Thai Journal of **Math**ematics
Volume 22 Number 1 (2024)
Pages 251–262

http://thaijmath.in.cmu.ac.th

ISSN 1686-0209

Annual Meeting in Mathematics 2023

Properties of the Graph Arising from Certain Map over a Finite Field

Pratchayaporn Doemlim[1,*], **Vichian Laohakosol**[2] **and Tuangrat Chaichana**[1]

[1] *Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand*
e-mail : pratchayaporn2539@gmail.com (P. Doemlim); tuangrat.c@chula.ac.th (T. Chaichana)

[2] *Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand*
e-mail : fscivil@ku.ac.th (V. Laohakosol)

Abstract For primes p and q, the graph obtained from iterating the map $x \mapsto x^p$ over the finite field of q^2 elements is considered. Asymptotic formulas for the sum, over bounded primes q, of the total number of elements in all cycles and that of all tail lengths are derived.

MSC: 11T30
Keywords: graph of iteration; finite field; cycle; tail

Submission date: 02.06.2023 / Acceptance date: 31.08.2023

1. Introduction

Throughout the entire paper, let q be a prime and $m \in \mathbb{N}$. Let $\mathbb{F}_{q^m}$ be the finite field of q^m elements, let $\mathbb{F}_{q^m}^* := \mathbb{F}_{q^m} \setminus \{0\}$, and let $g : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*$ be a function. The iterates of g are defined by

$$g^0(x) = x, \quad g^i(x) = g(g^{i-1}(x)) \quad (i \in \mathbb{N}).$$

By $G_g = (V, E)$, we refer to the directed graph whose vertex set is $V \subseteq \mathbb{F}_{q^m}$ and whose directed edges in E are denoted by $(x, g(x))$. The *reverse graph* of G_g, denoted by $(G_g)_R$, is the graph (V, E_R) with directed edge set $E_R := \{(x, y) : (y, x) \in E\}$.

For $x \in \mathbb{F}_{q^m}$, the *orbit* of x is the directed path in a graph G_g of the map g starting at x. Since $\mathbb{F}_{q^m}$ is a finite field, there exists the least non-negative integer $t = t(x)$ such that $g^t(x) = g^{s_0}(x)$ for some positive integer $s_0 > t$. Let s be the least s_0 such that $g^t(x) = g^{s_0}(x)$, and let

$$c := c(x) = s - t > 0.$$

We then have $g^t(x) = g^{t+c}(x)$. The *tail* of x is the list of elements

$$x, g(x), g^2(x), \ldots, g^{t-1}(x),$$

*Corresponding author.

and t is called the *tail length* of x. The *cycle* of x is the list of elements

$$g^t(x), \ldots, g^{t+c-1}(x),$$

and c is called the *cycle length* of x. For general references on finite fields and graph theory, we refer to [4] and [10].

For $n \in \mathbb{N}$, $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$, denote by $\mathrm{ord}_n a$ the least positive integer such that $a^{\mathrm{ord}_n a} \equiv 1 \pmod{n}$. For $\alpha \in \mathbb{F}_{q^m}^*$, the *order* of α, denoted by $\mathcal{O}(\alpha)$, is the least positive integer such that $\alpha^{\mathcal{O}(\alpha)} = 1$. For a prime p and $n \in \mathbb{N}$, define $v_p(n)$ to be the exponent of the largest power of p that divides n, i.e., $p^{v_p(n)} \mid n$ but $p^{v_p(n)+1} \nmid n$.

In 1996, Rogers [8] studied properties of graphs obtained from iterating the quadratic map $g(x) = x^2$ over $\mathbb{F}_p$ for any p prime, and derived a formula for the number of cycles relative to g. In 2004, Vasiga and Shalit [3] studied graphs resulted from iterating the quadratic maps over the finite field $\mathbb{F}_p$, where p is an odd prime. Among other things they characterized the vertices of the corresponding directed graph in terms of primitive elements, gave formulas for the tail and cycle lengths, and assuming the extended Riemann hypothesis, derived asymptotic estimates for the sum of the number of elements in all cycles and the sum of all tail lengths.

In this work, we complement these two earlier works by considering the graph obtained from iterating the map $g(x) = x^p$ (p prime) over the finite field of q^m elements extending the ideas of [8] and [3]. Our discussion includes the structure of the graph so obtained, characterization of vertices in terms of primitive elements, the number of cycles, tail and cycle lengths, and asymptotic estimates, in the case $p = 2$, of the sum of the total number of elements in all cycles and that of all tail lengths.

