

COUNTING THE NUMBER OF 2-PERIODIC \mathbb{Z} -POINTS OF A DISCRETE DYNAMICAL SYSTEM WITH APPLICATIONS FROM ARITHMETIC STATISTICS, IV

BRIAN KINTU

June 30, 2025

Abstract

In this follow-up paper, we inspect a surprising relationship between the set of 2-periodic points of a polynomial map $\varphi_{d,c}$ defined by $\varphi_{d,c}(z) = z^d + c$ for all $c, z \in \mathbb{Z}$ and the coefficient c , where $d > 2$ is an integer. As in [?] we again wish to study here counting problems that are inspired by exciting advances of Bhargava-Shankar-Tsimerman and their collaborators on 2-torsion point-counting in arithmetic statistics, and also by Hutz's conjecture and Panraksa's work on 2-periodic point-counting in arithmetic dynamics. In doing so, we then first prove that for any given prime $p \geq 3$, the average number of distinct 2-periodic integral points of any $\varphi_{p,c}$ modulo p is either zero or unbounded as c tends to infinity; and so the average behavior here coinciding with the average behavior of the number of distinct fixed integral points of any $\varphi_{p,c}$ modulo p studied earlier in [?]. Inspired as in [?] by a conjecture of Hutz on 2-periodic rational points of any $\varphi_{p-1,c}$ for any given prime $p \geq 5$ in arithmetic dynamics, we then also prove that the average number of distinct 2-periodic integral points of any $\varphi_{p-1,c}$ modulo p is 1 or 2 or 0 as c tends to infinity; and so the average behavior here also coinciding with the average behavior of the number of distinct fixed integral points of any $\varphi_{p-1,c}$ modulo p studied earlier in [?]. Finally, as in [?] we then also apply here density and number field-counting results from arithmetic statistics, and consequently obtain again several counting and statistical results on irreducible monic integer polynomials $f(x) = \varphi_{p,c}^2(x) - x$ and $g(x) = \varphi_{p-1,c}^2(x) - x$ and algebraic number fields $K_f = \mathbb{Q}[x]/(f(x))$ and $L_g = \mathbb{Q}[x]/(g(x))$ arising naturally in our dynamical setting.

Contents

1 Introduction

Given any morphism $\varphi : \mathbb{P}^N(K) \rightarrow \mathbb{P}^N(K)$ of degree $d \geq 2$ defined on a projective space $\mathbb{P}^N(K)$ of dimension N , where K is a number field. Then for any $n \in \mathbb{Z}$ and $\alpha \in \mathbb{P}^N(K)$, we then call $\varphi^n = \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{n \text{ times}}$ the n^{th} iterate of φ ; and call $\varphi^n(\alpha)$ the n^{th} iteration of φ on α . By convention, φ^0 acts as the identity map, i.e., $\varphi^0(\alpha) = \alpha$ for every point $\alpha \in \mathbb{P}^N(K)$. As before, the everyday philosopher may want to know (quoting here Devaney [?]): “Where do points $\alpha, \varphi(\alpha), \varphi^2(\alpha), \dots, \varphi^n(\alpha)$ go as n becomes large, and what do they do when they get there?” Now for any given integer $n \geq 0$ and any given point $\alpha \in \mathbb{P}^N(K)$, we then call the set consisting of all the iterates $\varphi^n(\alpha)$ the (forward) orbit of α ; and which in dynamical systems we do usually denote it by $\mathcal{O}^+(\alpha)$.

As we mentioned in [?] that one of the main goals in arithmetic dynamics is to classify all the points $\alpha \in \mathbb{P}^N(K)$ according to the behavior of their forward orbits $\mathcal{O}^+(\alpha)$. In this direction, we recall that any point $\alpha \in \mathbb{P}^N(K)$ is called a *periodic point* of φ , whenever $\varphi^n(\alpha) = \alpha$ for some integer $n \in \mathbb{Z}_{\geq 0}$. In this case, any integer $n \geq 0$ such that the iterate $\varphi^n(\alpha) = \alpha$, is called *period* of α ; and the smallest such positive integer $n \geq 1$ is called the *exact period* of α . We recall $\text{Per}(\varphi, \mathbb{P}^N(K))$ to denote set of all periodic points of φ ; and also recall that for any given point $\alpha \in \text{Per}(\varphi, \mathbb{P}^N(K))$ the set of all iterates of φ on α is called *periodic orbit* of α . In their 1994 paper [?] and in his 1998 paper [?] respectively, Walde-Russo and Poonen give independently interesting examples of rational periodic points of any $\varphi_{2,c}$ defined over \mathbb{Q} ; and so the interested reader may wish to revisit [?, ?] to gain familiarity with the notion of periodicity of points. Inspired as in [?, ?] by the down-to-earth counting questions along with striking results of Bhargava-Shankar-Tsimerman [?] and their collaborators on 2-torsion point-counting in arithmetic statistics, we then study in Section ??, ??, ??, ??, ?? and ?? somewhat analogous counting and statistical questions on 2-periodic integral point-counting; and among them includes again the natural question: “How many distinct 2-periodic integral orbits can any $\varphi_{p,c}$ and $\varphi_{p-1,c}$ acting independently on $\mathbb{Z}/p\mathbb{Z}$ via iteration have on average as $c \rightarrow \infty$?” In doing so along with an inspiration from Narkiewicz's argument of ?? and also from ?? of Morton-Silverman's Conjecture ??, we then first prove the following main theorem on any $\varphi_{p,c}$ where $p \geq 3$ is any given prime; and which we state later more precisely as Theorem ??:

Theorem 1.1. *Let $p \geq 3$ be any fixed prime integer, and let $\varphi_{p,c}$ be a polynomial map defined by $\varphi_{p,c}(z) = z^p + c$ for all $c, z \in \mathbb{Z}$. Then the number of distinct 2-periodic integral points of any $\varphi_{p,c}$ modulo p is either p or zero.*

Previously in article [?] we proved that the number of distinct fixed integral points of any $\varphi_{p-1,c}$ modulo p for any given prime $p \geq 5$ is equal to 1 or 2 or 0; from which it then also followed that the average number of distinct fixed integral points of any $\varphi_{p-1,c}$ modulo p is also equal to 1 or 2 or 0 as prime $p \rightarrow \infty$. Moreover, we then also observed in [[?], Remark 3.3] that the expected total number of distinct fixed integral points in the whole family of maps $\varphi_{p-1,c}$ modulo p is equal to $1 + 2 + 0 = 3$. So now, inspired further by work in arithmetic statistics along with Hutz's Conjecture ?? (though as in [?] we do not again intend to prove Conjecture ??) and Panraksa's work [?] in arithmetic dynamics, we revisit the setting in Section ?? and then consider in Section ?? any $\varphi_{p-1,c}$ of even degree $p - 1$ iterated on the space $\mathbb{Z}/p\mathbb{Z}$ where $p \geq 5$ is any given prime. In doing so, we then also prove the following main theorem on any $\varphi_{p-1,c}$; which we state later more precisely as Theorem ??:

Theorem 1.2. *Let $p \geq 5$ be any fixed prime integer, and let $\varphi_{p-1,c}$ be a map defined by $\varphi_{p-1,c}(z) = z^{p-1} + c$ for all $c, z \in \mathbb{Z}$. Then the number of distinct 2-periodic integral points of any $\varphi_{p-1,c}$ modulo p is 1 or 2 or zero.*

Notice that the count obtained in Theorem ?? and more precisely in Theorem ?? on the number of distinct 2-periodic integral points of any $\varphi_{p-1,c}$ modulo p is independent of p (and hence independent of $\deg(\varphi_{p-1,c})$) in each of the possibilities. Moreover, we may also observe that the expected total count (namely, $1 + 1 + 2 + 0 = 4$) in Theorem ?? (and hence in Theorem ??) on the number of distinct 2-periodic integral points in the whole family of maps $\varphi_{p-1,c}$ modulo p is also independent of p and $\deg(\varphi_{p-1,c})$. On the other hand, we may also notice that the count obtained in Theorem ?? on the number of distinct 2-periodic integral points of any $\varphi_{p,c}$ modulo p may depend on p (and hence on $\deg(\varphi_{p,c})$) in one of the two possibilities. As a result, the expected total count (namely, $p + 0 = p$) in Theorem ?? on the number of distinct 2-periodic integral points in the whole family of maps $\varphi_{p,c}$ modulo p may not only depend on degree p , but may also grow to infinity as degree $p \rightarrow \infty$.

Motivated by work of Adam-Fares [?] in arithmetic dynamics and by a “counting-application” philosophy in arithmetic statistics, we then inspect again in a forthcoming article [?] the aforementioned relationship where we consider the space \mathbb{Z}_p of all p -adic integers. In doing so, we then prove 2-periodic integral point-counting result and asymptotics on any $\varphi_{p,c}$ iterated on $\mathbb{Z}_p/p\mathbb{Z}_p$ that's very analogous to the counting and asymptotics proved in this article, and also prove 2-periodic integral point-counting result and asymptotics on any $\varphi_{p-1,c}$ iterated on $\mathbb{Z}_p/p\mathbb{Z}_p$ that's also very analogous to the counting and asymptotics proved in this same article. Inspired by work of Narkiewicz [?] along with K -rational periodic version of Morton-Silverman's Conjecture ??, we then in upcoming work [?] revisit the setting in Section ?? and then consider any $\varphi_{p^\ell,c}$ defined over any number field K/\mathbb{Q} of degree $n \geq 2$, where $p \geq 3$ is any prime and $\ell \geq 1$ is any integer. In doing so, we then also prove 2-periodic integral point count that's not only very analogous to the count in Theorem ??, but may also grow to infinity as $p \rightarrow \infty$. More in [?], we again revisit the setting in Section ?? and then consider any $\varphi_{(p-1)^\ell,c}$ defined over any number field K/\mathbb{Q} of degree $n \geq 2$, where $p \geq 5$ is any prime and $\ell \geq 1$ is any integer. In doing so, we then also prove 2-periodic integral point count that's not only very analogous to the count in Theorem ?? for every K/\mathbb{Q} , any prime p and any $\ell \in \mathbb{Z}^+$, but the proved count is also independent of n and p .

