and all } Q \in V(\overline{K}).$$

Proof. We are given that φ 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 $V_1,\dots,V_t$ such that on each V_i we can write

$$\varphi_i = \varphi|_{V_i} = [F_{i0}, F_{i1}, \dots, F_{iN}],$$

where the F_{ij} are homogeneous polynomials and such that

$$F_{i0}, F_{i1}, \dots, F_{iN} \quad \text{do not simultaneously vanish on } V_i.$$

We may view φ_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 φ_i, we have the elementary height estimate

$$h\bigl(\varphi_i(Q)\bigr) \le d_i h(Q) + C(\varphi_i), \quad \text{valid for all } Q \in \mathbb{P}^N(\overline{K}) \smallsetminus Z_i. \tag{4}$$

(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

$$\begin{aligned} h\bigl(\varphi(Q)\bigr) &= h\bigl(\varphi_i(Q)\bigr) && \text{for any } i \text{ with } Q \notin Z_i,\\ &\le \max_{i \text{ with } Q \notin Z_i} d_i h(Q) + C(\varphi_i) && \text{from (4)},\\ &\le \max_{1\le i\le n} d_i h(Q) + \max_{1\le i \le n} C(\varphi_i). \end{aligned}$$

Setting

$$d = \max\{2, d_1, \dots, d_t\} \quad \text{and} \quad C = \max\bigl\{C(\varphi_1), \dots, C(\varphi_t)\bigr\},$$

we have

$$h\bigl(\varphi(Q)\bigr) \le dh(Q) + C \quad \text{for all } Q \in V(\overline{K}).$$

Applying this iteratively yields

$$h\bigl(\varphi^n(Q)\bigr) \le d^n h(Q) + (1 + d + \cdots + d^{n-1})C \le d^n\bigl(h(Q) + C\bigr), \tag{5}$$

(note that $d \ge 2$ by assumption) which is the desired result. □

Remark 5. If $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ is a finite morphism of degree at least 2, then in the statement of Proposition 4 we can take $d = \deg\varphi$. More precisely, in this situation a standard property of height functions [6, B.2.5(b)] gives upper and lower bounds,

$$h\bigl(\varphi^n(Q)\bigr) = d^n\bigl(h(Q) + O(1)\bigr).$$

Remark 6. For maps of degree 1 on $\mathbb{P}^N$, the middle inequality in (5) yields the stronger estimate

$$h\bigl(\varphi^n(Q)\bigr) \le h(Q) + Cn.$$

Tracing through the proofs in this paper, this would give an exponential improvement in our results, and more generally, we get an exponential improvement for any $\varphi : V \to V$ satisfying $h\bigl(\varphi(Q)\bigr) \le h(Q) + O(1)$.

We illustrate with an example. Let $\varphi(z) = az$ with $a \in \mathbb{Q}^*$, so $m_p(\varphi, 1)$ is the order of a in the multiplicative group $\mathbb{F}_p^*$. Then in place of (1) we obtain

$$\sum_{p \text{ prime}} \frac{\log p}{p m_p(\varphi, 1)^s} \le \frac{2}{s} + O(1), \tag{6}$$

which allows us to replace Theorem 1(b) with

$$\underline{\boldsymbol{\delta}}\bigl\{p : m_p(\varphi, 1) \ge p^\epsilon\bigr\} \ge 1 - 2\epsilon. \tag{7}$$

The estimates (6) and (7) are special cases of results proven in [9]; see in particular [9, equation (3)] and the remark following [9, Theorem 4.2].

Proposition 7. *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 α_i and at least one β_i nonzero. Define fractional ideals

$$\mathfrak{A} = (\alpha_0, \ldots, \alpha_N), \quad \mathfrak{B} = (\beta_0, \ldots, \beta_N), \quad \mathfrak{D} = (\alpha_i\beta_j - \alpha_j\beta_i)_{0 \le i < j \le N}.$$

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 $A \ne B$. Then

$$\frac{1}{[K : \mathbb{Q}]} \log\left(\frac{\mathsf{N}\mathfrak{D}}{\mathsf{N}\mathfrak{A} \cdot \mathsf{N}\mathfrak{B}}\right) \le h(A) + h(B) + \log 2.$$

(*Here h is the absolute logarithmic height on $\mathbb{P}^N(\overline{\mathbb{Q}})$; see* [6, Part B], [8, Chapter 3], *or* [12, §§3.1,3.2,7.3].)