2. Basic Properties

We start by establishing basic properties about the graph (over $\mathbb{F}_{q^m}^*$) obtained from iterating the map $g(x) = x^p$ for a fixed prime p.

Theorem 2.1. *Let $\alpha \in \mathbb{F}_{q^m}^*$ be of order $\mathcal{O}(\alpha) := p^e\ell$, where $e \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$, $\ell \in \mathbb{N}$ with $\gcd(p, \ell) = 1$. Let $t := t(\alpha)$ and $c := c(\alpha)$ be the tail and the cycle lengths, respectively, of α. Then $t = v_p(\mathcal{O}(\alpha))$ and $c = ord_\ell p$.*

Proof. From $\alpha^{p^t} = g^t(\alpha) = g^{t+c}(\alpha) = \alpha^{p^{t+c}}$, we get

$$\alpha^{p^t(p^c-1)} = \alpha^{p^{t+c}-p^t} = 1.$$

Using the definition of order, we have $p^e\ell \mid p^t(p^c-1)$. Since $\gcd(p^e, p^c-1) = 1 = \gcd(\ell, p^t)$, we get $p^e \mid p^t$ and $\ell \mid (p^c - 1)$. Clearly, $e \leq t$. If $e < t$, since t is the smallest nonnegative integer such that $g^t(\alpha) = g^{t+c}(\alpha)$, we have

$$\alpha^{p^e} = g^e(\alpha) \neq g^{e+c}(\alpha) = \alpha^{p^{e+c}}$$

and so $\alpha^{p^e(p^c-1)} = \alpha^{p^{e+c}-p^e} \neq 1$, contradicting $\alpha^{p^e\ell} = 1$ and $\ell \mid (p^c - 1)$. Thus, $t = e$, which proves the first assertion.

To prove the second assertion, from $\ell \mid (p^c-1)$, we get $p^c \equiv 1 (\mathrm{mod}\ \ell)$, and so $\mathrm{ord}_\ell p \leq c$. If there exists $d \in \mathbb{N}$ such that $1 \leq d < c$ and $p^d \equiv 1 (\mathrm{mod}\ \ell)$. Then $\ell \mid (p^d - 1)$ and so $p^e\ell \mid p^t(p^d - 1)$. This implies that $\alpha^{p^{t+d}-p^t} = \alpha^{p^t(p^d-1)} = 1$, i.e.,

$$g^{t+d}(\alpha) = \alpha^{p^{t+d}} = \alpha^{p^t} = g^t(\alpha),$$

contradicting the minimality of $s = t + c$. ∎

For convenience, throughout the rest of the paper, we fix the following notation. Write

$$q^m - 1 = p^\tau \rho, \text{ where } \tau \in \mathbb{N}_0,\ \rho \in \mathbb{N}, \text{ and } \gcd(p, \rho) = 1. \tag{2.1}$$

The next theorem relates each tail with a primitive element.

Theorem 2.2. *Let γ be a primitive element of $\mathbb{F}_{q^m}^*$. Then*

(a) $\{a \in \mathbb{F}_{q^m}^* : t(a) = 0\} = \{\gamma^i : 1 \le i \le q^m - 1,\ v_p(i) \ge v_p(q^m - 1)\}$;
(b) for $1 \le k \le v_p(q^m - 1)$, *we have*

$$\{a \in \mathbb{F}_{q^m}^* : t(a) = k\} = \{\gamma^i : 1 \le i \le q^m - 1,\ v_p(i) = v_p(q^m - 1) - k\}.$$

Proof. (a) Any $a \in \mathbb{F}_{q^m}^*$ can be written as $a = \gamma^i$ for some $1 \le i \le q^m - 1$.
If $t(a) = 0$, there is $\ell \in \mathbb{N}$ such that $a = g^0(a) = g^{\ell+0}(a) = a^{p^\ell}$, and so $(\gamma^i)^{p^\ell - 1} = a^{p^\ell - 1} = 1$, yielding $p^\tau \rho \mid i(p^\ell - 1)$. Since $p \nmid (p^\ell - 1)$, we deduce that $p^\tau \mid i$, and so $v_p(i) \ge \tau = v_p(q^m - 1)$.