In addition, to the notion of a periodic point and a periodic orbit, we also recall that a point $\alpha \in \mathbb{P}^N(K)$ is called a *preperiodic point* of φ , whenever $\varphi^{m+n}(\alpha) = \varphi^m(\alpha)$ for some integers $m \geq 0$ and $n \geq 1$. In this case, we recall that the smallest integers $m \geq 0$ and $n \geq 1$ such that $\varphi^{m+n}(\alpha) = \varphi^m(\alpha)$, are called the *preperiod* and *eventual period* of α , resp. Again, we denote the set of preperiodic points of φ by $\text{PrePer}(\varphi, \mathbb{P}^N(K))$. For any given preperiodic point α of φ , we then call the set of all iterates of φ on α , the *preperiodic orbit* of α . Now observe for $m = 0$, we have $\varphi^n(\alpha) = \alpha$ and so α is a periodic point of period n . Thus, the set $\text{Per}(\varphi, \mathbb{P}^N(K)) \subseteq \text{PrePer}(\varphi, \mathbb{P}^N(K))$; however, it need not be $\text{PrePer}(\varphi, \mathbb{P}^N(K)) \subseteq \text{Per}(\varphi, \mathbb{P}^N(K))$. In their 2014 paper [?], Doyle-Faber-Krumm give nice examples (which also recovers examples in Poonen's paper [?]) of preperiodic points of any quadratic map φ defined over quadratic fields; and so the interested reader may wish to see works [?, ?].

In the year 1950, Northcott [?] used the theory of height functions to show that not only is the set $\text{PrePer}(\varphi, \mathbb{P}^N(K))$ always finite, but also for a given morphism φ the set $\text{PrePer}(\varphi, \mathbb{P}^N(K))$ can be computed effectively. Forty-five years later, in the year 1995, Morton and Silverman conjectured that $\text{PrePer}(\varphi, \mathbb{P}^N(K))$ can be bounded in terms of degree d of φ , degree D of K , and dimension N of the space $\mathbb{P}^N(K)$. This celebrated conjecture is called the *Uniform Boundedness Conjecture*; which we then restate here as the following conjecture:

Conjecture 1.3. [[?]] Fix integers $D \geq 1$, $N \geq 1$, and $d \geq 2$. There exists a constant $C' = C'(D, N, d)$ such that for all number fields K/\mathbb{Q} of degree at most D , and all morphisms $\varphi : \mathbb{P}^N(K) \rightarrow \mathbb{P}^N(K)$ of degree d defined over K , the total number of preperiodic points of a morphism φ is at most C' , i.e., $\#\text{PrePer}(\varphi, \mathbb{P}^N(K)) \leq C'$.

Note that a special case of Conjecture ?? is when the degree D of a number field K is $D = 1$, dimension N of a space $\mathbb{P}^N(K)$ is $N = 1$, and degree d of a morphism φ is $d = 2$. In this case, if φ is a polynomial morphism, then it is a quadratic map defined over the field \mathbb{Q} . Moreover, in this very special case, in the year 1995, Flynn and Poonen and Schaefer conjectured that a quadratic map has no points $z \in \mathbb{Q}$ with exact period more than 3. This

conjecture of Flynn-Poonen-Schaefer [?] (which has been resolved for cases $n = 4, 5$ in [?, ?] respectively and conditionally for $n = 6$ in [?] is, however, still open for all cases $n \geq 7$ and moreover, which also Hutz-Ingram [?] gave strong computational evidence supporting it) is restated here formally as the following conjecture. Note that in this same special case, rational points of exact period $n \in \{1, 2, 3\}$ were first found in the year 1994 by Russo-Walde [?] and also found in the year 1995 by Poonen [?] using a different set of techniques. We restate here the anticipated conjecture of Flynn-Poonen-Schaefer as the following conjecture:

Conjecture 1.4. [[?], Conjecture 2] If $n \geq 4$, then there is no quadratic polynomial $\varphi_{2,c}(z) = z^2 + c \in \mathbb{Q}[z]$ with a rational point of exact period n .

Now by assuming Conjecture ?? and also establishing interesting results on preperiodic points, in the year 1998, Poonen [?] then concluded that the total number of rational preperiodic points of any quadratic polynomial $\varphi_{2,c}(z)$ is at most nine. We restate here formally Poonen's result as the following corollary:

Corollary 1.5. [[?], Corollary 1] If Conjecture ?? holds, then $\#\text{PrePer}(\varphi_{2,c}, \mathbb{Q}) \leq 9$, for all quadratic maps $\varphi_{2,c}$ defined by $\varphi_{2,c}(z) = z^2 + c$ for all points $c, z \in \mathbb{Q}$.

Since $\text{Per}(\varphi, \mathbb{P}^N(K)) \subseteq \text{PrePer}(\varphi, \mathbb{P}^N(K))$ and so if the size of $\text{PrePer}(\varphi, \mathbb{P}^N(K))$ is bounded above, then the size of $\text{Per}(\varphi, \mathbb{P}^N(K))$ is also bounded above and moreover bounded above by the same upper bound. So then, we may extract out the following periodic version of Conjecture ??, and the reason we do so, is because in Sections ?? and ?? we study a dynamical setting in which K is replaced with \mathbb{Z} , $N = 1$ and degree $d = p$ for any given prime integer $p > 2$ and $d = p - 1$ for any any given prime $p > 3$, respectively; in the attempt of understanding (and not claiming to prove) the possibility and validity of a periodic version of Conjecture ??:

Conjecture 1.6. ((D, N) = (1, 1)-version of Conjecture ??) Fix an integer $d \geq 2$. There exists a constant $C' = C'(d)$ such that for all morphisms $\varphi : \mathbb{P}^1(\mathbb{Q}) \rightarrow \mathbb{P}^1(\mathbb{Q})$ of degree d , the number $\#\text{Per}(\varphi, \mathbb{P}^1(\mathbb{Q})) \leq C'(d)$.

History on the Connection Between the Size of $\text{Per}(\varphi_{d,c}, K)$ and the Coefficient c

In the year 1994, Walde and Russo not only proved [[?], Corollary 4] that for a quadratic map $\varphi_{2,c}$ defined over \mathbb{Q} with a periodic point, the denominator of a rational point c , denoted as $\text{den}(c)$, is a square but they also proved that $\text{den}(c)$ is even, whenever $\varphi_{2,c}$ admits a rational cycle of length $\ell \geq 3$. Moreover, Walde-Russo also proved [[?], Cor. 6, Thm 8 and Cor. 7] that the size $\#\text{Per}(\varphi_{2,c}, \mathbb{Q}) \leq 2$, whenever $\text{den}(c)$ is an odd integer.

Three years later, in the year 1997, Call-Goldstine [?] proved that the size of $\text{PrePer}(\varphi_{2,c}, \mathbb{Q})$ can be bounded above in terms of the number of distinct odd primes dividing $\text{den}(c)$. We state formally this result as:

Theorem 1.7. [[?], Theorem 6.9] Let $e > 0$ be an integer and let s be the number of distinct odd prime factors of e . Define $\varepsilon = 0, 1, 2$, if $4 \nmid e$, if $4 \mid e$ and $8 \nmid e$, if $8 \mid e$, respectively. Let $c = a/e^2$, where $a \in \mathbb{Z}$ and $\text{GCD}(a, e) = 1$. If $c \neq -2$, then the total number of \mathbb{Q} -preperiodic points of $\varphi_{2,c}$ is at most $2^{s+2+\varepsilon} + 1$. Moreover, a quadratic map $\varphi_{2,-2}$ has exactly six rational preperiodic points.

Eight years later, after the work of Call-Goldstine, in the year 2005, Benedetto [?] studied polynomial maps φ of arbitrary degree $d \geq 2$ defined over an arbitrary global field K , and then established the following result on the relationship between the size of the set $\text{PrePer}(\varphi, K)$ and the number of bad primes of φ in K :

Theorem 1.8. [[?], Main Theorem] Let K be a global field, $\varphi \in K[z]$ be a polynomial of degree $d \geq 2$ and s be the number of bad primes of φ in K . The number of preperiodic points of φ in $\mathbb{P}^N(K)$ is at most $O(s \log s)$.

Since Benedetto's Theorem ?? applies to any polynomial φ of arbitrary degree $d \geq 2$ defined over any number field K , it then follows that one can immediately apply Benedetto's Thm ?? to any polynomial φ of arbitrary odd or even degree $d > 2$ defined over any number field K and then obtain the upper bound in Theorem ??.

Seven years after the work of Benedetto, in the year 2012, Narkiewicz's work [?] not only showed that any $\varphi_{d,c}$ defined over \mathbb{Q} with odd degree $d \geq 3$ has no rational periodic points of exact period $n > 1$, but his also showed that the total number of \mathbb{Q} -preperiodic points is at most 4. We restate this result here as the following:

Theorem 1.9. [?] For any integer $n > 1$ and any odd integer $d \geq 3$, there is no $c \in \mathbb{Q}$ such that $\varphi_{d,c}$ defined by $\varphi_{d,c}(z)$ for all $c, z \in \mathbb{Q}$ has rational periodic points of exact period n . Moreover, $\#\text{PrePer}(\varphi_{d,c}, \mathbb{Q}) \leq 4$.

Three years after [?], in 2015, Hutz [?] developed an algorithm determining effectively all \mathbb{Q} -preperiodic points of a morphism defined over a given number field K ; from which he then made the following conjecture:

Conjecture 1.10. [[?], Conjecture 1a] For any integer $n > 2$, there is no even degree $d > 2$ and no point $c \in \mathbb{Q}$ such that the polynomial map $\varphi_{d,c}$ has rational points of exact period n . Moreover, $\#\text{PrePer}(\varphi_{d,c}, \mathbb{Q}) \leq 4$.

Remark 1.11. If Conjecture ?? held, it would then follow that the total number of 2-periodic rational points (and so the total number of 2-periodic integral points) of any $\varphi_{d,c}(x) = x^d + c$ of even degree $d > 2$ is equal to 4

or strictly less than 4. Moreover, since the monic polynomial $\varphi_{d,c}(x) \in \mathbb{Z}[x]$ has good reduction modulo p , then the total number of 2-periodic integral points of any reduced polynomial $\varphi_{d,c}(x)$ modulo p (and hence of any map $\varphi_{d,c}$ modulo p) is also equal to 4 or strictly less than 4. Furthermore, if Conjecture ?? held, then it would also follow that the total number of fixed integral points and 2-periodic integral points of any $\varphi_{d,c}(x)$ modulo p (and hence of any $\varphi_{d,c}$ modulo p) is also equal to 4 or strictly less than 4. But of course now the issue is that we unfortunately don't know as of this article whether Conjecture ?? holds or not, let alone whether 4 is the correct upper bound on the total number of fixed and 2-periodic rational (and hence integral) points of any polynomial map $\varphi_{d,c}$ of even degree $d > 2$. On whether any progress has been made on Conjecture ??, recently Panraksa [?] proved among many other results that the polynomial $\varphi_{4,c}(z) \in \mathbb{Q}[z]$ has rational points of exact period $n = 2$. Moreover, he also proved that $\varphi_{d,c}(z) \in \mathbb{Q}[z]$ has no rational points of exact period $n = 2$ for any $c \in \mathbb{Q}$ with $c \neq -1$ and $d = 6, 2k$ with $3 \mid 2k - 1$. The interested reader may find these mentioned results of Panraksa in his unconditional Thms. 2.1, 2.4 and Thm. 1.7 conditioned on the abc-conjecture in [?].