Proof. We let M_K be a set of absolute values on K normalized so as to obtain the absolute height, i.e., the height of a point $P = [x_0, \dots, x_N]$ is given by $h(P) = \sum_{v \in M_K} - \min_i\{v(x_i)\}$. We write M_K^∞ (respectively M_K^0) for the set of archimedean (respectively nonarchimedean) absolute values on K. We observe that with this normalization, the norm of a nonzero ideal $\mathfrak{C} = (\gamma_1, \dots, \gamma_n)$ is given by

$$\frac{1}{[K:\mathbb{Q}]} \log \mathsf{N}\mathfrak{C} = \sum_{v \in M_K^0} \min_{1 \le i \le n} v(\gamma_i).$$

Since $A \ne B$, there are indices i and j such that $\alpha_i \beta_j \ne \alpha_j \beta_i$. Relabeling the coordinates, we may assume without loss of generality that $\alpha_0\beta_1 \ne \alpha_1\beta_0$. We observe that for all $v \in M_K^\infty$ we have

$$\begin{aligned} (8) \qquad v(\alpha_0\beta_1 - \alpha_1\beta_0) &\ge \min\bigl\{v(\alpha_0\beta_1), v(\alpha_1\beta_0)\bigr\} + v(2) \\ &\ge \min\bigl\{v(\alpha_0), v(\alpha_1)\bigr\} + \min\bigl\{v(\beta_0), v(\beta_1)\bigr\} + v(2) \\ &\ge \min_{0 \le i \le N}\bigl\{v(\alpha_i)\bigr\} + \min_{0 \le i \le N}\bigl\{v(\beta_i)\bigr\} + v(2). \end{aligned}$$

We use this to compute

$$\begin{aligned} &\frac{1}{[K:\mathbb{Q}]} \log\left(\frac{\mathsf{N}\mathfrak{D}}{\mathsf{N}\mathfrak{A} \cdot \mathsf{N}\mathfrak{B}}\right) \\ &\qquad = \sum_{v \in M_K^0} \Bigl(\min_{0 \le i < j \le N} v(\alpha_i\beta_j - \alpha_j\beta_i) - \min_{0 \le i \le N} v(\alpha_i) - \min_{0 \le i \le N} v(\beta_i)\Bigr) \\ &\qquad \le \sum_{v \in M_K^0} \Bigl(v(\alpha_0\beta_1 - \alpha_1\beta_0) - \min_{0 \le i \le N} v(\alpha_i) - \min_{0 \le i \le N} v(\beta_i)\Bigr) \\ &\qquad = \sum_{v \in M_K} \Bigl(v(\alpha_0\beta_1 - \alpha_1\beta_0) - \min_{0 \le i \le N} v(\alpha_i) - \min_{0 \le i \le N} v(\beta_i)\Bigr) \\ &\qquad\qquad - \sum_{v \in M_K^\infty} \Bigl(v(\alpha_0\beta_1 - \alpha_1\beta_0) - \min_{0 \le i \le N} v(\alpha_i) - \min_{0 \le i \le N} v(\beta_i)\Bigr) \\ &\qquad \le \sum_{v \in M_K} \Bigl(v(\alpha_0\beta_1 - \alpha_1\beta_0) - \min_{0 \le i \le N} v(\alpha_i) - \min_{0 \le i \le N} v(\beta_i)\Bigr) \\ &\qquad\qquad - \sum_{v \in M_K^\infty} v(2) \qquad \text{from (8)}, \\ &\qquad = 0 + h(A) + h(B) + \log 2 \qquad \text{from the product formula.} \end{aligned}$$

This completes the proof of Proposition 7. □

Remark 8. The proof of Proposition 7 is elementary, but it may be illuminating to rephrase the argument using the theory of local heights relative to closed subschemes and arithmetic distance functions as developed in [11]. We briefly sketch. Since $A \ne B$, relabeling lets us assume that $\alpha_0\beta_1 \ne \alpha_1\beta_0$.