Conversely, consider $a = \gamma^i \in \mathbb{F}_{q^m}^*$ with $1 \le i \le q^m - 1$ and $v_p(i) \ge v_p(q^m - 1) = \tau$. Then $p^\tau \mid i$. Let $\ell = \operatorname{ord}_\rho p$. Then $p^\ell \equiv 1 \pmod{\rho}$, i.e., $\rho \mid (p^\ell - 1)$, and so $p^\tau \rho \mid i(p^\ell - 1)$ yielding $(\gamma^i)^{p^\ell - 1} = 1$. It follows that $g^\ell(\gamma^i) = (\gamma^i)^{p^\ell} = \gamma^i = g^0(\gamma^i)$ implying that $t(a) = t(\gamma^i) = 0$.

(b) Let $k \in \mathbb{N}$ with $1 \le k \le v_p(q^m - 1)$. Let $a = \gamma^i \in \mathbb{F}_{q^m}^*$ $(i \in \{1, \dots, q^m - 1\})$ be such that $t(a) = k$. Then there exists $\ell \in \mathbb{N}$ such that

$$(\gamma^i)^{p^k} = g^k(a) = g^{k+\ell}(a) = (\gamma^i)^{p^{k+\ell}} \quad \text{but} \quad (\gamma^i)^{p^{k-1}} = g^{k-1}(a) \ne g^{k-1+\ell}(a) = (\gamma^i)^{p^{k-1+\ell}}$$

showing that $(\gamma^i)^{p^{k+\ell} - p^k} = 1$ but $(\gamma^i)^{p^{k-1+\ell} - p^{k-1}} \ne 1$. Thus,

$$p^\tau \rho \mid ip^k(p^\ell - 1) \quad \text{but} \quad p^\tau \rho \nmid ip^{k-1}(p^\ell - 1). \tag{2.2}$$

We claim now that $p^\tau \nmid ip^{k-1}$. Write $i = p^r w$ for some $r \in \mathbb{N}_0$, $w \in \mathbb{N}$ with $\gcd(p, w) = 1$. If $p^\tau \mid ip^{k-1} = p^r w p^{k-1}$, then $p^\tau \mid p^r p^{k-1}$. Consequently, $\rho | w(p^\ell - 1)$ yielding $p^\tau \rho \mid ip^{k-1}(p^\ell - 1)$ which is a contradiction, and the claim is verified. From the claim and (2.2), we get $v_p(p^\tau) = v_p(ip^k)$, i.e., $\tau = v_p(i) + k$ and so $v_p(i) = \tau - k = v_p(q^m - 1) - k$.

Conversely, consider $\gamma^i \in \mathbb{F}_{q^m}^*$ with $1 \le i \le q^m - 1$ and $v_p(i) = v_p(q^m - 1) - k$. Then, $v_p(ip^k) = v_p(q^m - 1) = v_p(p^\tau \rho)$ implying that $p^\tau \mid ip^k$ but $p^\tau \nmid ip^{k-j}$ for all $1 \le j \le k$. Since $\gcd(p, \rho) = 1$, there exists $\ell \ge 1$ such that $\rho \mid (p^\ell - 1)$, and so $p^\tau \rho \mid ip^k(p^\ell - 1)$ but $p^\tau \rho \nmid ip^{k-j}(p^\ell - 1)$ for all $1 \le j \le k$. Thus,

$$(\gamma^i)^{p^k(p^\ell - 1)} = 1 \quad \text{but} \quad (\gamma^i)^{p^{k-j}(p^\ell - 1)} \ne 1 \ (1 \le j \le k),$$

i.e., $g^k(\gamma^i) = g^{k+\ell}(\gamma^i)$ but $g^{k-1}(\gamma^i) \ne g^{k-1+\ell}(\gamma^i)$, and so $t(\gamma^i) = k$. ∎

The next theorem deals with cycles.

Theorem 2.3. *We have*

(a) the total number of elements in all cycles is ρ;
(b) off each element in the cycles, there hangs a reversed complete p-ary tree of height $\tau - 1$ containing $\frac{p^\tau - 1}{p - 1}$ elements.

Proof. Let γ be a primitive element of $\mathbb{F}_{q^m}^*$ and $a \in \mathbb{F}_{q^m}^*$.

(a) If a is in a cycle, then $t(a) = 0$, and Theorem 2.2 (a) shows that

$$a = \gamma^i \ \ (1 \le i \le q^m - 1), \quad \text{and} \quad v_p(i) \ge v_p(q^m - 1) = \tau$$

so that the exponent i must be of the form $i = jp^\tau$ with $1 \le j \le \rho$, showing that the total number of elements in all cycles is ρ.

