Math. Res. Lett.
Volume 22, Number 01, 141–168, 2015

On the Fixed Points of the Map $x \mapsto x^x$ Modulo a Prime

Pär Kurlberg, Florian Luca and Igor E. Shparlinski

In this paper, we show that for almost all primes p there is an integer solution $x \in [2, p-1]$ to the congruence $x^x \equiv x \pmod p$. The solutions can be interpretated as fixed points of the map $x \mapsto x^x \pmod p$, and we study numerically and discuss some unexpected properties of the dynamical system associated with this map.

1. Introduction

1.1. Motivation

For a prime p, we consider the properties of the map

$$\psi_p : x \mapsto x^x \pmod p,$$

when it acts on the integers $x \in [1, p-1]$. By the results Crocker [5] and Somer [18], there are at least $\left\lfloor \sqrt{(p-1)/2} \right\rfloor$ and at most $3p/4 + O(p^{1/2+o(1)})$, respectively, distinct values of $x^x \pmod p$ when $1 \le x \le p-1$.

We also note that various estimates depending on the multiplicative order modulo p of a on the number $T(p, a)$ of solutions of the congruence

$$x^x \equiv a \pmod p, \quad 1 \le x \le p-1, \tag{1}$$

have been given in [1, 2]. In the most favorable case of $a = 1$, by Balog et al. [1, Corollary 5], we have

$$T(p, 1) \le p^{1/3+o(1)} \tag{2}$$

as $p \to \infty$. Furthermore, by Balog et al. [1, Bound (2)], for any integer a we have $T(p, a) \le p^{11/12+o(1)}$. Moreover, it is also shown in [1, Theorem 8] that the estimate

$$\#\{1 \le x, y \le p-1 \ : \ x^x \equiv y^y \pmod p\} \le p^{48/25+o(1)}$$

holds as $p \to \infty$.

The map ψ_p also appears in some cryptographic protocols (see [12, Sections 11.70 and 11.71]), so it certainly deserves more attention. Several conjectures and numerical data concerning this map can be found in [8].

Here, we address an apparently new problem and study the fixed points of the map ψ_p. Let $F(p)$ denotes the number of fixed points of the map ψ_p. That is,

$$F(p) = \#\{1 \le x \le p-1 \ : \ x^x \equiv x \pmod p\}.$$

Obviously $x = 1$ is always a fixed point, which we call *trivial*. We show that for most primes p the map ψ_p has a *non-trivial* fixed point $x \in [2, p-1]$. Thus, we are interested in primes p with $F(p) > 1$. In the opposite direction, it has been noted in [1, Theorem 8] that the method used to prove (2) also applies to the congruence $x^{x-1} \equiv 1 \pmod p$, and thus it implies the bound

$$F(p) \le p^{1/3+o(1)} \tag{3}$$

as $p \to \infty$.

We also study the quantity $F(p)$ and other dynamical properties (such as the period statistics) of the map ψ_p numerically. In particular, these numerical results reveal that a naïve point of view of treating ψ_p as a "random" function on the set $\{1, \dots, p-1\}$ is totally wrong. In particular, the numerical results significantly deviate from those predicted for truly random maps by the work of Flajolet and Odlyzko [6]. These results indicate that ψ_p tends to have shorter orbits and more fixed points than a random map even after removing the trivial fixed point $x = 1$. On the other hand, it is highly likely that the bound (3) is very far from being tight. We give some partial explanation for the "non-randomness" phenomenon, and introduce the notion of *random endomorphisms* in groups, which allows us to give some qualitative explanation for the numerical results. We consider developing a rigorous analysis of the random endomorphisms to be a challenging and important open topic.

Finally, in Section 5, we study the map $x \to x^{f(x)} \pmod p$ for general polynomials $f(X) \in \mathbb{Z}[X]$, and show that such a map can have at most $p^{6/13+o(1)}$ fixed points, as $p \to \infty$.

1.2. Notation

Before we give the precise statement we introduce some notation.

We define $\log x$ as $\log x = \max\{\ln x, 2\}$ where $\ln x$ is the natural logarithm. Furthermore, for an integer $k \geq 2$, we define recursively $\log_k x = \log(\log_{k-1} x)$.

Throughout the paper, we use the Landau symbols O and o and the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings. We recall that $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent to the fact that $|A| < cB$ holds with some constant c, while $A = o(B)$ means that $A/B \to 0$.

We further define the logarithmic integral

$$\mathrm{li}\,(N) = \int_2^N \frac{dt}{\log t}.$$

We always use p and q for prime numbers. We also use $\varphi(k)$ and $\omega(k)$ to denote the Euler function and the number of distinct prime divisors of an integer k.

Furthermore, $\mathbb{F}_p$ denotes a finite field of p elements, which we consider to be represented by the elements of the set $\{0, \ldots, p-1\}$, while $\mathbb{Z}/n\mathbb{Z}$ denotes the residue ring modulo an integer $n \geq 1$. In particular, it is convenient to consider the map ψ_p as acting on $\mathbb{F}_p$.

1.3. Heuristics on primes without non-trivial fix points

Let us write $\mathcal{A}$ for the set of prime numbers p for which ψ_p does not have a non-trivial fixed point $x \in [2, p-1]$:

$$\mathcal{A} = \{p \text{ prime} \ : \ F(p) = 1\}.$$

One easily finds that $\mathcal{A}$ is not empty. In particular, among the first 1000 primes, there are precisely 72 of them in $\mathcal{A}$. The first few elements of $\mathcal{A}$ are

$$3,\ 5,\ 7,\ 11,\ 53,\ 59,\ 83,\ 107,\ 179,\ 227,\ 269,\ \ldots \tag{4}$$

Quite likely, the set $\mathcal{A}$ is infinite, but we have not been able to prove this unconditionally. However, we can show this under some standard conjectures about prime numbers. For example, assume that

$$p \equiv 3 \pmod 8 \qquad \text{and} \qquad p - 1 = 2q, \tag{5}$$

where q is the prime (several elements from the above list (4): 11, 59, 83, 107, 179, 227, are of this form). Consider an integer solution x to $x^{x-1} \equiv 1 \pmod p$. Then the multiplicative order of x divides $x-1$, which is an integer less than $p-1$. However, this multiplicative order must also divide $p-1 = 2q$. So, the only possibilities are that the order of x is either 2 or q. If it is 2, then $x = 1$ (which is excluded) or $x = p-1$, which is not a fixed point as $\psi_p(p-1) = 1$. If it is q, then $q \mid x-1$, and since $x-1 < 2q$, we get that $x - 1 = q$, so $x = q + 1 = (p+1)/2$. Thus, we arrive at

$$1 \equiv x^{x-1} \equiv ((p+1)/2)^{(p-1)/2} \equiv 2^{-(p-1)/2} \equiv 2^{(p-1)/2} \pmod p,$$

by Fermat's Little theorem, which, in particular, implies that 2 is a quadratic residue modulo p. But, this is impossible as $p \equiv 3 \pmod 8$.

Standard conjectures then suggest that $\mathcal{A}$ is infinite, and, in fact, putting

$$\mathcal{A}(N) = \mathcal{A} \cap [1, N],$$

the standard heuristic on the density of primes p satisfying (5) makes us conjecture that the inequality

$$\#\mathcal{A}(N) > c_0 N/(\log N)^2$$

holds for all $N \geq 3$ with some positive constant c_0.

In Section 3, we give some further heuristic arguments suggesting that the stronger inequality

$$\#\mathcal{A}(N) \geq \frac{N}{(\log N)^2} \exp\left((1/\ln 2 + o(1)) \log_3 N \log_4 N\right) \tag{6}$$

holds as $N \to \infty$. In fact, in Section 3.1, we also give a heuristic argument that the "likelyhood" of ψ_p having no non-trivial fix points is of order $\exp(-\gamma(p) \cdot \tau(p-1))$, where $\tau(p-1)$ denotes the number of divisors of $p-1$ and $\gamma(p)$ is some explicit but quite irregular function of p taking values in $(0, 1)$; see (6) for more details. In particular, we expect that ψ_p is very likely to have non-trivial fixed points unless the number of prime factors of $p - 1$ is very small.

1.4. Main result

We obtain an unconditional result in the opposite direction of the previous heuristics, in the sense that $\mathcal{A}$ is fairly sparse. In particular, the estimate

$\#\mathcal{A}(N) = o(\pi(N))$ holds as $N \to \infty$, where, as usual, for a positive real number x we use $\pi(x)$ to denote the number of primes $p \le x$.