We define

$$D = \{x_0y_1 = x_1y_0\} \qquad \text{and} \qquad \Delta = \{x_iy_j = x_jy_i \text{ for all } i \text{ and } j\}.$$

Thus Δ 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 π_1 and π_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

$$\text{(9)} \qquad \lambda_\Delta(P,v) \le \lambda_D(P,v) + O_v(1) \quad \text{for all } P \in \bigl((\mathbb{P}^N \times \mathbb{P}^N) \smallsetminus |D|\bigr)(K),$$

where λ_Δ and λ_D are local height functions; see [11]. Here $O_v(1)$ denotes an M_K-bounded function in the sense of Lang [8]. By construction, the point (A,B) is not in the support of D. We also note that since D is an effective divisor, the local height λ_D is bounded below by an M_K-constant for all P not in the support of D. Hence evaluating (9) at $P = (A,B)$ and summing over $v \in M_K^0$ yields

$$\text{(10)} \qquad \begin{aligned} \sum_{v \in M_K^0} \lambda_\Delta\bigl((A,B),v\bigr) &\le \sum_{v \in M_K^0} \Bigl(\lambda_D\bigl((A,B),v\bigr) + O_v(1)\Bigr) \\ &\le \sum_{v \in M_K} \lambda_D\bigl((A,B),v\bigr) + O(1) \\ &= h_D\bigl((A,B)\bigr) + O(1) \\ &= h_{\pi_1^*H+\pi_2^*H}\bigl((A,B)\bigr) + O(1) \\ &= h(A) + h(B) + O(1). \end{aligned}$$

It remains to compute λ_Δ, which in the parlance of [11] is an arithmetic distance function. From [11], and using the generators of the ideal defining Δ, a representative local height function for Δ is

$$\lambda_\Delta\bigl((A,B),v\bigr) = \min_{0 \le i < j \le N} v(\alpha_i\beta_j - \alpha_j\beta_i) - \min_{0 \le i \le N} v(\alpha_i) - \min_{0 \le i \le N} v(\beta_i).$$

Summing over M_K^0 gives

$$\sum_{v \in M_K^0} \lambda_\Delta\bigl((A,B),v\bigr) = \frac{1}{[K:\mathbb{Q}]}(\log \mathsf{N}\mathfrak{D} - \log \mathsf{N}\mathfrak{A} - \log \mathsf{N}\mathfrak{B}),$$

and substituting this into (10) yields the desired result (with $\log 2$ replaced by a constant that might depend on N).

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 9. *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

$$\alpha_0,\dots,\alpha_N \in R_K \qquad \textit{and} \qquad (\alpha_0,\dots,\alpha_N) \bigm| \mathfrak{C}.$$

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

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

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

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

Hence if we let $\mathfrak{C}$ be the integral ideal $\mathfrak{C} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_h$, 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 $\mathfrak{C}$. □

3. An ideal characterization of orbit size

In this section we estimate the size of the product of all prime ideals satisfying $m_{\mathfrak{p}} \le m$.

Proposition 10. *With notation as in Section 1 and Theorem 2, for any integer $m \ge 1$, let $\mathfrak{D}(m) = \mathfrak{D}(m; K, V, \varphi, P)$ be the integral ideal defined by*

$$\mathfrak{D}(m) = \prod_{\substack{\text{prime } \mathfrak{p}\\ m_{\mathfrak{p}} \le m}} \mathfrak{p}. \tag{11}$$

Then there is a constant $C = C(K, V, \varphi, P)$ such that for all $m \ge 1$,

$$\log\log \mathsf{N}\mathfrak{D}(m) \le Cm. \tag{12}$$

Remark 11. If V is projective and φ is finite of degree $d \ge 2$, then the following more precise version holds:

$$\log\log \mathsf{N}\mathfrak{D}(m) \le (\log d)m + C\log m.$$

Proof. By definition, for primes of good reduction, $m_{\mathfrak{p}}(\varphi, P)$ is the smallest value of m such that there exist $r \ge 1$ and $s \ge 0$ satisfying

$$r + s = m \qquad \text{and} \qquad \varphi^{r+s}(P) \equiv \varphi^s(P) \pmod{\mathfrak{p}}.$$

Notice that s is the length of the tail and r is the length of the cycle in the orbit $\mathcal{O}_{\widetilde{\varphi}_{\mathfrak{p}}}(\widetilde{P} \bmod \mathfrak{p})$.