(b) For an element $\gamma^{jp^{\tau-1}}$ in a cycle, since all the roots of the equation $x^p = \gamma^{jp^\tau}$ take the form $x = \gamma^{jp^{\tau-1}+\frac{k(q^m-1)}{p}}$ $(0 \le k \le p-1)$, these are all elements whose first iterate gives γ^{jp^τ}. Among these p roots, there is exactly one root, $\gamma^{jp^{\tau-1}}$, being its preceding element in the cycle, and the remaining $p-1$ roots are elements with tail length being precisely 1. From (2.1) and Theorem 2.1, the longest tail length of any nonzero element in $\mathbb{F}_{q^m}$ is τ, so there hang from each of these $p-1$ elements of tail length 1, a reversed complete p-ary tree of height $\tau-1$ containing $1+p+p^2+\cdots+p^{\tau-1} = \frac{p^\tau-1}{p-1}$ elements. ∎

To analyze certain asymptotics about tail and cycle lengths extending those in [9], we define

- $T_0(q^m, p)$ to be the total number of elements in all cycles, i.e., the number of elements $a \in \mathbb{F}_{q^m}^*$ for which $t(a) = 0$;
- $T(q^m, p)$ to be the average value of $t(a)$ $(a \in \mathbb{F}_{q^m}^*)$, i.e., $T(q^m, p) = \frac{1}{q^m-1}\sum_{a\in\mathbb{F}_{q^m}^*} t(a)$.

Theorem 2.4. *We have*

(a) $T_0(q^m, p) = \rho$;
(b) $T(q^m, p) = \tau - \frac{p^\tau-1}{p^\tau(p-1)}$.

Proof. Part (a) is Theorem 2.3 (a). To prove (b), note that by Theorem 2.1, $t(\alpha) = v_p(\mathcal{O})$, where $p^e\ell = \mathcal{O}(\alpha) := \mathcal{O} \mid (q^m-1) = p^\tau\rho$. Since there are $\varphi(\mathcal{O})$ elements having the same order $\mathcal{O}$, we get

$$\begin{aligned} T(q^m,p) &= \frac{1}{q^m-1}\sum_{\alpha\in\mathbb{F}_{q^m}^*} t(\alpha) = \frac{1}{q^m-1}\sum_{\mathcal{O}\mid q^m-1} \varphi(\mathcal{O})v_p(\mathcal{O}) = \frac{1}{p^\tau\rho}\sum_{p^e\ell\mid p^\tau\rho} \varphi(p^e\ell)v_p(p^e\ell) \\ &= \frac{1}{p^\tau\rho}\sum_{\ell\mid\rho}\sum_{0\le e\le\tau} \varphi(\ell)\varphi(p^e)e = \frac{1}{p^\tau\rho}\sum_{\ell\mid\rho}\varphi(\ell)\sum_{1\le e\le\tau} p^{e-1}(p-1)\cdot e \\ &= \frac{1}{p^\tau\rho}(p-1)\rho\cdot\frac{(p-1)(\tau+1)p^\tau-(p^{\tau+1}-1)}{(p-1)^2} = \tau - \frac{p^\tau-1}{p^\tau(p-1)}. \end{aligned}$$

∎

3. Asymptotic Estimates

For large $x > 0$, denote by $\pi(x, \ell, k)$ the number of primes $\le x$ which are congruent to $k \mod \ell$, where ℓ, k are positive integers with $\gcd(k, \ell) = 1$. For our asymptotic estimate, the usual prime number theorem for arithmetic progressions is not sufficient to obtain a good error term. To this end, we adopt the following version of extended prime number theorem for arithmetic progressions due to E. Alkan [1, Equation (3.36), p. 11]. *Assume that there exists a real number* $\theta \in [1/2, 1)$ *such that for all* $\ell \le x$, *we have*

$$\pi(x, \ell, k) = \frac{\mathrm{li}(x)}{\varphi(\ell)} + O(x^\theta \log x), \tag{3.1}$$

where $\mathrm{li}(x) = \int_2^x \frac{1}{\log t}dt$.
As mentioned in [1], this version of the prime number theorem for arithmetic progressions is a consequence of the following *weak Riemann hypothesis*:

assume that there exists a real number $1/2 \le \theta < 1$ *such that all zeros of all Dirichlet L-functions* $L(s,\chi)$ *satisfy* $\Re(s) \le \theta$.

Using, [3, p. 28],

$$\int_2^x \frac{1}{\log t}dt = \frac{x}{\log x} + O\Big(\frac{x}{(\log x)^2}\Big) \tag{3.2}$$

and

$$\lim_{x\to\infty} \frac{x^\theta \log x}{x/(\log x)^2} = 0. \tag{3.3}$$

We start our asymptotic analysis with some useful results.