Let

$$\vartheta = \frac{1}{\zeta(2)} - \frac{1}{2\zeta(2)^2} = \frac{6\pi^2 - 18}{\pi^4} \simeq 0.4231\ldots, \tag{7}$$

where $\zeta(s)$ is the Riemann zeta-function.

Theorem 1. *We have*

$$\#\mathcal{A}(N) \le \frac{\pi(N)}{(\log_3 N)^{\vartheta + o(1)}}$$

as $N \to \infty$.

Our proof is based on an effective version of the Chebotarev density theorem that is due to Lagarias and Odlyzko [11].

2. Proof of Theorem 1

2.1. The strategy

Observe that a non-trivial fixed point corresponds to a solution of the congruence

$$x^{x-1} \equiv 1 \pmod p, \quad x \in \{2, 3, \ldots, p-1\}. \tag{8}$$

Thus, we wish to show that for almost all primes p the congruence (8) has a solution.

Given a prime p such that a "small" prime q divides $p-1$, we write $p - 1 = q \cdot a$, so $a = (p-1)/q$. For an integer x of the form $x = 1 + a\beta$, with $\beta \in \{1, \ldots, q-1\}$, we have

$$x^{x-1} \equiv (1 + a\beta)^{a\beta} \equiv (1 - \beta/q)^{\beta(p-1)/q} \pmod p.$$

Hence, we obtain a valid solution if $1 - \beta/q \equiv (q-\beta)/q \pmod p$ is a qth power modulo p for some $0 < \beta < q$. In other words, with $n = q - \beta$, we find that

$$x = 1 + a\beta = 1 + \frac{1}{q}(p-1)(q-n) \in [2, p-1]$$

is a solution to (8) provided that n/q is a qth power modulo p. Thus, it suffices to show that there exists a qth power modulo p of the form n/q with $n \in [1, q-1]$.

Note that the chance of a random element in the finite field of p elements $\mathbb{F}_p$ being a qth power equals $1/q$. So, heuristically, assuming that the set of qth powers has sufficiently random behavior, we can expect that the probability of this *not* happening is $(1-1/q)^{q-1} = 1/e + o(1)$ as $q \to \infty$.

The strategy we adopt is thus to consider primes $p \equiv 1 \pmod q$ for "many", say k, "small" (but not "too small") primes q; the "probability" that all such q fail to provide a valid solution x to the original congruence is expected to be about e^{-k}, *provided* that we can show that almost all primes p have such a property. We do this though not in a direct way. In particular, for the "individual" probability of q to fail we only obtain an upper bound of $1 - \vartheta = 0.576\ldots$ rather than $1/e = 0.367\ldots$.

2.2. The Chebotarev density theorem

We let $\mathbb{L}$ be a finite Galois extension of $\mathbb{Q}$ with Galois group G of degree $d = [\mathbb{L} : \mathbb{Q}]$ and discriminant Δ. Let $\mathcal{C}$ be a union of conjugacy classes of G. We define

$$\pi_{\mathcal{C}}(N, \mathbb{L}/\mathbb{Q}) = \#\{p \le N \ : \ p \text{ unramified in } \mathbb{L}/\mathbb{Q}, \ \sigma_p \in \mathcal{C}\},$$

where σ_p is the Artin symbol of p in the extension $\mathbb{L}/\mathbb{Q}$ (see [7]).

A combination of a version of the Chebotarev density theorem due to Lagarias and Odlyzko [11] with a bound of Stark [19] for a possible Siegel zero, yields the following result (see also [14, Lemma 6]).

Lemma 2. *There are absolute constants $A_1, A_2 > 0$ such that if*

$$\log N \ \ge \ 10d(\log|\Delta|)^2, \tag{9}$$

then

$$\begin{aligned} &\left|\pi_{\mathcal{C}}(N, \mathbb{L}/\mathbb{Q}) - \frac{\#\mathcal{C}}{\#G}\mathrm{li}\,(N)\right| \\ &\qquad \ll \frac{\#\mathcal{C}}{\#G}\mathrm{li}\left(N^{\beta}\right) + |\mathcal{C}| N \exp\left(-A_1\sqrt{\frac{\log N}{d}}\right) \end{aligned} \tag{10}$$

with some β satisfying the inequality

$$\beta \ < \ 1 - \frac{A_2}{\max\{|\Delta|^{1/d}, \log|\Delta|\}},$$

where $|\mathcal{C}|$ is the number of conjugacy classes in $\mathcal{C}$.

Winckler [21] has recently obtained a version of Lemma 2 with fully explicit constants.

2.3. Some preliminaries on Kummer extensions

Let q be prime. We note that

$$\{p \le N : p \equiv 1 \pmod q,\ n/q \text{ is a } q\text{th power modulo } p\}$$

is, apart from the $O(\log(qn))$ ramified primes all dividing qn, equal to the set of primes $p \le N$ such that p splits completely in the Kummer extension $\mathbb{K}_{q,n} = \mathbb{L}_q(\sqrt[q]{n/q})$, where $\mathbb{L}_q = \mathbb{Q}(\zeta_q)$ is the cyclotomic extension generated by the primitive qth root of unity $\zeta_q = \mathbf{e}^{2\pi i/q}$. Note further that the condition that p splits completely in $\mathbb{L}_q$ is equivalent to $p \equiv 1 \pmod q$.

The ideas behind our argument can be outlined as follows. Note that choosing a prime ideal $P \mid p$ in the ring of integers of $\mathbb{L}_q$ essentially amounts to choosing a non-trivial qth root of unity in $\mathbb{F}_p$. Moreover, having made such a choice, the action of the Artin map $\sigma_{P,n} \in \mathrm{Gal}(\mathbb{K}_{q,n}/\mathbb{L}_q)$ (note that this Galois group is Abelian) allows us, via Kummer theory, to associate with an integer n a canonical element in $\mathbb{Z}/q\mathbb{Z}$; furthermore, this allows us to make "compatible" choices of elements in $\mathbb{Z}/q\mathbb{Z}$ associated with different integers n.

To fix the ideas, let g be a non-trivial qth root modulo p. By Kummer theory, we can then find "compatible" integers $x_0, x_1, x_2, \ldots, x_{q-1}$ modulo q such that $g^{x_0} \in q \cdot (\mathbb{F}_p^\times)^q$, and $g^{x_n} \in n \cdot (\mathbb{F}_p^\times)^q$ for $n = 1, 2, \ldots, q-1$ (where $(\mathbb{F}_p^\times)^q$ is the set of qth powers in $\mathbb{F}_p^\times$ and $\lambda \cdot (\mathbb{F}_p^\times)^q$ denotes the element-wise multiplication).

Note that knowledge of x_k for all *prime* $k < q$, determines x_n modulo q for n *composite*. Moreover, the condition that n/q is not a qth power for all $n \in [1, q-1]$ is equivalent to $x_n \not\equiv x_0 \pmod q$ for $1 \le n \le q-1$.

2.4. A system of linear forms modulo q

Motivated by the arguments of Section 2.3, we study a system of certain linear equations modulo q. Let $d = \pi(q-1)$, and given an integer $n \in [1, q-1]$, define a linear form $\mathcal{L}_n : \mathbb{F}_q^d \to \mathbb{F}_q$ by

$$\mathcal{L}_n(\mathbf{v}) = \sum_{i=1}^{d} \alpha_{i,n} v_i,$$

where $\mathbf{v} = (v_1, \ldots, v_d)$ and the coefficients $\{\alpha_{i,n}\}$ are read from the prime factorization

$$n = \prod_{i=1}^{d} p_i^{\alpha_{i,n}}.$$

Given $x_0 \in \mathbb{F}_q$, we study

$$N_q = \#\{\mathbf{v} \in \mathbb{F}_q^d \ : \ \mathcal{L}_n(\mathbf{v}) \neq x_0 \text{ for all } n \in \{1, 2, \ldots, q-1\}\}.$$

For q large, it seems reasonable to expect that N_q should be of size q^d/e since, for a fixed non-zero vector $\mathbf{v}$, the "probability" that $\mathcal{L}_n(\mathbf{v}) \neq x_0$ for all n *if the forms are randomly chosen*, equals $(1 - 1/q)^{q-1} \simeq 1/e$. Equivalently, if we define

$$c(q) = N_q/q^d,$$

we expect that $c(q) = 1/e + o(1)$ as $q \to \infty$.

While we are not able to prove that $c(q)$ approaches $1/e$ as q becomes large, we prove a weaker upper bound which is sufficient for our purposes.

Lemma 3. *As q tends to infinity, we have*

$$c(q) \leq 1 - \vartheta + o(1),$$

where ϑ is given by (7).