We let $\mathfrak{C}$ be the ideal described in Lemma 9. Then for each $n \ge 0$ we can write

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

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

$$\mathfrak{A}(n) := \bigl(A_0(n),\dots,A_N(n)\bigr) \quad \text{divides the ideal } \mathfrak{C}.$$

It follows that for all primes of good reduction $\mathfrak{p} \nmid \mathfrak{C}$ we have

$$\begin{aligned}\varphi^{r+s}(P) \equiv \varphi^s(P) \pmod{\mathfrak{p}} \\ \iff \quad A_i(r+s)A_j(s) \equiv A_i(s)A_j(r+s) \pmod{\mathfrak{p}} \\ \text{for all } 0 \le i < j \le N.\end{aligned}$$

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

$$\mathfrak{B}(r,s) = \bigl(A_i(r+s)A_j(s) - A_i(s)A_j(r+s)\bigr)_{0 \le i < j \le N}$$

and define $\mathfrak{D}'(m)$ to be the product

$$\mathfrak{D}'(m) = \prod_{\substack{r \ge 1,\, s \ge 0 \\ r+s=m}} \mathfrak{B}(r,s),$$

then for all primes $\mathfrak{p} \nmid \mathfrak{C}$ we have

$$m_{\mathfrak{p}}(\varphi, P) \le m \quad \iff \quad \mathfrak{p} \mid \mathfrak{D}'(m).$$

Thus $\mathfrak{D}(m)$ and $\mathfrak{D}'(m)$ agree up to finitely many prime factors. More precisely, $\mathfrak{D}(m) \mid \mathfrak{C}\mathfrak{D}'(m)$, where $\mathfrak{C}$ is independent of m, so it suffices to prove (12) with $\mathfrak{D}'(m)$ in place of $\mathfrak{D}(m)$. We also note that the assumption that P has infinite φ-orbit tells us that

$$\varphi^{r+s}(P) \ne \varphi^s(P) \quad \text{for all } r \ge 1 \text{ and } s \ge 0,$$

so $\mathfrak{D}'(m) \ne 0$.

It remains to estimate the norm of $\mathfrak{D}'(m)$. We apply Proposition 7, which with our notation says that

$$\frac{1}{[K:\mathbb{Q}]} \log \frac{\mathsf{N}\mathfrak{B}(r,s)}{\mathsf{N}\mathfrak{A}(r+s)\mathsf{N}\mathfrak{A}(s)} \le h\bigl(\varphi^{r+s}(P)\bigr) + h\bigl(\varphi^s(P)\bigr) + O(1).$$

Using the fact that $\mathsf{N}\mathfrak{A}(r+s)$ and $\mathsf{N}\mathfrak{A}(s)$ are smaller than $\mathsf{N}\mathfrak{C}$, which only depends on K, we find that

$$\frac{1}{[K:\mathbb{Q}]} \log \mathsf{N}\mathfrak{B}(r,s) \le h\bigl(\varphi^{r+s}(P)\bigr) + h\bigl(\varphi^s(P)\bigr) + O(1).$$

Next we apply Proposition 4 to estimate the heights, which gives

$$\log \mathsf{N}\mathfrak{B}(r,s) \le Cd^{r+s},$$

where $C = C(K,V,\varphi,P)$ and $d = d(V,\varphi) \ge 2$. 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

$$\log \mathsf{N}\mathfrak{D}'(m) = \sum_{\substack{r \ge 1, s \ge 0 \\ r+s=m}} \log \mathsf{N}\mathfrak{B}(r,s) \le \sum_{\substack{r \ge 1, s \ge 0 \\ r+s=m}} Cd^{r+s} \le Cmd^{m+1} \le Cd^{2m}.$$

Taking one more logarithm yields

$$\log\log \mathsf{N}\mathfrak{D}'(m) \ll m,$$

where the implied constant is independent of m. □

An immediate corollary of Proposition 10 is a weak lower bound for $m_{\mathfrak{p}}$.

Corollary 12. *With notation as in Section 1, there is a constant $C = C(K,V,\varphi,P)$ so that*

$$m_{\mathfrak{p}}(\varphi,P) \ge C \log\log \mathsf{N}\mathfrak{p} \quad \text{for all primes } \mathfrak{p}.$$

Proof. For each $m \ge 1$, let $\mathfrak{D}(m)$ be the ideal (11) defined in Proposition 10. Then for all primes $\mathfrak{p}$ with $m_{\mathfrak{p}} < \infty$ we have

$$\mathfrak{p} \mid \mathfrak{D}(m_{\mathfrak{p}}) \qquad \text{and} \qquad \log\log \mathsf{N}\mathfrak{D}(m_{\mathfrak{p}}) \le C m_{\mathfrak{p}}.$$

The divisibility implies that $\mathsf{N}\mathfrak{D}(m_{\mathfrak{p}}) \ge \mathsf{N}\mathfrak{p}$, which gives the desired result. □

4. An analytic estimate

We now prove the key analytic estimate required for the proof of Theorem 2. This analytic result is a dynamical analog of a theorem of Romanoff [10], see also [2, 3, 7, 9]. The exact form of the infinite series used in Theorem 13 is not obvious from the earlier work, but once this series has been correctly formulated, the proof of the required estimate follows the general lines of the proof in [9].