Lemma 3.1. *Let* ℓ, k *be as above. For* $x \ge 2$, *let* f *be a real-valued continuously differentiable function on* $[1,x]$. *Then*

$$\sum_{\substack{q\le x,\ q \text{ primes}\\ q\equiv k(\mathrm{mod}\ \ell)}} f(q) = \frac{1}{\varphi(\ell)}\int_2^x \frac{f(t)}{\log t}dt + f(x)\varepsilon(x) - \int_2^x f'(t)\varepsilon(t)dt + O(1),$$

where $\varepsilon(x) := O(x^\theta \log x)$.

Proof. Let

$$a(n) = \begin{cases} 1 & \text{if } n \text{ is prime, } n \equiv k \ (\mathrm{mod}\ \ell),\\ 0 & \text{otherwise,}\end{cases}$$

so that

$$A(x) := \sum_{n\le x} a(n) = \sum_{\substack{n\le x,\ n \text{ primes}\\ n\equiv k \ (\mathrm{mod}\ \ell)}} 1 = \pi(x,\ell,k).$$

Since $A(x)$ is a step function with jump $a(n)$ at each $n \in \mathbb{N}$, the sum can be expressed as a Stieltjes integral

$$\sum_{\substack{2\le q\le x,\ q \text{ primes}\\ q\equiv k(\mathrm{mod}\ \ell)}} f(q) = \sum_{2\le n\le x} a(n)f(n) = \int_2^x f(t)dA(t). \tag{3.4}$$

Using the definition of li and integration by parts, we get

$$\begin{aligned}\int_2^x f(t)dA(t) &= \int_2^x f(t)d\left(\frac{1}{\varphi(\ell)}\mathrm{li}(t) + \varepsilon(t)\right) = \frac{1}{\varphi(\ell)}\int_2^x \frac{f(t)}{\log t}dt + \int_2^x f(t)\varepsilon'(t)dt + O(1)\\ &= \frac{1}{\varphi(\ell)}\int_2^x \frac{f(t)}{\log t}dt + f(x)\varepsilon(x) - \int_2^x f'(t)\varepsilon(t)dt + O(1).\end{aligned} \tag{3.5}$$

and the desired result follows immediately from (3.4) and (3.5). ∎

Lemma 3.2. *Assume the weak Riemann hypothesis. For $i \in \mathbb{N}_0$ and $k,\ N \in \mathbb{N}$ with $\gcd(k,p)=1$. we have*

$$\pi(N^{1/2},p^{i+1},k) := \sum_{\substack{q\le N^{1/2},\ q \text{ primes}\\ q\equiv k(\mathrm{mod}\ p^{i+1})}} 1 = \frac{1}{p^i(p-1)}\left(\frac{N^{1/2}}{\log N^{1/2}} + O\Big(\frac{N^{1/2}}{(\log N)^2}\Big)\right) + O(N^{\theta/2}\log N) \tag{3.6}$$

$$\sum_{\substack{q\le N^{1/2},\ q \text{ primes}\\ q\equiv k(\mathrm{mod}\ p^{i+1})}} q^2 = \frac{1}{p^i(p-1)}\left(\frac{N^{3/2}}{\log N^{3/2}} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\right) + O\Big(N^{1+\frac{\theta}{2}}\log N\Big) \tag{3.7}$$

$$\sum_{q\le N^{1/2},\ q \text{ primes}} q^2 = \frac{2N^{3/2}}{3\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big) + O\Big(N^{1+\frac{\theta}{2}}\log N\Big), \tag{3.8}$$

provided that for (3.6) and (3.7) to make sense the index i is subject to the condition

$$i \le N_1 := \lfloor \log_2\Big(\frac{N^{\frac{1-\theta}{2}}}{(\log N)^3}\Big)\rfloor.$$

(Note as in (3.1) that the expression on the right-hand side of (3.7) is independent of k.)