Proof. For $n > 1$, the linear form $\mathcal{L}_n$ is non-trivial and the equation $\mathcal{L}_n(\mathbf{v}) = x_0$ has at least one solution; hence exactly q^{d-1} solutions. Further, given two *square-free* integers $2 \leq m < n < q$, we note that the corresponding linear forms $\mathcal{L}_n$ and $\mathcal{L}_m$ are independent. Thus, there are exactly q^{d-2} solutions $\mathbf{v}$ to

$$\mathcal{L}_n(\mathbf{v}) = \mathcal{L}_m(\mathbf{v}) = x_0.$$

Let M denotes the number of square-free positive integers up to q. Thus, we have $M = (1/\zeta(2) + o(1))q$ as $q \to \infty$.

To obtain an upper bound, we discard the condition that $\mathcal{L}_n(\mathbf{v}) \neq x_0$ for non-squarefree n. Then, removing those $\mathbf{v}$ for which $\mathcal{L}_n(\mathbf{v}) = x_0$ for some square-free n, and adding back in vectors $\mathbf{v}$ for which $\mathcal{L}_n(\mathbf{v}) = \mathcal{L}_m(\mathbf{v}) = x_0$ for pairs of distinct square-free m, n (in essence, truncating the inclusion–exclusion principle at the third step), we find that

$$N_q \leq q^d - Mq^{d-1} + \binom{M}{2} q^{d-2} = q^d(1 - 1/\zeta(2) + 1/(2\zeta(2)^2) + o(1)),$$

as $q \to \infty$, and the result follows. □

2.5. Independence of field extensions

For a prime $q \mid Q$ we consider the algebraic number field

$$\mathbb{K}_q = \mathbb{Q}(\zeta_q, \sqrt[q]{2}, \sqrt[q]{3}, \sqrt[q]{5}, \ldots, \sqrt[q]{q});$$

that is, we adjoin the qth roots of the unity and the qth roots of the primes $p \le q$ to $\mathbb{Q}$.

Assume that Q is a product of k distinct primes $q_1, \ldots, q_k$. We define

$$\mathbb{K}_Q = \mathbb{K}_{q_1} \circ \mathbb{K}_{q_2} \circ \cdots \circ \mathbb{K}_{q_k}$$

to be the composite field obtained from the fields $\mathbb{K}_q$ as q ranges over the prime divisors of Q.

Lemma 4. *Assume that Q is an* **odd** *integer. Then the field extensions $\mathbb{L}_q(\sqrt[q]{\ell})/\mathbb{L}_q$ are linearly disjoint as (q, ℓ) ranges over pairs of primes such that $\ell \le q$ and $q \mid Q$.*

Proof. We break the argument in two steps.

First, we show that if q is fixed, then $\mathbb{L}_q(\sqrt[q]{\ell})/\mathbb{L}_q$ are linearly disjoint once ℓ ranges over primes $\ell \le q$. If this is not so, then there exist $s \ge 2$ primes $\ell_1, \ldots, \ell_s$ such that $\mathbb{L}_q \subsetneq \mathbb{K}$ where

$$\mathbb{K} = \mathbb{L}_q(\sqrt[q]{\ell_1}, \ldots, \sqrt[q]{\ell_{s-1}}) \cap \mathbb{L}_q(\sqrt[q]{\ell_s}).$$

Observe that $\mathbb{K}/\mathbb{Q}$ is normal as an intersection of normal extensions. We show that $\mathbb{K} = \mathbb{L}_q(\sqrt[q]{\ell_s})$. Indeed, if this is not so, then, by Galois theory, the group $\mathrm{Gal}(\mathbb{L}_q(\sqrt[q]{\ell_s})/\mathbb{K})$ is a proper non-trivial normal subgroup of $\mathrm{Gal}(\mathbb{L}_q(\sqrt[q]{\ell_s})/\mathbb{L}_q)$, but this last group has order q, a prime number. This shows that $\mathbb{K} = \mathbb{L}_q(\sqrt[q]{\ell_s})$. So,

$$\mathbb{L}_q(\sqrt[q]{\ell_s}) \subseteq \mathbb{L}_q(\sqrt[q]{\ell_1}, \ldots, \sqrt[q]{\ell_{s-1}}). \tag{11}$$

The discriminant of the field on the left is divisible only by the primes q and ℓ_s, while the discriminant of the field on the right is divisible by the primes q and $\ell_1, \ldots, \ell_{s-1}$. We get an immediate contradiction unless $\ell_s = q$. So, it remains to treat the case $\ell_s = q$. If $s = 2$, then we get

$$\mathbb{L}_q(\sqrt[q]{q}) \subseteq \mathbb{L}_q(\sqrt[q]{\ell_1}).$$

Since both extensions above have the same degree $q(q-1)$ over $\mathbb{Q}$, it follows that the above containment is in fact an equality. This is false because ℓ_1 ramifies in the field on the right but not in the field on the left.

Assume now that $s \geq 3$ is minimal such that containment (11) holds for some prime $q = \ell_s$ and some primes $\ell_1 < \cdots < \ell_{s-1} < q$. Further, by the minimality of s, $\sqrt[q]{q}$ cannot belong to any field of the type $\mathbb{Q}(\zeta_q, \sqrt[q]{\ell_{i_1}}, \ldots, \sqrt[q]{\ell_{i_t}})$ for some proper subset $\{i_1, \ldots, i_t\}$ of $\{1, \ldots, s-1\}$. Thus, we get a relation of the type

$$\sqrt[q]{q} = R_0 + R_1 \sqrt[q]{\ell_{s-1}} + \cdots + R_{q-1}(\sqrt[q]{\ell_{s-1}})^{q-1},$$

where $R_i = S_i(\zeta_q, \sqrt[q]{\ell_1}, \ldots, \sqrt[q]{\ell_{s-2}})$ for some

$$S_i(X_0, X_1, \ldots, X_{s-2}) \in \mathbb{Q}[X_0, \ldots, X_{s-2}]$$

and at least one of $R_1, \ldots, R_{q-1}$ is non-zero. Hence, $\sqrt[q]{\ell_{s-1}}$ is an algebraic number of degrees at most $q-1$ over the normal field

$$\mathbb{Q}(\zeta_q, \sqrt[q]{q}, \sqrt[q]{\ell_1}, \ldots, \sqrt[q]{\ell_{s-2}}).$$

Since $\mathbb{Q}(\ell_s^{1/q})$ is in fact of prime degree q over $\mathbb{Q}$, we get that

$$\sqrt[q]{\ell_{s-1}} \in \mathbb{Q}(\zeta_q, \sqrt[q]{q}, \sqrt[q]{\ell_1}, \ldots, \sqrt[q]{\ell_{s-2}}),$$

giving

$$\mathbb{Q}(\sqrt[q]{\ell_{s-1}}) \subseteq \mathbb{Q}(\zeta_q, \sqrt[q]{q}, \sqrt[q]{\ell_1}, \ldots, \sqrt[q]{\ell_{s-2}}).$$

However, this last field inclusion is false because the discriminant of the field on the left is divisible by the prime ℓ_{s-1}, while the discriminant of the field on the right is divisible only by primes $\ell_1, \ldots, \ell_{s-2}$ and q.

We next show that the fields $\mathbb{K}_q$ are linearly disjoint as q varies over the prime factors of Q. Again assume that this is not so and conclude that there exist $s \geq 2$ prime factors of Q denoted $q_1 < \cdots < q_s$ such that

$$\mathbb{Q} \subset \mathbb{K} = \mathbb{K}_{q_1} \cdots \mathbb{K}_{q_{s-1}} \cap \mathbb{K}_{q_s}.$$

Observe that all prime factors dividing the order of the Galois group of $\mathbb{K}_{q_s}/\mathbb{Q}$ divide $q_s(q_s-1)$, while the Galois group of $\mathbb{K}_{q_1} \cdots \mathbb{K}_{q_{s-1}}$ has order divisible only by primes dividing $q_1(q_1-1)\cdots q_{s-1}(q_{s-1}-1)$. Thus, the order of the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, as a factor group of $\mathrm{Gal}(\mathbb{K}_{q_s}/\mathbb{Q})$, can be divisible only by primes dividing $q_s - 1$.