Twenty-eight years later, after the work of Walde-Russo, in the year 2022, Eliahou-Fares proved [[?], Theorem 2.12] that the denominator of a rational point $-c$, denoted as $\text{den}(-c)$ is divisible by 16, whenever $\varphi_{2,-c}$ defined by $\varphi_{2,-c}(z) = z^2 - c$ for all $c, z \in \mathbb{Q}$ admits a rational cycle of length $\ell \geq 3$. Moreover, they also proved [[?], Proposition 2.8] that the size $\#\text{Per}(\varphi_{2,-c}, \mathbb{Q}) \leq 2$, whenever $\text{den}(-c)$ is an odd integer. Motivated by [?], Eliahou-Fares [?] also proved that the size of $\text{Per}(\varphi_{2,-c}, \mathbb{Q})$ can be bounded above by using information on $\text{den}(-c)$, namely, information in terms of the number of distinct primes dividing $\text{den}(-c)$. Moreover, they in [?] also showed that the upper bound is four, whenever $c \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. We restate here their results as:

Corollary 1.12. *[[?, ?], Cor. 3.11 and Cor. 4.4, respectively] Let $c \in \mathbb{Q}$ such that $\text{den}(c) = d^2$ with $d \in 4\mathbb{N}$. Let s be the number of distinct primes dividing d . Then, the total number of \mathbb{Q} -periodic points of $\varphi_{2,-c}$ is at most $2^s + 2$. Moreover, for $c \in \mathbb{Q}^*$ such that the $\text{den}(c)$ is a power of a prime number. Then, $\#\text{Per}(\varphi_{2,c}, \mathbb{Q}) \leq 4$.*

The purpose of this article is to once again inspect further the above connection, independently in the case of polynomial maps $\varphi_{p,c}$ of odd prime degree p defined over \mathbb{Z} for any given prime integer $p \geq 3$ and in the case of polynomial maps $\varphi_{p-1,c}$ of even degree $p-1$ defined over \mathbb{Z} for any given prime integer $p \geq 5$; and doing so from a spirit that is truly inspired and guided by some of the many striking developments in arithmetic statistics.

2 On Number of 2-Periodic Integral Points of any Family of Polynomial Maps $\varphi_{p,c}$

In this section, we wish to count the number of distinct 2-periodic integral points of any polynomial map $\varphi_{p,c}$, first by modulo 3 and then count by modulo p for any given prime integer $p \geq 3$. To this end, we let $p \geq 3$ be any prime integer, $c \in \mathbb{Z}$ be any integer, and then define the following 2-periodic point-counting function

$$N_c^{(2)}(p) := \#\{z \in \mathbb{Z}/p\mathbb{Z} : \varphi_{p,c}(z) - z \not\equiv 0 \pmod{p}, \text{ but } \varphi_{p,c}^2(z) - z \equiv 0 \pmod{p}\}. \quad (1)$$

We then first prove the following theorem on the number of distinct 2-periodic points of any $\varphi_{3,c}$ modulo 3:

Theorem 2.1. *Let $\varphi_{3,c}$ be a cubic map defined by $\varphi_{3,c}(z) = z^3 + c$ for all $c, z \in \mathbb{Z}$, and let $N_c^{(2)}(3)$ be defined as in (??). Then $N_c^{(2)}(3) = 3$ for every coefficient $c = 3t$; otherwise, we have $N_c^{(2)}(3) = 0$ for any coefficient $c \neq 3t$.*

Proof. Let $f(z) = \varphi_{3,c}^2(z) - z = \varphi_{3,c}(\varphi_{3,c}(z)) - z = (z^3 + c)^3 - z + c$, and notice that applying the binomial theorem on the polynomial $(z^3 + c)^3$, we then obtain that $f(z) = z^9 + 3z^6c + 3z^3c^2 - z + c^3 + c$. Now for every coefficient $c = 3t$ of the polynomial $f(z)$, reducing both sides of $f(z)$ modulo 3, we then obtain that $f(z) \equiv z^9 - z \pmod{3}$; and so the reduced polynomial $f(z)$ modulo 3 is now a polynomial defined over a finite field $\mathbb{Z}/3\mathbb{Z}$ of order 3. Moreover, it is a well-known fact about polynomials over finite fields that the cubic polynomial $h(x) := x^3 - x$ vanishes at each of the three distinct elements in $\mathbb{Z}/3\mathbb{Z}$; and so we then obtain $z^3 = z$ for every $z \in \mathbb{Z}/3\mathbb{Z}$. But now $z^9 = (z^3)^3 = z^3 = z$ for every $z \in \mathbb{Z}/3\mathbb{Z}$, and so the reduced polynomial $f(z) \equiv 0$ for every point $z \in \mathbb{Z}/3\mathbb{Z}$. Hence, we then conclude that $\#\{z \in \mathbb{Z}/3\mathbb{Z} : \varphi_{3,c}(z) - z \not\equiv 0 \pmod{3}, \text{ but } \varphi_{3,c}^2(z) - z \equiv 0 \pmod{3}\} = 3$, and so the number $N_c^{(2)}(3) = 3$. To see the second part, we first note that since the coefficient $c \neq 3t$, then this also means $c \not\equiv 0 \pmod{3}$. But now observe that the polynomial $(z^3 + c)^3 - z + c \equiv c^3 + c \pmod{3}$ for every $z \in \mathbb{Z}/3\mathbb{Z}$, since we also observed earlier that $z^9 = z$ for every $z \in \mathbb{Z}/3\mathbb{Z}$; and since also $c^3 + c \not\equiv 0 \pmod{3}$ for every coefficient $c \not\equiv 0 \pmod{3}$, it then follows that $f(z) \not\equiv 0 \pmod{3}$ for every point $z \in \mathbb{Z}/3\mathbb{Z}$. This then means that the monic polynomial $\varphi_{3,c}^2(x) - x$ has no roots in $\mathbb{Z}/3\mathbb{Z}$ for every coefficient $c \neq 3t$, and hence we then conclude that the number $N_c^{(2)}(3) = 0$ as also desired. This then completes the whole proof, as needed. \square

We now wish to generalize Theorem ?? to any polynomial map $\varphi_{p,c}$ for any given prime $p \geq 3$. More precisely, we prove that the number of distinct 2-periodic integral points of any $\varphi_{p,c}$ modulo p is either p or 0:

Theorem 2.2. Let $p \geq 3$ be any fixed prime integer, and let $\varphi_{p,c}$ be defined by $\varphi_{p,c}(z) = z^p + c$ for all $c, z \in \mathbb{Z}$. Let $N_c^{(2)}(p)$ be as in (??). Then $N_c^{(2)}(p) = p$ for every coefficient $c = pt$; otherwise, $N_c^{(2)}(p) = 0$ for every $c \neq pt$.

Proof. By applying a similar argument as in the Proof of Theorem ??, we then obtain the count as desired. That is, let $f(z) = \varphi_{p,c}^2(z) - z = \varphi_{p,c}(\varphi_{p,c}(z)) - z = (z^p + c)^p - z + c$, and again notice that applying the binomial theorem on the polynomial $(z^p + c)^p$ and also for every coefficient $c = pt$, reducing both sides of $f(z)$ modulo p , it then follows that $f(z) \equiv z^{p^2} - z \pmod{p}$. So now, it is a well-known general fact about polynomials over finite fields that the monic polynomial $h(x) = x^p - x$ vanishes at every element in a finite field $\mathbb{Z}/p\mathbb{Z}$ of p distinct elements; and so we then obtain $z^p = z$ and hence $z^{p^2} = (z^p)^p = z$ for every $z \in \mathbb{Z}/p\mathbb{Z}$. But then the reduced polynomial $f(z) \equiv 0 \pmod{p}$ for every point $z \in \mathbb{Z}/p\mathbb{Z}$; and so we then conclude that $\#\{z \in \mathbb{Z}/p\mathbb{Z} : \varphi_{p,c}(z) - z \not\equiv 0 \pmod{p}, \text{ but } \varphi_{p,c}^2(z) - z \equiv 0 \pmod{p}\} = p$, and so the number $N_c^{(2)}(p) = p$. To see the second part, we as before first note that for every coefficient $c \neq pt$, then this also means that $c \not\equiv 0 \pmod{p}$. But then the monic polynomial $(z^p + c)^p - z + c \equiv c^p + c \pmod{p}$ for every element $z \in \mathbb{Z}/p\mathbb{Z}$, since we also know that $z^{p^2} = z$ for every $z \in \mathbb{Z}/p\mathbb{Z}$; and because $c^p + c \not\equiv 0 \pmod{p}$ for every $c \not\equiv 0 \pmod{p}$, we then obtain that $f(z) \not\equiv 0 \pmod{p}$ for every $z \in \mathbb{Z}/p\mathbb{Z}$. This then means $\varphi_{p,c}^2(x) - x$ has no roots in $\mathbb{Z}/p\mathbb{Z}$ for every $c \neq pt$, and hence we conclude $N_c^{(2)}(p) = 0$ as also desired. This then completes the whole proof, as needed. \square

Remark 2.3. With now Theorem ??, we may to each 2-periodic integral point of $\varphi_{p,c}$ associate 2-periodic integral orbit. So then, a dynamical translation of Theorem ?? is the claim that the number of distinct 2-periodic integral orbits that any $\varphi_{p,c}$ has when iterated on the space $\mathbb{Z}/p\mathbb{Z}$ is either p or zero. As we mentioned in Introduction ?? that the count obtained in Theorem ?? on the number of distinct 2-periodic integral points of any $\varphi_{p,c}$ modulo p may depend on p (and hence depend on $\deg(\varphi_{p,c})$) in one of the two possibilities. As a result, the expected total count (namely, $p + 0 = p$) in Theorem ?? on the number of distinct 2-periodic integral points in the whole family of polynomial maps $\varphi_{p,c}$ modulo p may not only depend on p , but may also tend to infinity as $p \rightarrow \infty$; a somewhat interesting phenomenon coinciding precisely with a phenomenon remarked in [?], Remark 2.5] on the expected (total) number of distinct fixed integral points (orbits) in the whole family of maps $\varphi_{p,c}$ modulo p , however, differing very significantly from a phenomenon remarked about in Remark ??.