Proof. From (3.1), we have

$$\pi(N^{1/2},p^{i+1},k) = \sum_{\substack{q\le N^{1/2},\ q \text{ primes}\\ q\equiv k(\mathrm{mod}\ p^{i+1})}} 1 = \frac{1}{p^i(p-1)}\left(\frac{N^{1/2}}{\log N^{1/2}} + O\Big(\frac{N^{1/2}}{(\log N)^2}\Big)\right) + O(N^{\theta/2}\log N).$$

To prove (3.7), we substitute $f(t)=t^2,\ x=N^{1/2},\ \ell=p^{i+1}$ into Lemma 3.1, we get

$$\sum_{\substack{q\le N^{1/2},\ q \text{ primes}\\ q\equiv k(\mathrm{mod}\ p^{i+1})}} q^2 = \frac{1}{\varphi(p^{i+1})}\int_2^{N^{1/2}} \frac{t^2}{\log t}dt + N\varepsilon(N^{1/2}) - \int_2^{N^{1/2}} 2t\,\varepsilon(t)dt + O(1)$$

$$= \frac{1}{p^i(p-1)}\int_{2^3}^{N^{3/2}} \frac{1}{\log u}du + O\Big(N^{1+\theta/2}(\log N)\Big).$$

We now treat the terms on the right-hand side separately. Using (3.2), the main term is

$$\frac{1}{p^i(p-1)}\int_{2^3}^{N^{3/2}} \frac{1}{\log u}du = \frac{1}{p^i(p-1)}\left(\frac{2N^{3/2}}{3\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\right). \tag{3.9}$$

Then we have (3.7).

The proof of (3.8) is simpler but follows the same line as that of (3.7). Using [3, Theorem 2.7.1, p. 29] with $f(t)=t^2,\ x=N^{1/2}$ and proceed with the above computations, we get

$$\sum_{q\le N^{1/2},\ q \text{ primes}} q^2 = \frac{2N^{3/2}}{3\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big) + O(N^{\theta/2}\log N).$$

■

Lemma 3.3. *For each $i \in \mathbb{N}_0$, we have $p^i \,||\, (q^2-1)$ if and only if there exists a unique $r \in \{1, 2, \ldots, p-1\}$ such that $q^2 - 1 \equiv rp^i \pmod{p^{i+1}}$.*

Proof. The sufficiency part is clear. To prove the necessity part, assume that $p^i \,||\, (q^2-1)$. Then $p^i \mid (q^2-1)$ and $p^{i+1} \nmid (q^2-1)$ implying that there exists a unique $\ell \in \mathbb{N}$ such that $q^2 - 1 = p^i\ell$, $\gcd(p, \ell) = 1$. The last requirement shows that there are unique $k \in \mathbb{N}_0, r \in \{1, \ldots, p-1\}$ such that $\ell = pk + r$. Thus, $q^2 - 1 = p^i(pk + r) = p^{i+1}k + rp^i$, and the desired assertion follows. ∎

Lemma 3.4. *Given $i \in \mathbb{N}_0$, the congruence $q^2 \equiv 2^i + 1 \pmod{2^{i+1}}$ has*

- *when $i = 0$ exactly one solution $q = 2 \equiv 0$ (mod 2);*
- *when $i = 1, 2$ no solution;*
- *when $i \geq 3$ a total of four solutions*

Proof. The cases $i = 0, 1, 2$ are easily checked directly. For $i \geq 3$, From [5, Theorem 4.6, p. 174], the congruence has four solutions. Indeed, it is readily checked that the four solutions are $2^{i-1} \pm 1$, $2^i + 2^{i-1} \pm 1$. ∎

Our first asymptotic result deals with the case $m = 2$, and the iteration map $g(x) = x^2$ over $\mathbb{F}_{q^2}^*$.

Theorem 3.5. *Assume the weak Riemann hypothesis. Let*

$$ST_0(2, N) := \sum_{q^2 \leq N,\ q \text{ primes}} T_0(q^2, 2),$$

where T_0 is as in Theorem 2.4. Then

$$ST_0(2, N) = \frac{1}{18} \frac{N^{3/2}}{\log N} + O\left(\frac{N^{3/2}}{(\log N)^2}\right).$$

Proof. Write $q^2 - 1 = 2^\tau \rho$, where $\tau = v_2(q^2-1)$ and $\gcd(2, \rho) = 1$. From Theorem 2.4, we know that $T_0(q^2, 2) = \frac{q^2-1}{2^{v_2(q^2-1)}}$, and so

$$ST_0(2, N) = \sum_{q \leq N^{1/2},\ q \text{ primes}} \frac{q^2-1}{2^{v_2(q^2-1)}} = \sum_{0 \leq i \leq \lfloor \log_2(N-1) \rfloor} \sum_{\substack{q \leq N^{1/2},\ q \text{ primes} \\ 2^i \,||\, (q^2-1)}} \frac{q^2-1}{2^i}. \tag{3.10}$$