Theorem 13. *With notation as in Theorem 2, let $\lambda \ge 1$. Then there is a constant $C = C(K,V,\varphi,P,\lambda)$ so that*

$$\sum_{\mathfrak{p}\in\operatorname{Spec} R_K} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{s m_{\mathfrak{p}}^{\lambda}}} \le \frac{C}{s^{1/\lambda}} \quad \text{for all } s > 0. \tag{13}$$

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

$$g(t) = \frac{\log t}{t} \quad \text{and} \quad G(t) = e^{-st^{\lambda}}. \tag{14}$$

We use Abel summation to rewrite the series $S(\varphi,P,\lambda,s)$ in (13) as follows:

$$\begin{aligned} S(\varphi,P,\lambda,s) &= \sum_{\mathfrak{p}\in\operatorname{Spec} R_K} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{s m_{p}^{\lambda}}} \\ &= \sum_{\mathfrak{p}\in\operatorname{Spec} R_K} g(\mathsf{N}\mathfrak{p}) G(m_{\mathfrak{p}}) \\ &= \sum_{m\ge1}\Bigl(\sum_{\substack{\mathfrak{p}\in\operatorname{Spec} R_K\\ m_{\mathfrak{p}}=m}} g(\mathsf{N}\mathfrak{p}) G(m)\Bigr) \\ &= \sum_{m\ge1} G(m)\Bigl(\sum_{\substack{\mathfrak{p}\in\operatorname{Spec} R_K\\ m_{\mathfrak{p}}\le m}} g(\mathsf{N}\mathfrak{p}) - \sum_{\substack{\mathfrak{p}\in\operatorname{Spec} R_K\\ m_{\mathfrak{p}}\le m-1}} g(\mathsf{N}\mathfrak{p})\Bigr) \\ &= \sum_{m\ge1} \bigl(G(m) - G(m+1)\bigr) \sum_{\substack{\mathfrak{p}\in\operatorname{Spec} R_K\\ m_{\mathfrak{p}}\le m}} g(\mathsf{N}\mathfrak{p}). \end{aligned} \tag{15}$$

The mean value theorem gives

$$\begin{aligned} G(m) - G(m+1) \le \sup_{m<\theta<m+1} -G'(\theta) &= \sup_{m<\theta<m+1} s\lambda\theta^{\lambda-1}e^{-s\theta^\lambda} \\ &\le s\lambda(m+1)^{\lambda-1}e^{-sm^\lambda} \\ &\le s\lambda(2m)^{\lambda-1}e^{-sm^\lambda}. \end{aligned}$$

Substituting into (15) yields

$$S(\varphi,\alpha,\lambda,s) \le \sum_{m\ge1} s\lambda(2m)^{\lambda-1}e^{-sm^\lambda} \sum_{\substack{\mathfrak{p}\in\operatorname{Spec}R_K \\ m_\mathfrak{p}\le m}} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}}. \tag{16}$$

To deal with the inner sum, we use two results. The first, Proposition 10, was proven earlier. The second is as follows.

Lemma 14. *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*

$$\sum_{\mathfrak{p}\mid\mathfrak{D}} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}} \le c_1 \log\log \mathsf{N}\mathfrak{D} + c_2.$$

Proof. This is a standard result. See for example [9, Corollary 2.3] for a derivation and an explicit value for c_1. □

Using the two lemmas, we obtain the bound

$$\begin{aligned} &S(\varphi,\alpha,\lambda,s) \\ &\quad\le \sum_{m\ge1} s\lambda(2m)^{\lambda-1}e^{-sm^\lambda} \sum_{\substack{\mathfrak{p}\in\operatorname{Spec}R_K \\ m_p\le m}} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}} \quad \text{from (16)} \\ &\quad= \sum_{m\ge1} s\lambda(2m)^{\lambda-1}e^{-sm^\lambda} \sum_{\substack{\mathfrak{p}\in\operatorname{Spec}R_K \\ \mathfrak{p}\mid\mathfrak{D}(m)}} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}} \quad \text{by definition of } \mathfrak{D}(m) \\ &\quad\le \sum_{m\ge1} s\lambda(2m)^{\lambda-1}e^{-sm^\lambda}\bigl(c_1\log\log \mathsf{N}\mathfrak{D}(m) + c_2\bigr) \quad \text{from Lemma 14} \\ &\quad\le Cs\sum_{m\ge1} m^\lambda e^{-sm^\lambda} \quad \text{from Proposition 10.} \end{aligned}$$

Here $C = C(K,V,\varphi,P,\lambda)$, but is independent of s. 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 λ. (For example, if $\lambda = 2$, then it is more-or-less a theta function). Instead we use the following elementary estimate.