3 On Number of 2-Periodic Integral Points of any Family of Polynomial Maps $\varphi_{p-1,c}$

As in Section ??, we in this section also wish to count the number of distinct 2-periodic integral points of any $\varphi_{p-1,c}$, first by modulo 5 and then by modulo p for any given prime integer $p \geq 5$. As before, we again let $p \geq 5$ be any given prime, $c \in \mathbb{Z}$ be any integer, and then define the following 2-periodic point-counting function

$$M_c^{(2)}(p) := \#\{z \in \mathbb{Z}/p\mathbb{Z} : \varphi_{p-1,c}(z) - z \not\equiv 0 \pmod{p}, \text{ but } \varphi_{p-1,c}^2(z) - z \equiv 0 \pmod{p}\}. \quad (2)$$

We then first prove the following theorem on the number of distinct 2-periodic points of any $\varphi_{4,c}$ modulo 5:

Theorem 3.1. Let $\varphi_{4,c}$ be defined by $\varphi_{4,c}(z) = z^4 + c$ for all $c, z \in \mathbb{Z}$, and let $M_c^{(2)}(5)$ be defined as in (??). Then $M_c^{(2)}(5) = 1$ or 2 for every $c \equiv \pm 1 \pmod{5}$ or $c = 5t$, resp.; otherwise, $M_c^{(2)}(5) = 0$ for every $c \not\equiv \pm 1, 0 \pmod{5}$.

Proof. Let $g(z) = \varphi_{4,c}^2(z) - z = \varphi_{4,c}(\varphi_{4,c}(z)) - z = (z^4 + c)^4 - z + c$, and notice that applying the binomial theorem on the polynomial $(z^4 + c)^4$, we then obtain that $g(z) = z^{16} + 4z^{12}c + 6z^8c^2 + 4z^4c^3 - z + c^4 + c$. Now for every coefficient $c = 5t$, reducing both sides of $g(z)$ modulo 5, we then obtain $g(z) \equiv z^{16} - z \pmod{5}$; and so the reduced polynomial $g(z)$ modulo 5 is now a polynomial defined over a finite field $\mathbb{Z}/5\mathbb{Z}$ of order 5. Now recall by Fermat's Little Theorem that $z^4 \equiv 1 \pmod{5}$ for every integer z indivisible by 5 (equivalently, $z^4 = 1$ for every $z \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$). But then $z^{16} = (z^4)^4 = 1$ for every $z \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$ and so $g(z) \equiv 1 - z \pmod{5}$ for every nonzero $z \in \mathbb{Z}/5\mathbb{Z}$; and from which it then follows that the reduced polynomial $g(z)$ modulo 5 has a root in $\mathbb{Z}/5\mathbb{Z}$, namely, $z \equiv 1 \pmod{5}$. Moreover, since z is also a linear factor of $g(z) \equiv z(z^{15} - 1) \pmod{5}$, then $z \equiv 0 \pmod{5}$ is also a root of $g(z)$ modulo 5. Hence, we then conclude that $\#\{z \in \mathbb{Z}/5\mathbb{Z} : \varphi_{4,c}(z) - z \not\equiv 0 \pmod{5}, \text{ but } \varphi_{4,c}^2(z) - z \equiv 0 \pmod{5}\} = 2$, and so the number $M_c^{(2)}(5) = 2$. To see that $M_c^{(2)}(5) = 1$ for every coefficient $c \equiv 1 \pmod{5}$, we note that with $c \equiv 1 \pmod{5}$ and also $z^4 = 1$ for every $z \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$, then reducing $g(z) = (z^4 + c)^4 - z + c$ modulo 5, we then obtain $g(z) \equiv 2 - z \pmod{5}$ and so $g(z)$ modulo 5 has a root in $\mathbb{Z}/5\mathbb{Z}$, namely, $z \equiv 2 \pmod{5}$; and so we conclude $M_c^{(2)}(5) = 1$. We now show $M_c^{(2)}(5) = 1$ for every coefficient $c \equiv -1 \pmod{5}$. Again, we note that with $c \equiv -1 \pmod{5}$ and also $z^4 = 1$ for

every $z \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$, then reducing $g(z) = (z^4 + c)^4 - z + c$ modulo 5, we then obtain $g(z) \equiv -(z + 1) \pmod{5}$ and so $g(z)$ modulo 5 has a root in $\mathbb{Z}/5\mathbb{Z}$, namely, $z \equiv -1 \pmod{5}$; and so we then conclude $M_c^{(2)}(5) = 1$.

Finally, we now show that the number $M_c^{(2)}(5) = 0$ for every coefficient $c \not\equiv \pm 1, 0 \pmod{5}$. Let's suppose that $(z^4 + c)^4 - z + c \equiv 0 \pmod{5}$ for some nonzero $z \in \mathbb{Z}/5\mathbb{Z}$ and for every $c \not\equiv \pm 1, 0 \pmod{5}$. Then since $z^4 = 1$ in $\mathbb{Z}/5\mathbb{Z} \setminus \{0\}$ and so $(z^4 + c)^4 = (1 + c)^4$ in $\mathbb{Z}/5\mathbb{Z} \setminus \{0\}$, it then follows $(z^4 + c)^4 - z + c = (1 + c)^4 - z + c$ for some $z \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$. Moreover, we also note that $(1 + c)^4 - z + c \equiv 2 - z + (c^2 + 4c^3) \pmod{5}$; and so $2 - z + (c^2 + 4c^3) \equiv 0 \pmod{5}$ as by the above supposition. Now observe that $2 - z + (c^2 + 4c^3) \equiv 0 \pmod{5}$ can happen if $2 - z \equiv 0 \pmod{5}$ and also $c^2 + 4c^3 \equiv 0 \pmod{5}$. But then we may also recall from the first part that $2 - z \equiv 0 \pmod{5}$ whenever $c \equiv 1 \pmod{5}$; which then contradicts the earlier condition $c \not\equiv \pm 1, 0 \pmod{5}$. Thus, we then conclude $M_c^{(2)}(5) = 0$ as also desired; which then completes the whole proof, as needed. \square

We now wish to generalize Theorem ?? to any $\varphi_{p-1,c}$ for any prime $p \geq 5$. More precisely, we prove that the number of distinct 2-periodic integral points of any polynomial map $\varphi_{p-1,c}$ modulo p is also 1 or 2 or zero:

Theorem 3.2. *Let $p \geq 5$ be any fixed prime integer, and let $\varphi_{p-1,c}$ be a polynomial map defined by $\varphi_{p-1,c}(z) = z^{p-1} + c$ for all $c, z \in \mathbb{Z}$. Let $M_c^{(2)}(p)$ be the number defined as in (?). Then $M_c^{(2)}(p) = 1$ or 2 for every coefficient $c \equiv \pm 1 \pmod{p}$ or $c = pt$, respectively; otherwise, we have $M_c^{(2)}(p) = 0$ for every coefficient $c \not\equiv \pm 1, 0 \pmod{p}$.*

Proof. By applying a similar counting argument as in the Proof of Theorem ??, we then obtain the count as desired. That is, let $g(z) = \varphi_{p-1,c}^2(z) - z = \varphi_{p-1,c}(\varphi_{p-1,c}(z)) - z = (z^{p-1} + c)^{p-1} - z + c$, and again note that applying the binomial theorem on $(z^{p-1} + c)^{p-1}$ and also for every coefficient $c = pt$, reducing both sides of $g(z)$ modulo p , we then obtain $g(z) \equiv z^{(p-1)^2} - z \pmod{p}$; and so $g(z)$ modulo p is a polynomial defined over a finite field $\mathbb{Z}/p\mathbb{Z}$ of p distinct elements. Now since by Fermat's Little Theorem (FLT) we know $z^{p-1} \equiv 1 \pmod{p}$ for every integer z indivisible by p (equivalently, $z^{p-1} = 1$ for every $z \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$), it then also follows that $z^{(p-1)^2} = 1$ for every $z \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ and so $g(z) \equiv 1 - z \pmod{p}$ for every nonzero $z \in \mathbb{Z}/p\mathbb{Z}$ and so $g(z)$ modulo p has a root in $\mathbb{Z}/p\mathbb{Z}$, namely, $z \equiv 1 \pmod{p}$. Moreover, since z is also a linear factor of $g(z) \equiv z(z^{(p-1)^2-1} - 1) \pmod{p}$, then $z \equiv 0 \pmod{p}$ is also root of $g(z)$ modulo p . Hence, we then conclude that $\#\{z \in \mathbb{Z}/p\mathbb{Z} : \varphi_{p-1,c}(z) - z \not\equiv 0 \pmod{p}, \text{ but } \varphi_{p-1,c}^2(z) - z \equiv 0 \pmod{p}\} = 2$, and so the number $M_c^{(2)}(p) = 2$. To see that $M_c^{(2)}(p) = 1$ for every coefficient $c \equiv 1 \pmod{p}$, we again note that with $c \equiv 1 \pmod{p}$ and also $z^{p-1} = 1$ for every $z \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, then reducing $g(z) = (z^{p-1} + c)^{p-1} - z + c$ modulo p , we then obtain $g(z) \equiv 2 - z \pmod{p}$, since we also know $2^{p-1} \equiv 1 \pmod{p}$ by (FLT); and so $g(z)$ modulo p has a root in $\mathbb{Z}/p\mathbb{Z}$, namely, $z \equiv 2 \pmod{p}$ and so we conclude $M_c^{(2)}(p) = 1$. We now show $M_c^{(2)}(p) = 1$ for every coefficient $c \equiv -1 \pmod{p}$. As before, we again note that with $c \equiv -1 \pmod{p}$ and also $z^{p-1} = 1$ for every $z \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, then reducing $g(z) = (z^{p-1} + c)^{p-1} - z + c$ modulo p , we then obtain $g(z) \equiv -(z + 1) \pmod{p}$ for every nonzero $z \in \mathbb{Z}/p\mathbb{Z}$ and so $g(z)$ modulo p has a root in $\mathbb{Z}/p\mathbb{Z}$, namely, $z \equiv -1 \pmod{p}$; and so we conclude $M_c^{(2)}(p) = 1$.