By Lemma 3.3, we have

$$ST_0(2, N) = \sum_{0 \leq i \leq \lfloor \log_2(N-1) \rfloor} \frac{1}{2^i} \left(\sum_{\substack{q \leq N^{1/2},\ q \text{ primes} \\ q^2 \equiv 2^i + 1 \pmod{2^{i+1}}}} q^2 - \sum_{\substack{q \leq N^{1/2},\ q \text{ primes} \\ q^2 \equiv 2^i + 1 \pmod{2^{i+1}}}} 1 \right). \tag{3.11}$$

If $i \geq 3$, by Lemma 3.4 and its proof, we get

$$\sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2 = \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv 2^{i-1}+1 \pmod{2^{i+1}}}} q^2 + \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv 2^{i-1}-1 \pmod{2^{i+1}}}} q^2 + \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv 2^{i-1}+2^i+1 \pmod{2^{i+1}}}} q^2 + \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv 2^{i-1}+2^i-1 \pmod{2^{i+1}}}} q^2$$

Using the estimate from Lemma 3.2 and (3.3), for $i \geq 3$ we obtain

$$\sum_{\substack{q\leq N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2 = 4 \sum_{\substack{q\leq N^{1/2}\\ q\equiv k \pmod{2^{i+1}}}} q^2 = \frac{4}{2^i}\left(\frac{N^{3/2}}{\log N^{3/2}} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\right) + O\Big(N^{1+\frac{\theta}{2}}\log N\Big). \tag{3.12}$$

Going back to (3.11), making use of Lemma 3.4 and the observations after (3.1) and in Lemma 3.2, we have

$$\begin{aligned} ST_0(2,N) &= \left(4 + \sum_{3\leq i\leq \lfloor \log_2(N-1)\rfloor} \frac{1}{2^i} \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2\right) \\ &\quad - \left(1 + \sum_{3\leq i\leq \lfloor \log_2(N-1)\rfloor} \frac{1}{2^i} \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} 1\right) \\ &= 3 + \sum_{3\leq i\leq \lfloor \log_2(N-1)\rfloor} \frac{4}{2^i}\left(\sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv k \pmod{2^{i+1}}}} q^2 - \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv k \pmod{2^{i+1}}}} 1\right) := 3 + A - B, \end{aligned} \tag{3.13}$$

for some fixed $k \in \mathbb{N}$, where

$$A := \sum_{3\leq i\leq \lfloor \log_2(N-1)\rfloor} \frac{4}{2^i} \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv k \pmod{2^{i+1}}}} q^2, \quad B := \sum_{3\leq i\leq \lfloor \log_2(N-1)\rfloor} \frac{4}{2^i} \sum_{\substack{q\leq N^{1/2},\ q \text{ primes}\\ q\equiv k \pmod{2^{i+1}}}} 1.$$

We apply the estimate (3.7) to compute A, so to ensure that the main term in the sum A is strictly greater than the second error term, the corresponding index i must satisfy $i \leq \mathit{https} : //\mathit{www.overleaf.com/project/656d4d4e8c41f0768c4454a3}N_1$ with N_1 as in Lemma 3.2. So we split the sum A into two sums

$$A := A_1 + A_2, \tag{3.14}$$

where

$$\begin{aligned}A_1 &= \frac{8}{3}\sum_{3\le i\le N_1}\frac{1}{2^i}\left\{\frac{1}{2^i}\left(\frac{N^{3/2}}{\log N}+O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\right)+O\Big(N^{1+\frac{\theta}{2}}\log N\Big)\right\}\\ &= \frac{8}{3}\sum_{3\le i\le N_1}\frac{1}{4^i}\Big(\frac{N^{3/2}}{\log N}\Big)+O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)+O\Big(N^{1+\frac{\theta}{2}}\log N\Big)\\ &= \frac{8}{3}\left(\frac{1}{48}+O\Big(\frac{(\log N)^4}{N^{1-\theta}}\Big)\right)\Big(\frac{N^{3/2}}{\log N}\Big)+O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\\ &= \frac{1}{18}\Big(\frac{N^{3/2}}{\log N}\Big)+O\Big(\frac{N^{3/2}}{(\log N)^2}\Big).\end{aligned}$$