The subgroup $\mathrm{Gal}(\mathbb{K}_{q_s}/\mathbb{K})$ is normal, so by the above observation on possible prime divisors of its order, must contain the q_s-Sylow subgroup of $\mathrm{Gal}(\mathbb{K}_{q_s}/\mathbb{Q})$, which is isomorphic to $(\mathbb{Z}/q_s\mathbb{Z})^{\pi(q_s)}$. However, the Galois group $\mathrm{Gal}(\mathbb{K}_{q_s}/\mathbb{Q})$ is isomorphic to a semi-direct product of $\mathbb{Z}/(q_s-1)\mathbb{Z}$ with $(\mathbb{Z}/q_s)^{\pi(q_s)}$, where the first cyclic group acts diagonally as the group of automorphisms of $\mathbb{Z}/q_s\mathbb{Z}$. It is not hard to see that in the Galois group $\mathrm{Gal}(\mathbb{K}_{q_s}/\mathbb{Q})$, the q_s-Sylow subgroup is maximal normal. This shows, via Galois correspondence between subgroups and subfields, that $\mathrm{Gal}(\mathbb{K}_{q_s}/\mathbb{K})$ is the q_s-Sylow subgroup, so $\mathbb{K} = \mathbb{L}_{q_s}$ is the cyclotomic field.

In particular, $\mathbb{K}$ contains the q_sth roots of unity and hence the discriminant of $\mathbb{K}$ is divisible by q_s — a, which is impossible since the discriminant of $\mathbb{K}_{q_1}\cdots\mathbb{K}_{q_{s-1}}$ is divisible only by primes up to q_{s-1}.

Altogether, this shows that the field extensions $\mathbb{L}_q(\sqrt[q]{\ell})/\mathbb{L}_q$ are indeed linearly disjoint as (q,ℓ) ranges over pairs of primes such that $\ell \le q$, thereby concluding the proof. □

2.6. Estimating the degree and discriminant of $\mathbb{K}_Q$

We keep the notations from Section 2.5. Put d_Q and Δ_Q for the degree and discriminant of $\mathbb{K}_Q$, respectively.

Lemma 5. *The bounds*

(i) $d_Q \le \exp(q_k^2)$,

(ii) $\Delta_Q \le \exp(\exp(2q_k^2))$

hold for large enough k.

Proof. It is clear that $\mathbb{K}_Q$ is the compositum of

$$n = (\pi(q_1)+1) + (\pi(q_2)+1) + \cdots + (\pi(q_k)+1) < \frac{q_k^2}{\log q_k} \tag{12}$$

fields $\mathbb{K}_{i,j} = \mathbb{Q}(r_i^{1/q_j})$, where $r_i \in \{1\} \cup \{p \le q_j\}$ and $j = 1,\ldots,k$, each of degree at most q_k. The inequality (12) above holds for large k. Thus, (i) follows. For (ii), observe that the discriminant of each of $\mathbb{K}_{i,j}$ is at most $q_k^{2q_k}$. Label these fields in some way as $\mathbb{K}_1,\ldots,\mathbb{K}_n$ and let $\mathbb{L}_j = \mathbb{K}_1 \circ \mathbb{K}_2 \circ \cdots \circ \mathbb{K}_j$

for $j = 1, \ldots, n$. Note that $\mathbb{L}_{j+1} = \mathbb{L}_j \circ \mathbb{K}_{j+1}$, therefore

$$\Delta_{\mathbb{L}_{j+1}} \le \Delta_{\mathbb{L}_j}^{[\mathbb{K}_{j+1}:\mathbb{Q}]} \cdot \Delta_{\mathbb{K}_{j+1}}^{[\mathbb{L}_j:\mathbb{Q}]}.$$

Since $[\mathbb{K}_{j+1} : \mathbb{Q}] \le q_k$, $[\mathbb{L}_j : \mathbb{Q}] \le q_k^j$ and $\Delta_{\mathbb{K}_j} \le q_k^{2q_k}$, we conclude that if we put λ_j for some constant such that $\Delta_{\mathbb{L}_j} \le q_k^{\lambda_j q_k^j}$, then the inequalities

$$\lambda_1 \le 2 \quad \text{and} \quad \lambda_{j+1} \le \lambda_j + 2$$

hold for $j = 1, \ldots, n-1$. Hence, $\lambda_j \le 2j$ for $j = 1, \ldots, n$. With $j = n$, we obtain

$$\Delta_Q \le q_k^{2nq_k^n} < \exp(\exp(2q_k^2))$$

for all large k, thus proving (ii). □

2.7. Some technical estimates

For a square-free integer S, we define

$$c(S) = \prod_{q|S} c(q).$$

For positive integers L and R with $Q = LR$, define

$$\mathcal{P}_{L,R}(N) = \{p \le N \ : \ \gcd(p-1, Q) = L\}$$

and

$$\widetilde{\mathcal{P}}_{L,R}(N) = \{p \in \mathcal{P}_{L,R}(N) \ : \ n/q \notin (\mathbb{F}_p^\times)^q \text{ for all } q \mid L \text{ and } 0 < n < q\}.$$

Lemma 6. *If*

$$6q_k^2 < \log_2 N, \tag{13}$$

then for square-free relatively prime integers L and R we have

$$\#\widetilde{\mathcal{P}}_{L,R}(N) \ll \pi(N) \cdot \frac{c(L)}{\varphi(L)} \cdot \prod_{q|R} \left(\frac{q-2}{q-1}\right). \tag{14}$$

Proof. This follows from the Chebotarev density theorem. More precisely, a prime p counted by $\#\widetilde{\mathcal{P}}_{L,R}(N)$ has the following property: $p \equiv 1 \pmod q$

for each prime $q \mid L$ and for all $1 \le n < q$, n/q is not a qth power in $\mathbb{F}_p^\times$. So we now concentrate on the counting function, say denoted by $T_{L,R}(N)$, for such primes, for which in fact one can easily derive an asymptotic formula from the Chebotarev density theorem.

Indeed, in terms of the image of the Frobenius map, the relative size of the corresponding conjugacy classes in $\mathrm{Gal}(\mathbb{K}_q/\mathbb{Q})$, is given by $c(q)$ (see Section 2.4). Since by Lemma 4, the field extensions $\mathbb{K}_{q_i}$ are linearly disjoint for $i = 1, \ldots, k$, the relative size inside $\mathrm{Gal}(\mathbb{K}_L/\mathbb{Q})$ is given by $c(L)$. This takes care of the main term in the asymptotic formula for $T_{L,R}(N)$.

For the error term, we appeal to Lemmas 2 and 5. More precisely, by Lemma 5, we have

$$10 d_Q (\log \Delta_Q)^2 < 10 \exp(5q_k^2)) < \log N$$

for large k by the assumption (13), so the inequality (9) holds. As for error terms, we have

$$d_Q \le \exp(q_k^2) < (\log N)^{1/6}$$

so the second error term in (10) is negligible with respect to the main term. Finally, we note that the first error term in (10) is at most comparable with the main term and it could be incorporated into it given that (14) is only an upper bound estimate. □

We now set

$$Q_t = \prod_{t<q\le e^t} q. \tag{15}$$

Thus, Q has $k = \pi(e^t) - \pi(t)$ prime factors labeled $q_1, \ldots, q_k$. The inequality (13) is satisfied for this choice of Q provided that N is large and

$$t = \frac{1}{3} \log_3 N. \tag{16}$$

We get the following result.

Lemma 7. *If N is large and* (16) *holds, then*

$$\#\mathcal{P}_{1,Q_t}(N) \ll \frac{\pi(N) \log_4 N}{\log_3 N}.$$

Proof. By the Brun sieve [20, Theorem 3, Section I.4.2], and on recalling Mertens formula [20, Section I.1.5], we have

$$\#\{p \le N \ : \ \gcd(p-1, Q_t) = 1\} \ll \pi(N) \prod_{q \mid Q_t} \left(\frac{q-2}{q-1}\right) \ll \frac{\pi(N) \log t}{t},$$

and the result now follows from (16). □

2.8. Concluding the proof

We assume that Q_t is given by (15) where t is given by (16). In particular, the conditions of Lemmas 6 and 7 are satisfied.