Finally, we now show that the number $M_c^{(2)}(p) = 0$ for every coefficient $c \not\equiv \pm 1, 0 \pmod{p}$. As before, let's suppose that $(z^{p-1} + c)^{p-1} - z + c \equiv 0 \pmod{p}$ for some nonzero $z \in \mathbb{Z}/p\mathbb{Z}$ and for every coefficient $c \not\equiv \pm 1, 0 \pmod{p}$. Then since $z^{p-1} = 1$ in $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ and so $(z^{p-1} + c)^{p-1} = (1 + c)^{p-1}$ in $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, then $(z^{p-1} + c)^{p-1} - z + c = (1 + c)^{p-1} - z + c$ for every $z \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Now applying the binomial theorem and then reducing modulo p , we then obtain $(1 + c)^{p-1} - z + c \equiv 2 - z + ((p-1)c^{p-2} + \dots + pc) \pmod{p}$, since also $p \nmid c$ and so by (FLT) we know $c^{p-1} \equiv 1 \pmod{p}$; and so $2 - z + ((p-1)c^{p-2} + \dots + pc) \equiv 0 \pmod{p}$ as by the above supposition. So now, we may again observe $2 - z + ((p-1)c^{p-2} + \dots + pc) \equiv 0 \pmod{p}$ can happen whenever $2 - z \equiv 0 \pmod{p}$ and also $(p-1)c^{p-2} + \dots + pc \equiv 0 \pmod{p}$. But then we may again also recall from the first part that $2 - z \equiv 0 \pmod{p}$ whenever $c \equiv 1 \pmod{p}$; which then contradicts the earlier condition $c \not\equiv \pm 1, 0 \pmod{p}$. Thus, we then conclude $M_c^{(2)}(p) = 0$; which then completes the whole proof, as desired. \square

Remark 3.3. As before, with now Theorem ?? at our disposal, we may again to each distinct 2-periodic integral point of $\varphi_{p-1,c}$ associate 2-periodic integral orbit. In doing so, we then also obtain a dynamical translation of Theorem ??, namely, the claim that the number of distinct 2-periodic orbits that any $\varphi_{p-1,c}$ has when iterated on the space $\mathbb{Z}/p\mathbb{Z}$ is 1 or 2 or zero. Again, as we've already mentioned in Introduction ?? that the count obtained in Theorem ?? on the number of distinct 2-periodic integral points of any $\varphi_{p-1,c}$ modulo p is independent of p (and hence independent of the degree of $\varphi_{p-1,c}$) in each of the possibilities considered. Moreover, we may also observe that the expected total count of the number of distinct 2-periodic integral points (orbits) in the whole family of maps $\varphi_{p-1,c}$ modulo p (namely, $1 + 1 + 2 + 0 = 4$) is also independent of p (and so independent of $\deg(\varphi_{p-1,c})$); a somewhat interesting phenomenon differing significantly from a phenomenon that we remarked in ??, however, coinciding somewhat surprisingly with an observation that we noted earlier on Conjecture ??. Furthermore, recall in [?], Thm. 3.2] we found $z \equiv 1, 0, 2 \pmod{p}$ are fixed integral points of $\varphi_{p-1,c}$ modulo

p , and moreover we've also found here in the Proof of Thm. ?? that $z \equiv 1, 0, 2 \pmod{p}$ are also 2-periodic integral points of $\varphi_{p-1,c}$ modulo p . It may then follow from Proof of Thm. ?? that the expected total number of distinct fixed and 2-periodic integral points in the whole family of maps $\varphi_{p-1,c}$ modulo p is 4; a somewhat interesting observation coinciding with the first predicted upper bound 4 observed in Remark ?? on Conj.??.

4 On the Average Number of 2-Periodic Points of any Polynomial Map $\varphi_{p,c}$ & $\varphi_{p-1,c}$

In this section, we wish to study the asymptotic behavior of each of the 2-periodic point-counting functions $N_c^{(2)}(p)$ and $M_c^{(2)}(p)$ as $c \rightarrow \infty$. First, we wish to determine: “What is the average value of the function $N_c^{(2)}(p)$ as $c \rightarrow \infty$?” The following corollary shows that the average value of $N_c^{(2)}(p)$ is zero or unbounded as $c \rightarrow \infty$:

Corollary 4.1. *Let $p \geq 3$ be any prime integer. Then the average value of 2-periodic point-counting function $N_c^{(2)}(p)$ is either equal to zero or unbounded as $c \rightarrow \infty$. More precisely, we have*

$$(a) \text{ Avg } N_{c \neq pt}^{(2)}(p) := \lim_{c \rightarrow \infty} \frac{\sum_{\substack{3 \leq p \leq c, \\ p \nmid c}} N_c^{(2)}(p)}{\sum_{\substack{3 \leq p \leq c, \\ p \nmid c}} 1} = 0.$$

$$(b) \text{ Avg } N_{c=pt}^{(2)}(p) := \lim_{c \rightarrow \infty} \frac{\sum_{\substack{3 \leq p \leq c, \\ p | c}} N_c^{(2)}(p)}{\sum_{\substack{3 \leq p \leq c, \\ p | c}} 1} = \infty.$$

Proof. Since from Theorem ?? we know that $N_c^{(2)}(p) = 0$ for any $p \nmid c$, we then obtain $\lim_{c \rightarrow \infty} \frac{\sum_{\substack{3 \leq p \leq c, \\ p \nmid c}} N_c^{(2)}(p)}{\sum_{\substack{3 \leq p \leq c, \\ p | c}} 1} = 0$;

and so the average value of $N_c^{(2)}(p)$, namely, $\text{Avg } N_{c \neq pt}^{(2)}(p) = 0$. Similarly, since $N_c^{(2)}(p) = p$ for any $p | c$, then summing over all $p \geq 3$ for which $p | c$, we then obtain $\sum_{\substack{3 \leq p \leq c, \\ p | c}} N_c^{(2)}(p) = \sum_{\substack{3 \leq p \leq c, \\ p | c}} p =: \sigma_{1,p}(c)$, where $\sigma_1(n)$ is by definition the number of divisors of a positive integer n . More to this, we notice $\sum_{\substack{3 \leq p \leq c, \\ p | c}} 1 = \omega(c)$,

where $\omega(n)$ is by definition the number of distinct prime factors of n ; and so $\frac{\sum_{\substack{3 \leq p \leq c, \\ p | c}} N_c^{(2)}(p)}{\sum_{\substack{3 \leq p \leq c, \\ p | c}} 1} = \frac{\sigma_{1,p}(c)}{\omega(c)}$. Now

observe $\sigma_{1,p}(c) = \sum_{\substack{3 \leq p \leq c, \\ p | c}} p \leq \sum_{\substack{3 \leq p \leq c}} p$ for each $c \in \mathbb{Z}_{\geq 3}$, and since from [?] we also know that $\sum_{\substack{3 \leq p \leq c}} p = \frac{c^2}{2}(\log c + \log \log c - \frac{3}{2} + \frac{\log \log c - 5/2}{\log c}) + O(\frac{c^2(\log \log c)^2}{\log^2 c})$ for each $c \geq 3$, we then obtain $\sigma_{1,p}(c) \leq \frac{c^2}{2}(\log c + \log \log c - \frac{3}{2} + \frac{\log \log c - 5/2}{\log c}) + O(\frac{c^2(\log \log c)^2}{\log^2 c})$. Moreover, it is also a well-known fact that $\omega(c) \leq \frac{\log c}{\log 2}$ for every $c \in \mathbb{Z}_{\geq 3}$. Now since $\frac{\log c}{\log 2} \rightarrow \infty$ very slow as $c \rightarrow \infty$, then $\omega(c) \rightarrow \infty$ very slow as $c \rightarrow \infty$. On the other hand, since $\frac{c^2}{2}(\log c + \log \log c - \frac{3}{2} + \frac{\log \log c - 5/2}{\log c}) + O(\frac{c^2(\log \log c)^2}{\log^2 c}) \rightarrow \infty$ very fast as $c \rightarrow \infty$, then $\sigma_{1,p}(c) \rightarrow \infty$ very fast as $c \rightarrow \infty$. But then $\frac{\sigma_{1,p}(c)}{\omega(c)} \rightarrow \infty$ very fast as $c \rightarrow \infty$ and so $\lim_{c \rightarrow \infty} \frac{\sum_{\substack{3 \leq p \leq c, \\ p | c}} N_c^{(2)}(p)}{\sum_{\substack{3 \leq p \leq c, \\ p | c}} 1} = \infty$; and from which we then conclude that $\text{Avg } N_{c=pt}^{(2)}(p) = \infty$, as also desired. This then completes the whole proof, as needed. \square

Remark 4.2. From arithmetic statistics to arithmetic dynamics, Cor. ?? shows that any $\varphi_{p,c}$ iterated on the space $\mathbb{Z}/p\mathbb{Z}$ has on average zero or unbounded number of distinct 2-periodic integral orbits modulo p as $c \rightarrow \infty$; a somewhat interesting average phenomenon coinciding precisely with an averaging phenomenon remarked in [[?], Remark 7.2] on the average number of distinct fixed orbits of any map $\varphi_{p,c}$ iterated on the space $\mathbb{Z}/p\mathbb{Z}$.

Similarly, we also wish to determine: “What is the average value of the function $M_c^{(2)}(p)$ as $c \rightarrow \infty$?” The following corollary shows that the average value of $M_c^{(2)}(p)$ exists and is moreover 1 or 2 or 0 as $c \rightarrow \infty$:

Corollary 4.3. *Let $p \geq 5$ be any prime integer. Then the average value of 2-periodic point-counting function $M_c^{(2)}(p)$ exists and is equal to 1 or 2 or 0 as $c \rightarrow \infty$. More precisely, we have*

$$(a) \text{ Avg } M_{c \pm 1 = pt}^{(2)}(p) := \lim_{(c \pm 1) \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq (c \pm 1), \\ p | (c \pm 1)}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq (c \pm 1), \\ p | (c \pm 1)}} 1} = 1.$$

$$(b) \text{ Avg } M_{c=pt}^{(2)}(p) := \lim_{c \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq c, \\ p | c}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq c, \\ p | c}} 1} = 2.$$

$$(c) \text{ Avg } M_{c \not\equiv \pm 1, 0 \pmod{p}}^{(2)}(p) := \lim_{c \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq c, \\ c \not\equiv \pm 1, 0 \pmod{p}}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq c, \\ c \not\equiv \pm 1, 0 \pmod{p}}} 1} = 0.$$

Proof. Since from Theorem ?? we know $M_c^{(2)}(p) = 1$ for any p such that $p \mid (c-1)$ or $p \mid (c+1)$, it then follows $\lim_{(c-1) \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq (c-1), \\ p \mid (c-1)}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq (c-1), \\ p \mid (c-1)}} 1} = \lim_{(c-1) \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq (c-1), \\ p \mid (c-1)}} 1}{\sum_{\substack{5 \leq p \leq (c-1), \\ p \mid (c-1)}} 1} = 1$ or $\lim_{(c+1) \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq (c+1), \\ p \mid (c+1)}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq (c+1), \\ p \mid (c+1)}} 1} = \lim_{(c+1) \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq (c+1), \\ p \mid (c+1)}} 1}{\sum_{\substack{5 \leq p \leq (c+1), \\ p \mid (c+1)}} 1} = 1$; and so $\text{Avg } M_{c-1=pt}^{(2)}(p) = 1$ or $\text{Avg } M_{c+1=pt}^{(2)}(p) = 1$. Similarly, since from Theorem ?? we know $M_c^{(2)}(p) = 2$ or 0 for any prime p such that $p \mid c$ or p such that $c \not\equiv \pm 1, 0 \pmod{p}$ respectively, we then obtain $\lim_{c \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq c, \\ p \mid c}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq c, \\ p \mid c}} 1} = 2$ or $\lim_{c \rightarrow \infty} \frac{\sum_{\substack{5 \leq p \leq c, \\ c \not\equiv \pm 1, 0 \pmod{p}}} M_c^{(2)}(p)}{\sum_{\substack{5 \leq p \leq c, \\ c \not\equiv \pm 1, 0 \pmod{p}}} 1} = 0$, resp.; and so $\text{Avg } M_{c=pt}^{(2)}(p) = 2$ or $\text{Avg } M_{c \not\equiv \pm 1, 0 \pmod{p}}^{(2)}(p) = 0$, respectively. This then completes the whole proof, as required. \square

Remark 4.4. As before, we again note that from arithmetic statistics to arithmetic dynamics, Corollary ?? shows that any polynomial map $\varphi_{p-1,c}$ iterated on $\mathbb{Z}/p\mathbb{Z}$ has on average one or two or no 2-periodic orbits as $c \rightarrow \infty$; a somewhat interesting average phenomenon coinciding precisely with an averaging phenomenon remarked in [[?], Rem. 4.4] on the average number of distinct fixed orbits of any map $\varphi_{p-1,c}$ iterated on $\mathbb{Z}/p\mathbb{Z}$.