Lemma 15. *Fix $\lambda > 0$ and $\mu \geq 0$. There is a constant $C = C(\lambda, \mu)$ so that*

$$\sum_{m=1}^{\infty} m^{\mu} e^{-sm^{\lambda}} \leq C s^{-(\mu+1)/\lambda} \qquad \textit{for all } s > 0.$$

Proof. We note that the function $t^{\mu}e^{-st^{\lambda}}$ has a unique maximum on $[0, \infty)$. This allows us to estimate

$$\begin{aligned}\sum_{m=1}^{\infty} m^{\mu} e^{-sm^{\lambda}} &\leq 2\int_0^{\infty} t^{\mu} e^{-st^{\lambda}}\,dt \\ &= 2s^{-(\mu+1)/\lambda}\int_0^{\infty} u^{\mu}e^{-u^{\lambda}}\,du \quad \text{letting } u = s^{1/\lambda}t.\end{aligned}$$

The integral converges and is independent of s. □

Applying Lemma 15 with $\mu = \lambda$ and substituting in above yields

$$\begin{aligned}S(\varphi, \alpha, \lambda, s) &\leq C_1(K, V, \varphi, P, \lambda)s \cdot C_2(\lambda)s^{-(\lambda+1)/\lambda} \\ &= C_3(K, V, \varphi, P, \lambda)s^{-1/\lambda}.\end{aligned}$$

This completes the proof of Theorem 13. □

5. Proof of Theorem 2

We now use the analytic estimate provided by Theorem 13 to prove our main density results.

Proof of Theorem 2. (a) For any $0 < \gamma < 1$ we let

$$\mathcal{P}_{\gamma} = \left\{\mathfrak{p} \in \operatorname{Spec}(R_K) : m_{\mathfrak{p}} \leq (\log \mathsf{N}\mathfrak{p})^{\gamma}\right\}.$$

Then for all $s > 0$ we have

$$\begin{aligned}(17) \qquad \frac{C}{s^{\gamma}} &\geq \sum_{\mathfrak{p}\in\operatorname{Spec} R_K} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{sm_{\mathfrak{p}}^{1/\gamma}}} && \text{from Theorem 13 with } \lambda = 1/\gamma, \\ &\geq \sum_{\mathfrak{p}\in\mathcal{P}_{\gamma}} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{sm_{\mathfrak{p}}^{1/\gamma}}} \\ &\geq \sum_{\mathfrak{p}\in\mathcal{P}_{\gamma}} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{s\log \mathsf{N}\mathfrak{p}}} && \text{by the definition of } \mathcal{P}_{\gamma}, \\ &= \sum_{\mathfrak{p}\in\mathcal{P}_{\gamma}} \frac{\log \mathsf{N}\mathfrak{p}}{(\mathsf{N}\mathfrak{p})^{1+s}}.\end{aligned}$$

Hence

$$\overline{\boldsymbol{\delta}}(\mathcal{P}_{\gamma}) = \limsup_{s\to 1^+}(s-1)\sum_{\mathfrak{p}\in\mathcal{P}_{\gamma}} \frac{\log \mathsf{N}\mathfrak{p}}{(\mathsf{N}\mathfrak{p})^{s}} \qquad \text{by definition of upper density,}$$

$$
\begin{aligned}
&= \limsup_{s\to 0^+} s \sum_{\mathfrak{p}\in\mathcal{P}_\gamma} \frac{\log \mathsf{N}\mathfrak{p}}{(\mathsf{N}\mathfrak{p})^{s+1}} && \text{replacing } s \text{ by } s+1,\\
&\le \limsup_{s\to 0^+} C s^{1-\gamma} && \text{from (17)},\\
&= 0 && \text{since } \gamma < 1.
\end{aligned}
$$

Since the density is always nonnegative, this proves that $\boldsymbol{\delta}(\mathcal{P}_\gamma) = 0$. This is equivalent to Theorem 2(a), which asserts that the complement of $\mathcal{P}_\gamma$ has density 1.