By Lemma 6, we have

$$\sum_{LR=Q_t,\ L>1} \#\widetilde{\mathcal{P}}_{L,\ R}(N) \ll \pi(N) \sum_{LR=Q_t,\ L>1} \frac{c(L)}{\varphi(L)} \cdot \prod_{q \mid R} \left(\frac{q-2}{q-1}\right). \tag{17}$$

Furthermore,

$$\begin{aligned}
\sum_{\substack{LR=Q_t\\ L>1}} \frac{c(L)}{\varphi(L)} \cdot \prod_{q \mid R} \left(\frac{q-2}{q-1}\right) &= \prod_{q \mid Q_t} \left(\frac{q-2}{q-1}\right) \sum_{\substack{LR=Q_t\\ L>1}} \frac{c(L)}{\varphi(L)} \cdot \prod_{q \mid L} \frac{q-1}{q-2}\\
&= \prod_{q \mid Q_t} \left(\frac{q-2}{q-1}\right) \sum_{\substack{LR=Q_t\\ L>1}} c(L) \cdot \prod_{q \mid L} \frac{1}{q-2}\\
&\le \prod_{q \mid Q_t} \left(\frac{q-2}{q-1}\right) \sum_{L \mid Q_t} \prod_{q \mid L} \left(\frac{c(q)}{q-2}\right)\\
&= \prod_{q \mid Q_t} \left(\frac{q-2}{q-1}\right) \prod_{q \mid Q_t} \left(1 + \frac{c(q)}{q-2}\right)\\
&= \prod_{q \mid Q_t} \left(1 - \frac{1-c(q)}{q-1}\right).
\end{aligned}$$

Thus, recalling (17), we obtain

$$\sum_{LR=Q_t, L>1} \#\widetilde{\mathcal{P}}_{L,R}(N) \ll \pi(N) \prod_{q \mid Q_t} \left(1 - \frac{1-c(q)}{q-1}\right).$$

Using Lemma 3 and then the Mertens formula again, we obtain

$$\begin{aligned}\prod_{q \mid Q_t} \left(1 - \frac{1-c(q)}{q-1}\right) &\ll \exp\left(-\sum_{q \mid Q_t} \frac{1-c(q)}{q}\right) \\ &\ll \exp\left(-(\vartheta + o(1)) \sum_{q \mid Q_t} \frac{1}{q}\right) \\ &= \exp\left(-(\vartheta + o(1)) \log t\right) = \frac{1}{(\log_3 N)^{\vartheta + o(1)}}\end{aligned}$$

and so

$$\sum_{LR = Q_t, L > 1} \#\widetilde{\mathcal{P}}_{L,R}(N) \le \frac{\pi(N)}{(\log_3 N)^{\vartheta + o(1)}}$$

as $N \to \infty$. With Lemma 7, we finally get that

$$\begin{aligned}\#\mathcal{A}(N) &\ll \#\mathcal{P}_{1,Q_t}(N) + \sum_{LR = Q_t, L > 1} \#\widetilde{\mathcal{P}}_{L,R}(N) \\ &\ll \pi(N) \left(\frac{\log_4 N}{\log_3 N} + \frac{1}{(\log_3 N)^{\vartheta + o(1)}}\right)\end{aligned}$$

as $N \to \infty$, which finishes the proof.

3. Further remarks on $\#\mathcal{A}(N)$

3.1. Heuristic arguments

Recall that $x = 1$ is always a trivial fixed point, and note that $x = p - 1$ is never a fixed point. Hence, we only consider x whose multiplicative order is greater than two, and the exponent $x - 1$ ranging over integers in the interval $[1, p - 3]$.

If $d \mid p - 1$ and x are a primitive dth root of unity *and* we make the assumption that the exponent $x - 1$ is "independent" of x, the "chance" that $x^{x-1} \equiv 1 \pmod p$ equals the chance that $d \mid x - 1$; this occurs with probability

$$\frac{\lfloor (p-3)/d \rfloor}{p-3} = \frac{(p-1)/d - 1}{p-3} = 1/d + O(1/p). \tag{18}$$

Letting x range over the set of $\varphi(d)$ primitive dth roots of unity, the probability that $x^{x-1} \not\equiv 1 \pmod p$ for all of them, assuming independence, equals

$$\left(1 - \frac{\lfloor (p-3)/d \rfloor}{p-3}\right)^{\varphi(d)}.$$

Moreover, with the further assumption of independence when d ranges over divisors of $p-1$, this suggests that

$$\#\mathcal{A}(N) = (1+o(1))H(N)$$

as $N \to \infty$, where

$$H(N) = \sum_{p<N} \prod_{\substack{d \mid p-1 \\ 2<d<p-1}} \left(1 - \frac{\lfloor (p-3)/d \rfloor}{p-3}\right)^{\varphi(d)}. \tag{19}$$

For p fixed (but large) we similarly find that the heuristic probability of the map ψ_p having no (non-trivial) fixed points, using that

$$\left(1 - \left(\frac{1}{d} + O(p^{-1})\right)\right)^{\varphi(d)} = \exp\left(\varphi(d) \ln\left(1 - \left(\frac{1}{d} + O(p^{-1})\right)\right)\right)$$

is given by $\exp(-\Delta_p)$, where

$$\begin{aligned}
\Delta_p &= - \sum_{\substack{d \mid p-1 \\ 2<d<p-1}} \varphi(d) \ln\left(1 - \left(\frac{1}{d} + O(p^{-1})\right)\right) \\
&= \sum_{\substack{d \mid p-1 \\ 2<d<p-1}} \varphi(d) \left(\frac{1}{d} + \frac{1}{2d^2} + O(p^{-1} + d^{-3})\right) \\
&= \sum_{d \mid p-1} \varphi(d) \left(\frac{1}{d} + \frac{1}{2d^2} + O(p^{-1} + d^{-3})\right) + O(1) \\
&= \tau(p-1) \cdot \prod_{q^e \| p-1} \left(1 - \frac{e}{(1+e)q}\right) + O\left(\sum_{d \mid p-1} 1/d\right),
\end{aligned} \tag{20}$$

where as usual, $q^e \| n$ means that $q^e \mid n$ but $q^{e+1} \nmid n$.

Hence, ψ_p is exceeding likely to have a non-trivial fixed point unless $p-1$ has rather few prime factors. Restricting to p such that $p-1$ is square-free, and, motivated by the results of Sathe [16] and Selberg [17], assuming that for any fixed $\varepsilon > 0$ and $k \le (2-\varepsilon)\log_2 N$, we have

$$\#\{p \le N \ : \ \omega(p-1) = k\} \sim \frac{N(\log_2 N)^{k-1}}{(k-1)! \log^2 N},$$

we expect that the number of $p \le x$ such that ψ_p has no non-trivial fixed point modulo p is, for any integer $k > 0$, is

$$H(N) \gg \sum_{p \le N} \exp(-\Delta_p) \ge \sum_{1 \le k \le (2-\varepsilon)\log_2 N} \frac{N(\log_2 N)^{k-1} \exp(-2^{k+o(k)})}{(k-1)! \log^2 N}.$$

Using the trivial estimate $1 \le (k-1)! \le k^k$ we see that $(k-1)!$ can be absorbed in $2^{k+o(k)}$ in the exponent. Furthermore, for any positive integer $k \le (2-\varepsilon)\log_2 N$ we have

$$H(N) \gg \frac{N \exp\left(k \log_3 N - 2^{k+o(k)}\right)}{(\log N)^2 \log_2 N}.$$

Thus, taking

$$k = \left\lfloor \left(\frac{1}{\ln 2} - \eta\right) \log_4 N \right\rfloor,$$

for an arbitrary $\eta > 0$ gives the bound

$$H(N) \ge \frac{N}{(\log N)^2} \exp\left((1/\ln 2 - \eta + o(1)) \log_3 N \log_4 N\right),$$

(note that using other admissible values of k does not significantly improve this bound; just one optimally chosen value suffices). Since $\eta > 0$ is arbitrary, we obtain the expected lower bound (6).

In fact we believe that the lower bound (6) is close to the actual order of magnitude of both $\#\mathcal{A}(N)$ and $H(N)$.

The above argument, in particular (18), also suggests that the expected value of the total number of non-trivial fixed points over all primes $p \le N$ is

$$\sum_{p \le N} F(p) = (1 + o(1))K(N),$$

where

$$K(N) = \sum_{p \le N} \sum_{\substack{d \mid p-1 \\ d > 2}} \frac{\varphi(d)}{d} = \sum_{d=3}^{N} \frac{\varphi(d)}{d} \sum_{\substack{p \le N \\ p \equiv 1 \pmod d}} 1. \tag{21}$$

Using the approximation

$$\sum_{\substack{p \le N \\ p \equiv 1 \pmod d}} 1 = (1 + o(1)) \frac{N}{\varphi(d) \log N},$$

it seems reasonable to expect that

$$K(N) = (1 + o(1))N.$$

3.2. Numerical results

In Table 1, we compare the observed data for all primes $p \le N$ for $N = 100,000 \cdot k$, $1 \le k \le 10$, that have no non-trivial fixed point with the heuristically predicted value $H(N)$ given by (19).