5 On the Density of Monic Integer Polynomials $\varphi_{p,c}(x)$ with the Number $N_c^{(2)}(p) = p$

In this section, we wish to ask and determine: “For a prime integer $p \geq 3$, what is the density of monic integer polynomials $\varphi_{p,c}(x) = x^p + c$ with p distinct 2-periodic integral points modulo p ?” The following corollary shows that there are very few integer polynomials $\varphi_{p,c}(x) = x^p + c$ with p distinct 2-periodic integral points modulo p :

Corollary 5.1. *Let $p \geq 3$ be a prime integer. Then the density of monic polynomials $\varphi_{p,c}(x) = x^p + c \in \mathbb{Z}[x]$ with the number $N_c^{(2)}(p) = p$ exists and is equal to 0% as $c \rightarrow \infty$. More precisely, we have*

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} = 0.$$

Proof. Since the defining condition $N_c^{(2)}(p) = p$ is as we proved in Theorem ??, determined whenever the coefficient c is divisible by any prime $p \geq 3$, hence, we may count $\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}$ by counting the number $\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } p \mid c \text{ for any fixed } c\}$. In that case, we then have

$$\frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} = \frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } p \mid c \text{ for any fixed } c\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}}.$$

So now, for any fixed positive integer $c \geq 3$, we then also have that the number

$$\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } p \mid c\} = \#\{p : 3 \leq p \leq c \text{ and } p \mid c\} = \sum_{3 \leq p \leq c, p \mid c} 1 = \omega(c),$$

where the counting function $\omega(c)$ is the number of distinct prime factors of c . Moreover, rewriting the number $\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\} = \sum_{3 \leq p \leq c} 1 = \pi(c)$, where $\pi(\cdot)$ is the prime-counting function, we then obtain

$$\frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } p \mid c \text{ for any fixed } c\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} = \frac{\omega(c)}{\pi(c)}.$$

Now recall from analytic number theory that for any positive integer c , we have $2^{\omega(c)} \leq \sigma(c) \leq 2^{\Omega(c)}$, where $\sigma(c)$ is the divisor function and $\Omega(c)$ counts the total number of prime factors of c , with respect to their multiplicity. So now taking logarithms, we then see that the inequality $2^{\omega(c)} \leq \sigma(c) \leq 2^{\Omega(c)}$ yields $\omega(c) \leq \frac{\log \sigma(c)}{\log 2}$; and hence yielding that $\frac{\omega(c)}{\pi(c)} \leq \frac{\log \sigma(c)}{\log 2 \cdot \pi(c)}$. Moreover, for all $\epsilon > 0$, we know $\sigma(c) = o(c^\epsilon)$ and so $\log \sigma(c) = \log o(c^\epsilon)$, which then yields that $\frac{\omega(c)}{\pi(c)} \leq \frac{\log o(c^\epsilon)}{\log 2 \cdot \pi(c)}$. But now for any fixed ϵ , if we take limit on both sides of the foregoing inequality as $c \rightarrow \infty$, we then obtain that $\lim_{c \rightarrow \infty} \frac{\log o(c^\epsilon)}{\log 2 \cdot \pi(c)} = 0$ and so we have $\lim_{c \rightarrow \infty} \frac{\omega(c)}{\pi(c)} \leq 0$. Hence, we have

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} \leq 0.$$

Moreover, we also observe that $\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\} \geq 1$, and so the quantity

$$\frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} \geq \frac{1}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} = 0.$$

Hence, we see $\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} \geq 0$ and which when combined with the above limit, we then obtain $\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = p\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} = 0$. This completes the whole proof, as desired. \square

Note that we may also interpret Corollary ?? as saying that the probability of choosing randomly a monic integer polynomial $\varphi_{p,c}(x)$ in the space $\mathbb{Z}[x]$ with exactly p distinct 2-periodic integral points modulo p is zero; a somewhat interesting probabilistic phenomenon coinciding with a phenomenon remarked in [[?], Sect. 5] on the probability of choosing randomly a monic $\varphi_{p,c}(x) \in \mathbb{Z}[x]$ with exactly three fixed integral points modulo p .

6 On Densities of Monic Integer Polynomials $\varphi_{p-1,c}(x)$ with $M_c^{(2)}(p) = 1$ & $M_c^{(2)}(p) = 2$

In this section, motivated by: “For a prime integer $p \geq 5$, what is the density of monics $\varphi_{p-1,c}(x) \in \mathbb{Z}[x]$ with two distinct 2-periodic points modulo p ?” we then also prove that the density of such monics $\varphi_{p-1,c}(x)$ is zero:

Corollary 6.1. *Let $p \geq 5$ be a prime integer. The density of monic polynomials $\varphi_{p-1,c}(x) = x^{p-1} + c \in \mathbb{Z}[x]$ with the number $M_c^{(2)}(p) = 2$ exists and is equal to 0% as $c \rightarrow \infty$. More precisely, we have*

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } M_c^{(2)}(p) = 2\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} = 0.$$

Proof. By applying the same reasoning as in the Proof of Corollary ??, we then obtain the limit as desired. \square

As before, we may also interpret Corollary ?? as saying that the probability of choosing randomly a monic polynomial $\varphi_{p-1,c}(x) = x^{p-1} + c$ in the space $\mathbb{Z}[x]$ with two distinct 2-periodic integral points modulo p is zero; a somewhat interesting probabilistic phenomenon coinciding with a phenomenon remarked in [[?], Sect. 6] on the probability of choosing randomly a monic $\varphi_{p-1,c}(x) \in \mathbb{Z}[x]$ with two distinct fixed integral points modulo p .

We also have the following corollary showing that the probability of choosing randomly a monic integer polynomial $\varphi_{p-1,c}(x) = x^{p-1} + c \in \mathbb{Z}[x]$ with only one 2-periodic integral point modulo p exists and is also zero:

Corollary 6.2. *Let $p \geq 5$ be a prime integer. The density of monic polynomials $\varphi_{p-1,c}(x) = x^{p-1} + c \in \mathbb{Z}[x]$ with the number $M_c^{(2)}(p) = 1$ exists and is equal to 0% as $c \rightarrow \infty$. More precisely, we have*

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } M_c^{(2)}(p) = 1\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} = 0.$$

Proof. As before, $M_c^{(2)}(p) = 1$ is as we proved in Theorem ??, determined whenever the coefficient c is such that $c \pm 1$ is divisible by any fixed prime $p \geq 5$; and so we may count $\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } M_c^{(2)}(p) = 1\}$ by simply counting the number $\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid (c \pm 1) \text{ for any fixed } c\}$. But now, since $c - 1 < c$, then if the number $\#\{p : 5 \leq p \leq c \text{ and } p \mid (c - 1)\} < \#\{p : 5 \leq p \leq c \text{ and } p \mid c\}$, we then obtain that

$$\frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid (c-1) \text{ for any fixed } c\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} < \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid c \text{ for any fixed } c\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}}.$$

Letting c tend to infinity on both sides of the above inequality and then applying Corollary ??, we then obtain

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid (c-1)\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} \leq \lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid c\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} = 0;$$

from which it then follows that

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } M_c^{(2)}(p) = 1\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} = 0, \text{ and hence showing the limit as desired in this case.}$$

Otherwise, if the number $\#\{p : 5 \leq p \leq c \text{ and } p \mid c\} < \#\{p : 5 \leq p \leq c \text{ and } p \mid (c - 1)\}$, we then have that

$$\frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid c \text{ for any fixed } c\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} < \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p \mid (c-1) \text{ for any fixed } c\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}}.$$

So now, taking limit as $c \rightarrow \infty$ on both sides of the above inequality and applying Corollary ?? and then applying a similar argument as in the Proof of Corollary ?? to obtain an upper bound zero, we then obtain

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p|(c-1)\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} = 0 = \lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } p|(c+1)\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}}$$

where the second limit follows from also observing $c < c+1$ and then applying an argument that is very similar to the one that has been given in the case when $c-1 < c$. This then completes the whole proof, as needed. \square

7 On Density of Integer Monics $\varphi_{p,c}(x)$ with $N_c^{(2)}(p) = 0$ and $\varphi_{p-1,c}(x)$ with $M_c^{(2)}(p) = 0$

Recall in Corollary ?? that a density of 0% of monic integer (and hence rational) polynomials $\varphi_{p,c}(x)$ have p distinct 2-periodic points modulo p ; and so the density of polynomials $\varphi_{p,c}^2(x) - x \in \mathbb{Z}[x]$ that are reducible modulo p is 0%. So now, we also wish to determine: “For a prime $p \geq 3$, what is the density of polynomials $\varphi_{p,c}(x) \in \mathbb{Z}[x]$ with no 2-periodic integral points modulo p ?” The following corollary shows that the probability of choosing randomly a polynomial $\varphi_{p,c}(x) \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(\varphi_{p,c}^2(x) - x)$ is a degree- p^2 number field is 1:

Corollary 7.1. *Let $p \geq 3$ be a prime integer. Then the density of monic polynomials $\varphi_{p,c}(x) = x^p + c \in \mathbb{Z}[x]$ with the number $N_c^{(2)}(p) = 0$ exists and is equal to 100% as $c \rightarrow \infty$. More precisely, we have*

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c \text{ and } N_c^{(2)}(p) = 0\}}{\#\{\varphi_{p,c}(x) \in \mathbb{Z}[x] : 3 \leq p \leq c\}} = 1.$$

Proof. Since the number $N_c^{(2)}(p) = p$ or 0 for any given prime integer $p \geq 3$ and since we also proved the density in Corollary ??, we then obtain the desired density (i.e., we obtain that the limit exists and is equal to 1). \square

Note that the foregoing corollary also shows that there are infinitely many polynomials $\varphi_{p,c}(x)$ over $\mathbb{Z} \subset \mathbb{Q}$ such that for $f(x) = \varphi_{p,c}^2(x) - x = (x^p + c)^p - x + c$, the quotient $K_f = \mathbb{Q}[x]/(f(x))$ induced by f is a number field of odd degree p^2 . Comparing the densities in Corollaries ?? and ??, one may then observe that in the whole family of monic integer polynomials $\varphi_{p,c}(x) = x^p + c$, almost all such monics have no 2-periodic integral points modulo p ; from which it then follows that almost all monic integer polynomials $f(x)$ are irreducible over \mathbb{Q} . This may then imply that the average value of $N_c^{(2)}(p)$ in the whole family of monic polynomials $\varphi_{p,c}(x)$ is zero.