(b) The proof is similar. Let $\epsilon > 0$ and define

$$\mathcal{P}_\epsilon = \bigl\{\mathfrak{p} \in \operatorname{Spec}(R_K) : m_\mathfrak{p} \le \epsilon \log \mathsf{N}\mathfrak{p}\bigr\}.$$

Applying Theorem 13 with $\lambda = 1$ and using the definition of $\mathcal{P}_\epsilon$, we estimate

$$
\begin{aligned}
\frac{C}{s} \ge \sum_{\mathfrak{p}\in\operatorname{Spec} R_K} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{s m_\mathfrak{p}}} \ge \sum_{\mathfrak{p}\in\mathcal{P}_\epsilon} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{s m_\mathfrak{p}}} &\ge \sum_{\mathfrak{p}\in\mathcal{P}_\epsilon} \frac{\log \mathsf{N}\mathfrak{p}}{\mathsf{N}\mathfrak{p}\cdot e^{s\epsilon \log \mathsf{N}\mathfrak{p}}}\\
&= \sum_{\mathfrak{p}\in\mathcal{P}_\gamma} \frac{\log \mathsf{N}\mathfrak{p}}{(\mathsf{N}\mathfrak{p})^{1+s\epsilon}}.
\end{aligned}
$$

Replacing s by s/ϵ yields

$$\frac{C\epsilon}{s} \ge \sum_{\mathfrak{p}\in\mathcal{P}_\gamma} \frac{\log \mathsf{N}\mathfrak{p}}{(\mathsf{N}\mathfrak{p})^{1+s}}.$$

Hence

$$\overline{\boldsymbol{\delta}}(\mathcal{P}_\epsilon) = \limsup_{s\to 0^+} s \sum_{\mathfrak{p}\in\mathcal{P}_\epsilon} \frac{\log \mathsf{N}\mathfrak{p}}{(\mathsf{N}\mathfrak{p})^{s+1}} \le C\epsilon.$$

It follows that the complement of $\mathcal{P}_\epsilon$ has lower density at least $1 - C\epsilon$. □

6. Conjectures and experiments

The density estimate provided by Theorem 2 is probably far from the truth. If the φ-orbit of a point P in $V(\mathbb{F}_\mathfrak{p})$ were truly a "random map" from $V(\mathbb{F}_\mathfrak{p})$ to itself, then the expected orbit length $m_\mathfrak{p}$ would be on the order of $\sqrt{\#V(\mathbb{F}_\mathfrak{p})} \approx \mathsf{N}\mathfrak{p}^{\frac{1}{2}\dim V}$. (See [4, 5] for statistical properties of orbits of random maps and [1] for the analysis of orbits of certain polynomial maps.) The following conjecture thus seems plausible.

Conjecture 16. *Let $K/\mathbb{Q}$ be a number field, let $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \ge 2$, and let $P \in \mathbb{P}^N(K)$ be a point whose φ-orbit is Zariski dense in $\mathbb{P}^N$. Then for every $\epsilon > 0$,*

$$\boldsymbol{\delta}\bigl\{\mathfrak{p} : m_\mathfrak{p}(\varphi, P) \le \mathsf{N}\mathfrak{p}^{\frac{N}{2}-\epsilon}\bigr\} = 0.$$

	z^2-2	z^2-1	z^2	z^2+1	z^2+2
$\lambda = 0.3$	0.038904	0.016799	0.029620	0.013705	0.012378
$\lambda = 0.4$	0.150752	0.087533	0.126437	0.079133	0.084439
$\lambda = 0.5$	0.323165	0.411141	0.282051	0.389920	0.397436
$\lambda = 0.55$	0.430150	0.721043	0.383289	0.702918	0.705128
$\lambda = 0.6$	0.541556	0.944739	0.487622	0.937666	0.941202
$\lambda = 0.7$	0.767462	0.999116	0.712644	0.997790	0.999116

TABLE 1. Proportion of $p < 20000$ with $m_p(z^2+c,3) \le p^\lambda$

We tested Conjecture 16 using quadratic polynomials z^2+c. For various values of c and various exponents λ, we computed the number of primes $p < 20000$ satisfying $m_p(z^2+c,3) < p^\lambda$. There are 2262 primes less than 20000, and Table 1 gives the value of the ratio

$$\frac{\#\{p < 20000 : m_p(\varphi_c,3) \le p^\lambda\}}{2262}$$

in each case.