In Table 2, we present data for the total number of fixed points for all primes $p \le N$ for $N = 50,000 \cdot k$, $1 \le k \le 9$, that have no non-trivial fixed point, and compare it with the heuristically predicted value given by (21).

Table 1: Number of primes $p \le N$ with no non-trivial fixed point

N	Observed	Predicted	Relative error
100,000	567	585.6	−0.0318
200,000	1007	1020.6	−0.0134
300,000	1358	1421.4	−0.0446
400,000	1715	1790.1	−0.0419
500,000	2068	2151.8	−0.0389
600,000	2404	2490.0	−0.0345
700,000	2725	2826.7	−0.0360
800,000	3053	3151.0	−0.0311
900,000	3350	3479.5	−0.0372
1,000,000	3632	3796.2	−0.0433

Table 2: Total number of observed non-trivial fixed points for $p \le N$ versus random model prediction

N	Observed	Predicted	Relative error
500,000	$465,413$	410686.1	0.1333
1,000,000	$936,280$	831872.7	0.1255
1,500,000	$1,408,964$	1256499.5	0.1213
2,000,000	$1,883,411$	1683081.9	0.1190
2,500,000	$2,357,781$	2110954.9	0.1169
3,000,000	$2,832,933$	2539862.9	0.1154
3,500,000	$3,306,597$	2968852.5	0.1138
4,000,000	$3,780,495$	3398836.9	0.1123
4,500,000	$4,256,757$	3829903.3	0.1115

When comparing predicted and observed values we note that there seems to be a consistent negative bias in Table 1 and a consistent positive bias in Table 2. As of now, we have no satisfactory explanation of this phenomenon.

4. Remarks on the dynamics of the map ψ_p

4.1. Orbit length model

Given a finite set X, a map $\eta : X \to X$, and a starting point x_0, define $x_{n+1} = \eta(x_n)$ for $n \in \mathbb{Z}^+$. Let $O_{\eta,x_0}(X) = \{x_0, x_1, \ldots\}$ denote the forward orbit of x_0 under η. Clearly, we have the trivial inequality $\#O_{\eta,x_0}(X) \le \#X$, but if η is a *random map* (that is, for each $x \in X$, we define its image $\eta(x)$ by uniformly selecting a random element of X), a simple "birthday paradox" argument shows that $\#O_{\eta,x_0}(X)$ is very likely to be of size roughly $(\#X)^{1/2}$; in particular, as $\#X \to \infty$, $\#O_{\eta,x_0}(X) \le (\#X)^{1/2+o(1)}$ holds with probability one.

Thus, if we naïvely model ψ_p as a random map, then, as $p \to \infty$, and selecting a random starting point x_0, the orbit size $\# O_{\psi_p,x_0}(\mathbb{F}_p)$ is expected to be roughly of size $\sqrt{p}$, see [6]. However, numerics indicate that $\#O_{\psi_p,x_0}(\mathbb{F}_p)$ often is *much smaller* than $\sqrt{p}$. In fact, in what follows, we give numerical evidence, and an heuristic model, that the probability density distribution of $\log \# O_{\psi_p,x_0}(\mathbb{F}_p)/\log p$ has support in $[0, 1/2]$.

In fact, it is easy to see that the orbit $O_{\psi_p,x_0}(\mathbb{F}_p)$ are shorter than expected from a random map as once a certain element $x \in O_{\psi_p,x_0}(\mathbb{F}_p)$ lies in a multiplicative subgroup of $\mathbb{F}_p^*$, then so does $\psi_p(x)$, and the remaining part of the orbit never leaves this subgroup. So, the behavior of orbits of ψ_p, originating at a point $x_0 \in \mathbb{F}_p^*$ is ruled by two (apparently independent) factors:

- random map-like behavior inside of a subgroup of $\mathbb{F}_p^*$ which eventually leads to a cycle formed by the "birthday paradox" (see [6] for an exhaustive treatise of the structure of random maps);
- reducing the size of the multiplicative subgroup where the iterations of ψ_p get locked in as they progress along the trajectory.

For example, if the initial point x_0 is not a primitive root of $\mathbb{F}_p$, this immediately puts all elements of the corresponding trajectory in a non-trivial multiplicative subgroup of $\mathbb{F}_p^*$.

Hence, we believe that the main reason for such small orbit lengths is that a correct model for ψ_p is that of a *random automorphism* on C_{p-1}, the cyclic group of cardinality $p-1$. Since ψ_p maps $\mathbb{F}_p^\times$ into itself, and, as groups $\mathbb{F}_p^\times \simeq C_{p-1}$, we may translate the dynamics $x_0 \to x_1 \to \cdots$ on $\mathbb{F}_p^\times$ to dynamics $y_0 \to y_1 \to \cdots$ on C_{p-1}. Under the assumption that the discrete log map (which identifies $\mathbb{F}_p^\times$ with C_{p-1}) behaves randomly, the image of ψ_p as a map of C_{p-1} can be viewed as "random" map $\varphi : \ C_{p-1} \to C_{p-1}$ given by

$$\varphi(y) \equiv \alpha_y y \pmod{p-1},$$

where $\alpha_y \in \mathbb{Z}/(p-1)\mathbb{Z}$ is selected randomly. In particular, once an iterate y_n "lands" in a subgroup $H \subset C_{p-1}$, it never "leaves"; and this makes much shorter orbit lengths likely.

For example, for primes p such that $p-1 = s \cdot t$, where s is the $p^{1/3}$-smooth part of $p-1$, and $s \gg p^{1/3}$, we find that it is very likely that the s-part of the orbit gets annihilated after at most $p^{1/3+\varepsilon}$ steps (write $C_{p-1} \simeq C_s \times C_t$ and say that the s-part of y_n is annihilated if the image of y_n in $C_s \times C_t$ is of the form $(0, *)$.) In fact, if a prime q divides $p-1$, it is easy to see that the probability of the q-part not being annihilated after k steps is given by $(1-1/q)^k$, which, if $q/k = o(1)$, is $o(1)$ as $q \to \infty$.

This leads to the following natural question. Let $\Psi_{d,p}$ be the endomorphisms of $\mathbb{F}_p^*$, indexed by the divisors $d \in [1, p-1]$ and generated by the map $x \mapsto x^d$, $x \in \mathbb{F}_p^*$.

Question 8. *Let $x_0 \in \mathbb{F}_p^*$ be chosen uniformly at random and let $\Psi_{d_1,p}, \ldots,$ $\Psi_{d_L,p}$ be a sequence of L random endomorphisms such that for every $j =$*

$1, \ldots, L$ *and* $d \mid p-1$ *we have*

$$\Pr[(p-1, d_j) = d] = \frac{\varphi((p-1)/d)}{p-1}.$$

What is the expected size of the smallest subgroup of $\mathbb{F}_p^*$ *that contains the element* $\Psi_{d_L,p}(\ldots(\Psi_{d_L,p}(x_0))\ldots)$*?*

Certainly, a version of Question 8 can be asked for any finite subgroup.

4.2. Orbit length statistics

If a map η behaves sufficiently randomly, then the bound $\#O_{\eta,x_0}(\mathbb{F}_p) \le p^{1/2+o(1)}$ is very likely to hold. In fact, it is known that for η random, $(\#O_{\eta,x_0}(\mathbb{F}_p))^2/(2p)$ converges in distribution to a mean one exponential as $p \to \infty$. In particular, the support of $\log \# O_{\eta,x_0}(\mathbb{F}_p)/\log p$ is essentially concentrated around 1/2.

See Figure 1 for an illustration of this well-known phenomenon, which also forms the basis of the so-called *Pollard's rho-factorization* algorithm, see [4, Section 5.2.1].

However, the orbit sizes of ψ_p behave very differently.