We also recall in Cor. ?? or ?? that a density of 0% of monic integer (and thus rational) polynomials $\varphi_{p-1,c}(x)$ have $M_c^{(2)}(p) = 2$ or 1, resp.; and so the density of polynomials $\varphi_{p-1,c}^2(x) - x \in \mathbb{Z}[x]$ that are reducible modulo p is 0%. We now ask: “For a prime $p \geq 5$, what is the density of monic polynomials $\varphi_{p-1,c}(x) \in \mathbb{Z}[x]$ with no 2-periodic integral points (mod p)?” The corollary below shows that the probability of choosing randomly a polynomial $\varphi_{p-1,c}(x) = x^{p-1} + c \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(\varphi_{p-1,c}^2(x) - x)$ is a number field of degree $(p-1)^2$ is 1:

Corollary 7.2. *Let $p \geq 5$ be a prime integer. The density of monic polynomials $\varphi_{p-1,c}(x) = x^{p-1} + c \in \mathbb{Z}[x]$ with the number $M_c^{(2)}(p) = 0$ exists and is equal to 100% as $c \rightarrow \infty$. More precisely, we have*

$$\lim_{c \rightarrow \infty} \frac{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c \text{ and } M_c^{(2)}(p) = 0\}}{\#\{\varphi_{p-1,c}(x) \in \mathbb{Z}[x] : 5 \leq p \leq c\}} = 1.$$

Proof. Recall that $M_c^{(2)}(p) = 1, 2$ or 0 for any given prime $p \geq 5$ and since we also proved the densities in Corollary ?? and ??, we now obtain the desired density (i.e., we get that the limit exists and is equal to 1). \square

As before, Corollary ?? also shows that there are infinitely many monic polynomials $\varphi_{p-1,c}(x)$ over $\mathbb{Z} \subset \mathbb{Q}$ such that for $g(x) = \varphi_{p-1,c}^2(x) - x = (x^{p-1} + c)^{p-1} - x + c$, the quotient $L_g = \mathbb{Q}[x]/(g(x))$ induced by g is a number field of even degree $(p-1)^2$. Again, if we compare the densities in Cor. ??, ?? and ??, we may then see that in the whole family of polynomials $\varphi_{p-1,c}(x) = x^{p-1} + c \in \mathbb{Z}[x]$, almost all such monics have no 2-periodic integral points modulo p ; and from which it then also follows that almost all monics $g(x) \in \mathbb{Z}[x]$ are irreducible over \mathbb{Q} . But this may also imply that the average value of $M_c^{(2)}(p)$ in the whole family of polynomials $\varphi_{p-1,c}(x)$ is zero.

Recall more generally from algebraic number theory that any number field K is always naturally equipped with a ring \mathcal{O}_K of integers in K ; and which is classically known to describe the arithmetic of K , but usually very difficult to compute in practice. So now, in our case here, it then follows that K_f has a ring of integers \mathcal{O}_{K_f} , and moreover we also have the following corollary showing that the probability of choosing randomly a polynomial $f(x) = (x^p + c)^p - x + c \in \mathbb{Z}[x]$ such that $\mathbb{Z}[x]/(f(x))$ is the ring of integers of K_f , is $\approx 60.7927\%$:

Corollary 7.3. *Assume Corollary ?? . When monic integer polynomials $f(x)$ are ordered by height $H(f)$ as defined in [?], the density of such polynomials $f(x)$ such that $\mathbb{Z}[x]/(f(x))$ is the ring of integers of K_f is $\zeta(2)^{-1}$.*

Proof. Since from Corollary ?? we know that there are infinitely many monic polynomials $f(x)$ over \mathbb{Z} (and hence over \mathbb{Q}) such that the quotient ring $K_f = \mathbb{Q}[x]/(f(x))$ is an algebraic number field of degree $\deg(f) = p^2$; and moreover associated to K_f is the ring of integers \mathcal{O}_{K_f} . This then means that the set of irreducible monic integer polynomials $f(x) = (x^p + c)^p - x + c \in \mathbb{Z}[x]$ such that K_f is an algebraic number field of odd degree p^2 is not empty. So now, applying here a theorem of Bhargava-Shankar-Wang [[?], Theorem 1.2] to the underlying family of monic integer polynomials $f(x)$ ordered by height $H(f)$ as defined in [?] such that $\mathcal{O}_{K_f} = \mathbb{Z}[x]/(f(x))$, it then follows that the density of such polynomials $f(x) \in \mathbb{Z}[x]$ is equal to $\zeta(2)^{-1} \approx 60.7927\%$ as needed. \square

As with K_f , every number field L_g induced by a polynomial g , is naturally equipped with the ring of integers \mathcal{O}_{L_g} , and which may also be very difficult to compute in practice. In this case, we again take great advantage of [[?], Thm. 1.2] to then show in the following corollary that the probability of choosing randomly a monic $g(x) = (x^{p-1} + c)^{p-1} - x + c \in \mathbb{Z}[x]$ such that $\mathbb{Z}[x]/(g(x))$ is the ring of integers of L_g is also $\approx 60.7927\%$:

Corollary 7.4. *Assume Corollary ?? . When monic integer polynomials $g(x)$ are ordered by height $H(g)$ as defined in [?], the density of such polynomials $g(x)$ such that $\mathbb{Z}[x]/(g(x))$ is the ring of integers of L_g is $\zeta(2)^{-1}$.*

Proof. By applying the same reasoning as in the Proof of Corollary ??, we then obtain the density as desired. \square

8 On the Number of Number fields K_f & L_g with Bounded Absolute Discriminant

Recall we saw from Corollary ?? that there is an infinite family of irreducible monic integer polynomials $f(x) = (x^p + c)^p - x + c$ such that the field K_f induced by f is an algebraic number field of odd degree $n = p^2$. Moreover, we also saw from Corollary ?? that one can always find an infinite family of irreducible monic integer polynomials $g(x) = (x^{p-1} + c)^{p-1} - x + c$ such that the field extension L_g over \mathbb{Q} induced by g is an algebraic number field of even degree $r = (p-1)^2$. Moreover, from standard theory of number fields, we may associate to K_f (resp., L_g) an integer $\text{Disc}(K_f)$ (resp., $\text{Disc}(L_g)$) called the discriminant. So now, inspired by number field-counting advances in arithmetic statistics, we then wish to study the problem of counting number fields. To do so, we wish to define and then understand the asymptotic behavior of the following counting functions

$$N_n(X) := \#\{K_f/\mathbb{Q} : [K_f : \mathbb{Q}] = n \text{ and } |\text{Disc}(K_f)| \leq X\} \quad (3)$$

$$M_r(X) := \#\{L_g/\mathbb{Q} : [L_g : \mathbb{Q}] = r \text{ and } |\text{Disc}(L_g)| \leq X\} \quad (4)$$

as a positive real number $X \rightarrow \infty$. To this end, motivated greatly by great work of Lemke Oliver-Thorne [?] on counting number fields and then applying [[?], Theorem 1.2 (1)] on the function $N_n(X)$, we then obtain:

Corollary 8.1. *Assume Corollary ??, and let $N_n(X)$ be the number defined as in (??). Then we have*

$$N_n(X) \ll_n X^{2d - \frac{d(d-1)(d+4)}{6n}} \ll X^{\frac{8\sqrt{n}}{3}}, \text{ where } d \text{ is the least integer for which } \binom{d+2}{2} \geq 2n+1. \quad (5)$$

Proof. To see inequality (??), we first recall from Corollary ?? the existence of infinitely many irreducible monic polynomials $f(x) \in \mathbb{Q}[x]$ such that the field K_f/\mathbb{Q} induced by f is an algebraic number field of degree $n = p^2$. This then means that the set of algebraic number fields K_f/\mathbb{Q} of odd degree n is not empty. Now applying [[?], Theorem 1.2 (1)] on the number $N_n(X)$, we then obtain immediately the upper bound, as indeed needed. \square

Motivated again by the same work of Lemke Oliver-Thorne [?], we again take great advantage of the first part of [[?], Theorem 1.2] by applying it on $M_r(X)$. In doing so, we then obtain the following corollary:

Corollary 8.2. *Assume Corollary ??, and let $M_r(X)$ be the number defined as in (??). Then we have*

$$M_r(X) \ll_r X^{2d - \frac{d(d-1)(d+4)}{6r}} \ll X^{\frac{8\sqrt{r}}{3}}, \text{ where } d \text{ is the least integer for which } \binom{d+2}{2} \geq 2r+1. \quad (6)$$

Proof. By applying a similar argument as in the Proof of Cor. ??, we then obtain the desired inequality (??). \square

We recall more generally that an algebraic number field K is called “*monogenic*” if there exists an algebraic number $\alpha \in K$ such that the ring \mathcal{O}_K of integers is the subring $\mathbb{Z}[\alpha]$ generated by α over \mathbb{Z} , i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$. So now, recall from the foregoing Corollary ?? that we counted number fields K_f with absolute discriminant $|\Delta(K_f)| < X$. Still in the same direction of counting number fields, we now wish to count monogenic number fields K_f with $|\Delta(K_f)| < X$ and such that the associated Galois group $\text{Gal}(K_f/\mathbb{Q})$ is the symmetric group S_{p^2} . To do so, we as in [?] take great advantage of Bhargava-Shankar-Wang’s result [[?], Cor. 1.3] and then obtain:

Corollary 8.3. *Assume Corollary ??. Then the number of isomorphism classes of algebraic number fields K_f of odd degree p^2 and with $|\Delta(K_f)| < X$ that are monogenic and have associated Galois group S_{p^2} is $\gg X^{\frac{1}{2} + \frac{1}{p^2}}$.*