As a complement to Conjecture 16, it is tempting to conjecture that $m_{\mathfrak{p}}(\varphi,P) \le \mathsf{N}\mathfrak{p}^{\frac{N}{2}+\epsilon}$ for almost all primes, but as Table 1 shows, not all maps behave equally randomly. In particular, the polynomials $\varphi(z) = z^2$ and $\varphi(z) = z^2-2$ seem to exhibit atypical behavior. This is not surprising, since they are associated to endomorphisms of the multiplicative group [12, §§6.1,6.2], so their complex and arithmetic dynamics are unusual compared to the dynamics of other quadratic polynomials. We do not have a general conjecture to complement Conjecture 16, but based on experimental and heuristic arguments, we make the following guess for quadratic polynomials.

Conjecture 17. *Let $K/\mathbb{Q}$ be a number field, let $c \in K$, let $\varphi_c(z) = z^2+c$, let $a \in K$ be a point whose φ_c-orbit is infinite, and let $\epsilon > 0$.*

(a) *If $c \ne 0, \frac{1}{2}$, then $\boldsymbol{\delta}\big\{\mathfrak{p} : m_{\mathfrak{p}}(\varphi_c,P) \le \mathsf{N}\mathfrak{p}^{\frac{1}{2}+\epsilon}\big\} = 1$.*

(b) *If $c = 0, \frac{1}{2}$, then $\boldsymbol{\delta}\big\{\mathfrak{p} : m_{\mathfrak{p}}(\varphi_c,P) \le \mathsf{N}\mathfrak{p}^{1-\epsilon}\big\} = 0$.*

References

[1] BACH, ERIC. Toward a theory of Pollard's rho method. *Inform. and Comput.* **90** (1991) 139–155. MR1094034 (92a:11151), Zbl 0716.11065.

[2] ERDŐS, PAUL; TURÁN, PAUL. Ein zahlentheoretischer Satz. *Bull. de l'institut de Math. et Mêc. a l'université Konybycheff de Tomsk*, I (1935) 101–103.

[3] ERDŐS, PAUL; TURÁN, PAUL. Über die Vereinfachung eines Landauschen Satzes. *Bull. de l'institut de Math. et Mêc. a l'université Konybycheff de Tomsk*, I (1935) 144–147.

[4] FLAJOLET, PHILIPPE; ODLYZKO, ANDREW M. Random mapping statistics. *Advances in cryptology—EUROCRYPT '89* (Houthalen, 1989), 329–354. Lecture Notes in Comput. Sci., 434. *Springer, Berlin*, 1990. MR1083961, Zbl 0747.05006.

[5] HARRIS, BERNARD. Probability distributions related to random mappings. *Ann. Math. Statist.* **31** (1960) 1045–1062. MR0119227 (22 #9993), Zbl 0158.34905.

[6] HINDRY, MARC; SILVERMAN, JOSEPH H. Diophantine geometry: an introduction. Graduate Texts in Mathematics, 201. *Springer-Verlag, New York*, 2000. MR1745599 (2001e:11058), Zbl 0948.11023.

[7] LANDAU, E. Verschärfung eines Romanoffschen Satzes. *Acta Arith.* **1** (1935) 43–62.

[8] LANG, SERGE. Fundamentals of Diophantine geometry. *Springer-Verlag, New York*, 1983. xviii+370 pp. ISBN: 0-387-90837-4. MR0715605 (85j:11005), Zbl 0528.14013.

[9] MURTY, M. RAM; ROSEN, MICHAEL; SILVERMAN, JOSEPH H. Variations on a theme of Romanoff. *Internat. J. Math.* **7** (1996) 373–391. MR1395936 (97d:11093), Zbl 0869.11004.

[10] ROMANOFF, N. P. Über einige Sätze der additiven Zahlentheorie. *Math. Ann.* **109** (1934) 668–678. MR1512916

[11] SILVERMAN, JOSEPH H. Arithmetic distance functions and height functions in Diophantine geometry. *Math. Ann.* **279** (1987) 193–216. MR919501 (89a:11066), Zbl 0607.14013.

[12] SILVERMAN, JOSEPH H. The arithmetic of dynamical systems. Graduate Texts in Mathematics, 241. *Springer-Verlag, New York*, 2007. x+511 pp. ISBN: 978-0-387-69903-5. MR2316407 (2008c:11002).

MATHEMATICS DEPARTMENT, BOX 1917, BROWN UNIVERSITY, PROVIDENCE, RI 02912 USA
jhs@math.brown.edu

This paper is available via http://nyjm.albany.edu/j/2008/14-27.html.