We remark that if $p = 2q+1$, where q is a Sophie Germain prime, then the second effect is negligible. Since the standard heuristic suggests a (relative) abundance of Sophie Germain primes, "on average" over primes p, the second effect is essentially invisible. However for a "typical" prime

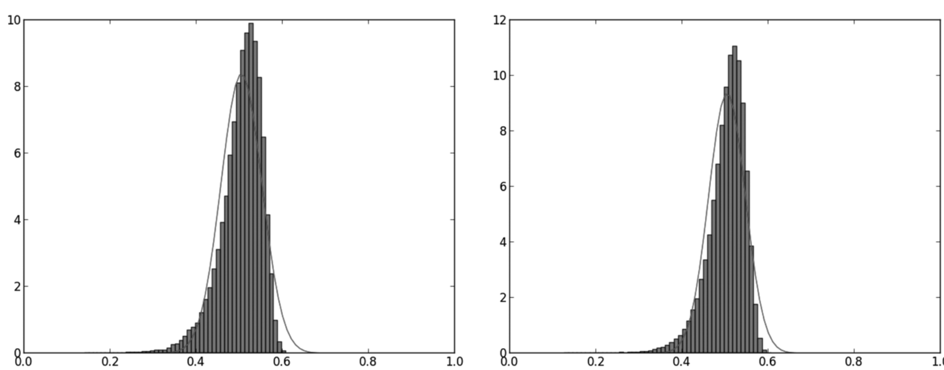

Figure 1: Histogram plot of $\log \#O_{\eta,x_0}(\mathbb{F}_p)/\log p$ with $\eta(x) = x^2+1$ for $p \le 1,000,000$ (left) and $p \le 5,000,000$ (right). Red curves indicate normal distributions with mean and variance fitted to the data

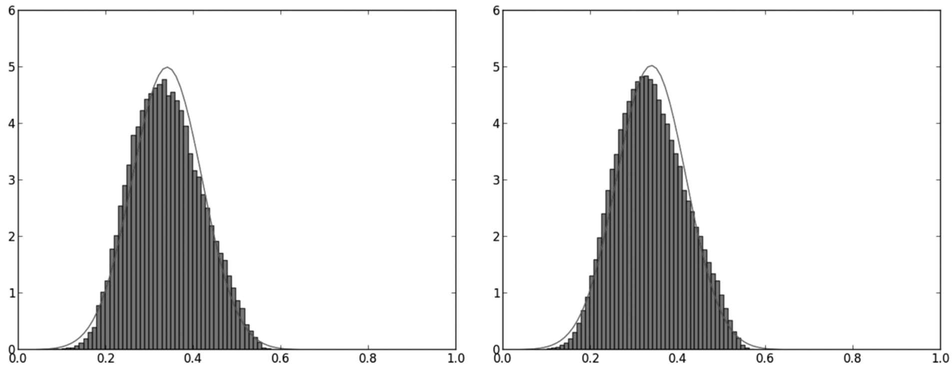

Figure 2: Histogram plots of $\log \#O_{\psi_p,x_0}(\mathbb{F}_p)/\log p$, $p \le 1,000,000$ (left) and $p \le 5,000,000$ (right). Red curves indicate normal distributions with mean and variance fitted to the data

the situation is quite different. In other words, under the standard heuristic expectation of abundance of Sophie Germain prime, the average value of the trajectory length is of order $p^{1/2}$ (possibly with some logarithmic factors), while the typical value is much smaller.

Furthermore, let $P(k)$ denote the largest prime divisor of an integer $k \ge 1$. If $\alpha \in (0,1)$ and p runs through a sequence of primes with $p-1 = q \cdot s$ where $q = P(p-1) = p^{\alpha+o(1)}$ and s is $p^{\alpha/2}$-smooth (which conjecturely holds for a positive proportion of the primes for any $\alpha \in (0,1)$), we expect that a random endomorphism has the orbit of size at most $p^{\alpha/2+o(1)}$. In turn, this suggests that the probability density function of $\log \#O_{\psi_p,x_0}(\mathbb{F}_p)/\log p$ is supported in the full interval $[0,1/2]$; see Figure 2 for an illustration of this phenomenon.

To further show the difference in orbit statistics, it is also interesting to compare statistics when normalized by dividing by $\sqrt{p}$, see Figure 3.

5. Comments and extensions

As we have mentioned in Section 2.4, it is natural to expect that the following holds:

Conjecture 9. *Let $x_0 \in \mathbb{F}_q$. Then*

$$\frac{\#\{\mathbf{v} \in \mathbb{F}_q^d \ : \ L_n(\mathbf{v}) \ne x_0 \ \textit{for}\ 1 \le n \le q\}}{q^d} = e^{-1} + o(1)$$

as $q \to \infty$, where $d = \pi(q-1)$.

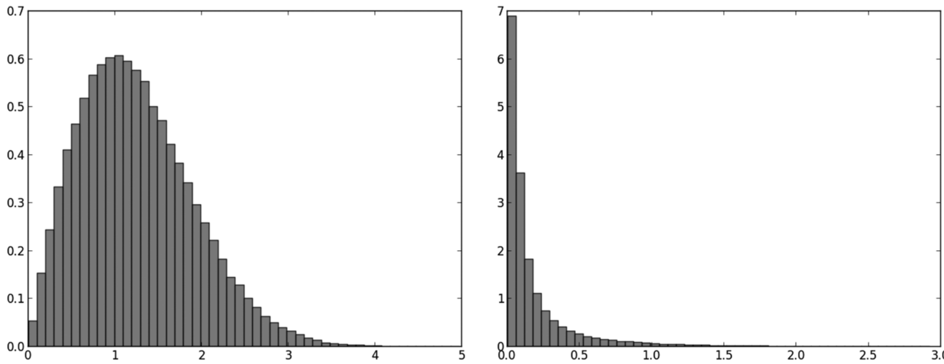

Figure 3: Histogram plots of $\#O_{\eta,x_0}(\mathbb{F}_p)/\sqrt{p}$ with $\eta(x) = x^2 + 1$ (left) and $\#O_{\psi_p,x_0}(\mathbb{F}_p)/\sqrt{p}$ (right) for $p \le 5,000,000$

In particular, Conjecture 9 implies that $\vartheta \simeq 0.4231\ldots$ in the bound of Theorem 1 can be replaced with $1 - 1/e \simeq 0.6321\ldots$.

Clearly the map ψ_p, as any map over $\mathbb{F}_p$ can be interpolated by polynomial, that is, for some unique polynomials $F_p(X) \in \mathbb{F}_p[X]$ of degree at most $p-1$ we have $\psi_p(x) = F_p(x)$ for $x \in \mathbb{F}_p$. It is natural to use $D_p = \deg F_p$ as a measure of "non-polynomiality" of the map ψ_p. In particular, we expect that D_p is close to its largest possible value $p-1$. Although we have not been able to establish this we show that

$$D_p \ge \left(\sqrt{2-\sqrt{3}} + o(1)\right) p^{1/2} = 0.5176\ldots p^{1/2}. \tag{22}$$

We remark that the x^x is a quadratic non-residue modulo p if and only if both x are odd and a quadratic non-residue. Using the Pólya–Vinogradov bound of sums of quadratic characters, it is trivial to show that there are $p/4 + O(p^{1/2}\log p)$ such values of $x = 0, 1\ldots, p-1$. Hence, for the sum of the Legendre symbols with F_p we have

$$\sum_{x\in\mathbb{F}_p} \left(\frac{F_p(x)}{p}\right) = p/2 + O(p^{1/2}\log p).$$

On the other hand, the results of Korobov [10] and Mit'kin [13] (which we use in a simplified form) imply that

$$\left|\sum_{x\in\mathbb{F}_p} \left(\frac{F_p(x)}{p}\right)\right| \le D_p\sqrt{p - D_p^2/4 + O(D_p)}$$

(provided that, say, $p \ge D_p^2/2 + 5$), which now implies (22).

For a prime p and a polynomial $f(X) \in \mathbb{Z}[X]$ we denote by $T_f(p)$ the number of solutions to the congruence

$$x^{f(x)} \equiv 1 \pmod p, \quad 1 \le x \le p-1. \tag{23}$$

We note that the number of fixed points of $x \to x^{f(x)}$ is given by $T_{f-1}(p)$.

Theorem 10. *If f is squarefree, we have*

$$T_f(p) \le p^{38/87+o(1)}$$

as $p \to \infty$.

Proof. Let us fix $d \mid p-1$ and denote by $\mathcal{X}_d$ the set of solutions to (23) with

$$\gcd(f(x), p-1) = d.$$

Clearly any element $x \in \mathcal{X}_d$ belongs to the multiplicative group $\mathcal{G}_d \subseteq \mathbb{F}_p^*$ of index d in the multiplicative group $\mathbb{F}_p^*$ of a finite field $\mathbb{F}_p$ of p elements. Therefore,

$$\#\mathcal{X}_d \le d. \tag{24}$$

Since $f(X)$ is squarefree, by the Nagell–Ore theorem (see [9] for its strongest known form) for each d there is a set $\mathcal{K}_d \subseteq \{0, \ldots, d-1\}$ of cardinality $\#\mathcal{K}_d = d^{o(1)}$ and such that every $x \in \mathcal{X}_d$ satisfies

$$x \equiv k \pmod d \tag{25}$$

for some $k \in \mathcal{K}_d$. Let us fix $k \in \mathcal{K}_d$ and denote by $\mathcal{X}_{d,k}$ the set of $x \in \mathcal{X}_d$ satisfying (25). Obviously,

$$\#\mathcal{X}_{d,k} \le (p-1)/d. \tag{26}$$

Thus, in particular, from (24) and (26), we see that $\#\mathcal{X}_{d,k} \le \sqrt{p-1}$. However, we now obtain a better bound.