Proof. By Cor. ??, it then also follows that there are infinitely many monic polynomials $f(x)$ over \mathbb{Z} (and so over \mathbb{Q}) such that the quotient K_f induced by f is an algebraic number field of odd degree p^2 . This then means that the set of algebraic number fields K_f/\mathbb{Q} of odd degree p^2 is not empty. So now, applying [[?], Cor. 1.3] to the underlying number fields K_f with $|\Delta(K_f)| < X$ that are monogenic and have associated Galois group S_{p^2} , we then obtain that the number of isomorphism classes of such number fields K_f is $\gg X^{\frac{1}{2} + \frac{1}{p^2}}$ as desired. \square

As before, we again take great advantage of Bhargava-Shankar-Wang’s result [[?], Cor. 1.3] to then also count in the following corollary the number of algebraic number fields L_g that are monogenic with absolute discriminant $|\Delta(L_g)| < X$ and such that the associated Galois group $\text{Gal}(L_g/\mathbb{Q})$ is the symmetric group $S_{(p-1)^2}$:

Corollary 8.4. *Assume Corollary ??. The number of isomorphism classes of algebraic number fields L_g of even degree $(p-1)^2$ and $|\Delta(L_g)| < X$ that are monogenic and have associated Galois group $S_{(p-1)^2}$ is $\gg X^{\frac{1}{2} + \frac{1}{(p-1)^2}}$.*

Proof. By applying the same reasoning as in the Proof of Corollary ??, we then obtain the count as desired. \square

9 On Number of Algebraic Number fields K_f & L_g with Prescribed Class Number

Recall from algebraic number theory that for any number field K with ring of integers \mathcal{O}_K , we then define the “*ideal class group*” $\text{Cl}(\mathcal{O}_K)$ of a number field K (also usually denoted as $\text{Cl}(K)$) to be the quotient of a free abelian group $\text{I}(\mathcal{O}_K)$ of all fractional ideals in K by a subgroup $\text{P}(\mathcal{O}_K)$ of all principal fractional ideals in K . It is a well-known fact that $\text{Cl}(\mathcal{O}_K) = \text{I}(\mathcal{O}_K)/\text{P}(\mathcal{O}_K)$ is an abelian group, and moreover $\text{Cl}(\mathcal{O}_K)$ is finite. The order of this group $\text{Cl}(\mathcal{O}_K)$ is called the “*class number*” of K (usually denoted as h_K). Though $\text{Cl}(\mathcal{O}_K)$ is classically known to provide a way of measuring how far the ring of integers \mathcal{O}_K is from being a unique factorization domain and moreover also known to be finite, computing $\text{Cl}(\mathcal{O}_K)$ in practice let alone determine precisely h_K , is a well-known hard problem in algebraic and analytic number theory and even more so in arithmetic statistics.

So now, recall from Corollary ?? that there is an infinite family of irreducible monic integer polynomials $f(x) = (x^p + c)^p - x + c$ such that K_f is an algebraic number field of odd degree p^2 . Moreover, in light of the foregoing discussion, we then also have an invariant $\text{Cl}(K_f)$ associated to each K_f and moreover h_{K_f} is finite. So now, inspired by work on class groups of number fields in arithmetic statistics and in particular by remarkable work of Ho-Shankar-Varma [?] on odd degree number fields with odd class number, we then also wish to count here the number of number fields K_f with associated Galois group S_{p^2} and with prescribed class number. To do so, we take great advantage of a nice theorem of Ho-Shankar-Varma [[?], Theorem 4(a)] to then obtain the following corollary on the existence of infinitely many S_{p^2} -number fields K_f with odd class number:

Corollary 9.1. *Assume Corollary ??, and let $n = p^2$ be any fixed odd integer. Then there exist infinitely many S_n -algebraic number fields K_f of odd degree n having odd class number. More precisely, we have*

$$\#\{K_f : |\Delta(K_f)| < X \text{ and } 2 \nmid |\text{Cl}(K_f)|\} \gg X^{\frac{n+1}{2n-2}},$$

where the implied constants depend on degree n and on an arbitrary finite set S of primes as given in [?].

Proof. From Cor. ??, it follows that the family of number fields K_f of degree $n = p^2$ is not empty. Now since n is an odd integer, we then see that the claim follows from [[?], Thm. 4(a)] by setting $K_f = K$ as needed. \square

As before, we may also recall from Corollary ?? the existence of an infinite family of irreducible monic integer polynomials $g(x) = (x^{p-1} + c)^{p-1} - x + c$ such that the quotient $L_g = \mathbb{Q}[x]/(g(x))$ induced by g is an algebraic number field of even degree $(p-1)^2$. But now as before we may also observe that to each such obtained number field L_g , we can also associate a finite group $\text{Cl}(L_g)$ and so h_{L_g} is finite. So now, by taking again great advantage of work on class groups of number fields in arithmetic statistics and in particular the nice

work of Siad [?] on S_n -number fields K of any even degree $n \geq 4$ and signature (r_1, r_2) where r_1 are the real embeddings of K and r_2 are the pairs of conjugate complex embeddings of K , we then also obtain the following:

Corollary 9.2. *Assume Corollary ??, and let $n = (p - 1)^2$ be an even integer. Then there are infinitely many monogenic S_n -algebraic number fields L_g of even degree n and any signature (r_1, r_2) having odd class number.*

Proof. To see this, we note that by Cor. ??, it follows that the family of number fields L_g of degree $n = (p - 1)^2$ is not empty. Now since n is even, we then note that the claim follows from [[?], Cor. 10] as indeed needed. \square

Acknowledgments

I'm truly grateful and deeply indebted to my long-time great advisors, Dr. Ilia Binder and Dr. Arul Shankar, for all their boundless generosity, friendship, and along with Dr. Jacob Tsimerman for everything. As a graduate research student, this work and my studies are hugely and wholeheartedly funded by Dr. Binder and Dr. Shankar. Any opinions expressed gladly in this article belong solely to me, the author, Brian Kintu; and should never be taken as a reflection of the views of anyone that has been very happily acknowledged by the author.

References

- [1] D. Adam and Y. Fares. On two affine-like dynamical systems in a local field. *J. Number Theory*. 132, 132, (2012), 2892-2906.
- [2] R L. Benedetto. Preperiodic points of polynomials over global fields. *J. Reine Angew. Math.*, 608:123–153, 2007.
- [3] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *Journal of the Amer. Math. Soc.*, Vol. 33(4), (2020), pp. 1087-1099.
- [4] M. Bhargava, A. Shankar, and X. Wang. Squarefree values of polynomial discriminants I. *Invent. Math.*, Vol. 228, (2022), pp. 1-37.
- [5] G S. Call and S W. Goldstine. Canonical heights on projective space. *J. Number Theory*, 63(2):211–243, 1997.
- [6] Robert L. Devaney. *An introduction to chaotic dynamical systems*. Addison-Wesley Studies in Nonlinearity. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, second edition, 1989.
- [7] J R. Doyle, X. Faber, and D. Krumm. Preperiodic points for quadratic polynomials over quadratic fields. *New York J. Math.*, 20:507–605, 2014.
- [8] S. Eliahou and Y. Fares. Poonen’s conjecture and Ramsey numbers. *Discrete Appl. Math.*, 209:102–106, 2016.
- [9] S. Eliahou and Y. Fares. Some results on the Flynn-Poonen-Schaefer conjecture. *Canadian Math. Bull.*, 65(3):598-611, 2022.
- [10] R. J. Lemke Oliver and F. Thorne. Upper bounds on number fields of given degree and bounded discriminant. *Duke Math. J.*, Vol. 171, No. 15, (2022), pp. 1-11.
- [11] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90(3):435–463, 1997.
- [12] W. Ho, A. Shankar, and I. Varma. Odd degree number fields with odd class number. *Duke Math. Journal.*, Vol. 167(5), (2018), pp. 1-53.
- [13] B. Hutz. Determination of all rational preperiodic points for morphisms of PN. *Math. Comp.*, 84(291):289–308, 2015.
- [14] B. Hutz and P. Ingram. On Poonen’s conjecture concerning rational preperiodic points of quadratic maps. *Rocky Mountain J. Math.*, 43(1):193–204, 2013.
- [15] B. Kintu. *Counting the number of 2-periodic \mathbb{Z}_p - and $\mathbb{F}_p[t]$ -points of a discrete dynamical system with applications from arithmetic statistics, VI*. In preparation.
- [16] B. Kintu. *Counting the number of 2-periodic \mathcal{O}_K -points of a discrete dynamical system with applications from arithmetic statistics, V*. In preparation.

- [17] B. Kintu. *Counting the number of integral fixed points of a discrete dynamical system with applications from arithmetic statistics, I*. <https://arxiv.org/abs/2501.04026>, pp. 1-14.
- [18] B. Kintu. *Counting the number of \mathbb{Z}_p - and $\mathbb{F}_p[t]$ -fixed points of a discrete dynamical system with applications from arithmetic statistics, III*. <https://arxiv.org/pdf/2505.24565>, pp. 1-25.
- [19] J.-P. Massias and G. Robin. Bornes effectives pour certaines fonctions concernant les nombres premiers. *Journal Th. Nombres de Bordeaux*, Vol. 8, (1996), 215–242.
- [20] P. Morton. Arithmetic properties of periodic points of quadratic maps. II. *Acta Arith.*, 87(2):89–102, 1998.
- [21] P. Morton and J H. Silverman. Rational periodic points of rational functions. *Internat. Math. Res. Notices*, (2):97–110, 1994.
- [22] W. Narkiewicz. Cycle-lengths of a class of monic binomials. *Functiones et Approximatio*, 42.2(suppl. 2):S65–S70, (2010), 163-168.
- [23] W. Narkiewicz. On a class of monic binomials. *Proc. Steklov Inst. Math.*, 280(suppl. 2):S65–S70, 2013.
- [24] D. G. Northcott. Periodic points on an algebraic variety. *Ann. of Math. (2)*, 51:167–177, 1950.
- [25] C. Panraksa. Rational periodic points of $x^d + c$ and fermat-catalan equations. *Internat. J. of Number Theory*, 18(05):1111–1129, 2022.
- [26] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over \mathbf{Q} : a refined conjecture. *Math. Z.*, 228(1):11–29, 1998.
- [27] A. Siad. *Monogenic fields with odd class number Part II: even degree*. <https://arxiv.org/pdf/2011.08842>, pp. 1-49.
- [28] M. Stoll. Rational 6-cycles under iteration of quadratic polynomials. *LMS J. Comput. Math.*, 11:367–380, 2008.
- [29] R. Walde and P. Russo. Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$. *Amer. Math. Monthly*, 101(4):318–331, 1994.

Dept. of Math. and Comp. Sciences (MCS), University of Toronto, Mississauga, Canada

E-mail address: **brian.kintu@mail.utoronto.ca**

June 30, 2025