We remark that the difference set

$$\mathcal{U}_{d,k} = \{x_1 - x_2 \ : \ x_1, x_2 \in \mathcal{X}_{d,k}\} \subseteq \mathbb{F}_p$$

is of cardinality at most

$$\#\mathcal{U}_{d,k} \le 2(p-1)/d \tag{27}$$

as it is contained in the reductions modulo p of integers $y \equiv 0 \pmod d$ from the interval $y \in [-(p-1), p-1]$. Similarly, for

$$\mathcal{V}_{d,k} = \{x_1 + x_2 - x_3 - x_4 \ : \ x_1, x_2, x_3, x_4 \in \mathcal{X}_{d,k}\} \subseteq \mathbb{F}_p,$$

we have

$$\#\mathcal{V}_{d,k} \le 4(p-1)/d. \tag{28}$$

Furthermore, the product set

$$\mathcal{W}_{d,k} = \{x_1 x_2 \ : \ x_1, x_2 \in \mathcal{X}_{d,k}\} \subseteq \mathbb{F}_p$$

is of cardinality at most

$$\#\mathcal{W}_{d,k} \le d \tag{29}$$

as it is contained in $\mathcal{G}_d$. Finally, as in [3, Section 1], we note that the Cauchy inequality implies that

$$E_{d,k} = \#\{(x_1, x_2, x_3, x_4) \in \mathcal{X}_{d,k}^4 \ : \ x_1 x_2 = x_3 x_4\}$$

satisfies

$$E_{d,k} \ge \frac{(\#\mathcal{X}_{d,k})^4}{\#\mathcal{W}_{d,k}}. \tag{30}$$

By the result of Bourgain and Garaev [3, Theorem 1.1] we have

$$E_{d,k}^4 \le \left(\#\mathcal{U}_{d,k} + \frac{(\#\mathcal{X}_{d,k})^3}{p}\right) (\#\mathcal{X}_{d,k})^5 \, (\#\mathcal{U}_{d,k})^4 \, \#\mathcal{V}_{d,k} p^{o(1)},$$

which together with (30) implies

$$(\#\mathcal{X}_{d,k})^{11} \le \left(\#\mathcal{U}_{d,k} + \frac{(\#\mathcal{X}_{d,k})^3}{p}\right) (\#\mathcal{U}_{d,k})^4 \, \#\mathcal{V}_{d,k} \, (\#\mathcal{W}_{d,k})^4 \, p^{o(1)} \tag{31}$$

as $p \to \infty$. Substituting the bounds (27)–(29) into (31), we derive

$$(\#\mathcal{X}_{d,k})^{11} \le \left(pd^{-1} + \frac{(\#\mathcal{X}_{d,k})^3}{p}\right) p^{5+o(1)} d^{-1}.$$

Thus,

$$\#\mathcal{X}_{d,k} \le \max\left\{p^{6/11}d^{-2/11}, p^{1/2}d^{-1/8}\right\}p^{o(1)}. \tag{32}$$

Furthermore, let

$$\mathcal{Y}_{d,k} = \{x_1 + x_2 + x_3 \ : \ x_1, x_2, x_3, x_4 \in \mathcal{X}_{d,k}\} \subseteq \mathbb{F}_p.$$

By a version of the sum-product estimate given in [15, Corollary 6], we have

$$(\#\mathcal{X}_{d,k})^{16} \ll (\#\mathcal{Y}_{d,k})^4 (\#\mathcal{W}_{d,k})^9 . \tag{33}$$

Similarly to (28), we also have

$$\#\mathcal{Y}_{d,k} \le 3(p-1)/d,$$

which together with (29), after substitution in (33) implies

$$\#\mathcal{X}_{d,k} \ll p^{1/4}d^{5/16}. \tag{34}$$

Using the bound (24) for $d < p^{4/11}$, the bound (34) for $p^{4/11} \le d < p^{52/87}$ and the bound (32) for $d \ge p^{52/87}$ we obtain

$$\#\mathcal{X}_{d,k} \le p^{38/87+o(1)}$$

as $p \to \infty$, which concludes the proof. □

Remark 11. We note that as long as d is square free, we have $\#\mathcal{K}_d = d^{o(1)}$ with no assumption of f being square free. Hence, we find that the upper bound on $T_f(p)$ holds without any assumption on $f(x)$ provided that $p-1$ is square free. In fact, it is enough to assume that the square full part of $p-1$ is of size $p^{o(1)}$.

Acknowledgments

Part of this work was done during visits of F.L. at KTH, Stockholm and Macquarie University, Australia and P.K. at the Mathematical Institute of the UNAM in Morelia, Mexico. These authors thank these institutions for their hospitality and support. P.K. was partially supported by grants from the Göran Gustafsson Foundation, the Knut and Alice Wallenberg foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council, F.L. was supported in part by Grants PAPIIT 104512, CONACyT

163787, CONACyT 193539 and a Marcos Moshinsky Fellowship, and I.E.S. was supported in part by ARC grants DP110100628 and DP130100237.

References

[1] A. Balog, K.A. Broughan and I.E. Shparlinski, *On the number of solutions of exponential congruences*, Acta Arith. **148** (2011), 93–103.

[2] A. Balog, K.A. Broughan and I.E. Shparlinski, *Sum-products estimates with several sets and applications*, Integers **12** (2012), 895–906.

[3] J. Bourgain and M.Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge. Philos. Soc. **146** (2008), 1–21.

[4] R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, Springer-Verlag, New York, 2005.

[5] R. Crocker, *On residues of n^n*, Amer. Math. Monthly **76** (1969), 1028–1029.

[6] P. Flajolet and A.M. Odlyzko, *Random mapping statistics*, Lecture Notes in Comput. Sci. **434**, (1990), 329–354.

[7] G. Gras, *Class field theory*, Springer-Verlag, Belin, 2005.

[8] J. Holden and P. Moree, *Some heuristics and and results for small cycles of the discrete logarithm*, Math. Comput. **75** (2006), 419–449.

[9] M.N. Huxley, *A note on polynomial congruences*, in 'Recent progress in analytic number theory', **1**, Academic Press, London, 1981, 193–196.

[10] N.M. Korobov, *An estimate of the sum of the Legendre symbols*, Dokl. Akad. Nauk SSSR **196** (1971), 764–767;
(in Russian), translated in Soviet Math. Dokl., **12** (1971), 241–245.

[11] J.C. Lagarias and A.M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Algebraic number fields, Academic Press, New York, 1977, 409–464.

[12] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.

[13] D.A. Mit'kin, *An estimate of the sum of the Legendre symbols with polynomials of an even degree*, Matem. Zametki **14** (1973), 73–81;
(in Russian), translated in Math. Notes, **14** 1973, 597–602.

[14] C. Pomerance and I.E. Shparlinski, *Rank statistics for a family of elliptic curves over a function field*, Pure Appl. Math. Q. **6** (2010), 21–40.

[15] O. Roche-Newton, M. Rudnev and I.D. Shkredov, *New bounds sum-product estimates over finite fields*, preprint, 2014, available at: http://arxiv.org/abs/1408.0542).

[16] L.G. Sathe, *On a problem of Hardy and Ramanujan on the distribution of integers having a given number of prime factors*, J. Indian Math. Soc. **17** (1953), 27–81.

[17] A. Selberg, *Note on a paper of L. G. Sathe*, J. Indian Math. Soc. **18** (1954), 83–87.

[18] L. Somer, *The residues of n^n modulo p*, Fibonacci Q. **19** (1981), 110–117.

[19] H.M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. **3** (1974), 135–152.

[20] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, 1995.

[21] B. Winckler, Théoréme de Chebotarev effectif, preprint, 2014, available at: http://arxiv.org/abs/1311.5715.

Department of Mathematics
Royal Institute of Technology
SE-100 44 Stockholm
Sweden
E-mail address: kurlberg@math.kth.se

School of Mathematics
University of the Witwatersrand
P.O. Box 2050
South Africa
E-mail address: florian.luca@wits.ac.za

Department of Pure Mathematics
University of New South Wales
Sydney, NSW 2052
Australia
E-mail address: igor.shparlinski@unsw.edu.au