By (3.8) in Lemma 3.2, we have

$$\sum_{\substack{q\le N^{1/2},\ q\text{ primes}\\ q\equiv k\pmod{2^{i+1}}}} q^2 \ll \frac{1}{2^i}\Big(\frac{N^{3/2}}{\log N}\Big),$$

and so

$$\begin{aligned}A_2 &= \sum_{N_1<i\le\lfloor\log_2(N-1)\rfloor}\frac{4}{2^i}\sum_{\substack{q\le N^{1/2},\ q\text{ primes}\\ q\equiv k\pmod{2^{i+1}}}} q^2\\ &\ll \sum_{N_1<i\le\lfloor\log_2(N-1)\rfloor}\frac{1}{2^i}\cdot\frac{1}{2^i}\Big(\frac{N^{3/2}}{\log N}\Big)\\ &= O(N^{1/2+\theta}(\log N)^5).\end{aligned}$$

Applying (3.6) of Lemma 3.2 and proceeding as in the computation of A, we get

$$\begin{aligned}B &= \sum_{3\le i\le N_1}\frac{4}{2^i}\left\{\frac{1}{2^i}\left(\frac{2N^{1/2}}{\log N}+O\Big(\frac{N^{1/2}}{(\log N)^2}\Big)\right)+O(N^{\theta/2}\log N)\right\}\\ &\quad+\sum_{N_1<i\le\lfloor\log_2(N-1)\rfloor}\frac{4}{2^i}\sum_{\substack{q\le N^{1/2},\ q\text{ primes}\\ q\equiv k\pmod{2^{i+1}}}} 1\\ &= \frac{1}{6}\frac{N^{1/2}}{\log N}+O\Big(\frac{N^{1/2}}{(\log N)^2}\Big)\end{aligned}\tag{3.15}$$

The desired result now follows from (3.13) to (3.15). ∎

Theorem 3.6. *Assume the weak Riemann hypothesis. Let*

$$ST(2,N) := \sum_{q^2\le N,\ q\text{ primes}}\ \sum_{a\in\mathbb{F}_{q^2}^*} t(a),$$

where $t(a)$ is the tail length of $a\in\mathbb{F}_{q^2}^*$. Then

$$ST(2,N) = \frac{37}{18}\frac{N^{3/2}}{\log N}+O\Big(\frac{N^{3/2}}{(\log N)^2}\Big).$$

Proof. From the definition of $T(q^2,2)$, equation (2.1) and Theorem 2.4 (b), we have

$$\begin{aligned} ST(2,N) &= \sum_{q\le N^{1/2},\ q \text{ primes}} (q^2-1)\left(v_2(q^2-1) - \frac{2^{v_2(q^2-1)}-1}{2^{v_2(q^2-1)}}\right) \\ &= A_1 - A_2 - A_3 + A_4, \end{aligned} \tag{3.16}$$

where

$$A_1 := \sum_{q\le N^{1/2},\ q \text{ primes}} q^2 v_2(q^2-1), \quad A_2 := \sum_{q\le N^{1/2},\ q \text{ primes}} v_2(q^2-1)$$

$$A_3 := \sum_{q\le N^{1/2},\ q \text{ primes}} (q^2-1), \quad A_4 := \sum_{q\le N^{1/2},\ q \text{ primes}} \frac{q^2-1}{2^{v_2(q^2-1)}}$$

Using (3.8) and the Prime Number Theorem [3, p.29], the third term in (3.16) becomes

$$A_3 = \frac{2N^{3/2}}{3\log N} + O\left(\frac{N^{3/2}}{(\log N)^2}\right). \tag{3.17}$$

From (3.10) and the result of Theorem 3.5, the last term in (3.16) becomes

$$A_4 = ST_0(2,N) = \frac{1}{18}\frac{N^{3/2}}{\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big). \tag{3.18}$$

To compute the first term in (3.16), we proceed along the line of the proof of Theorem 3.5, appealing to the number of solutions of relevant congruences in Lemma 3.4, using Lemma 3.2 and splitting the sum into suitable ranges, to get

$$\begin{aligned} A_1 &= \sum_{1\le i\le \lfloor \log_2(N-1)\rfloor} \ \sum_{\substack{q\le N^{1/2},\ q \text{ primes} \\ 2^i \| (q^2-1)}} iq^2 = \sum_{1\le i\le \lfloor \log_2(N-1)\rfloor} \ \sum_{\substack{q\le N^{1/2},\ q \text{ primes} \\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} iq^2 \\ &:= A_{11} + A_{12}, \end{aligned}$$

where

$$\begin{aligned} A_{11} &= \sum_{1\le i\le N_1} \ \sum_{\substack{q\le N^{1/2},\ q \text{ primes} \\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} iq^2 = \sum_{3\le i\le N_1} i\cdot 4 \sum_{\substack{q\le N^{1/2},\ q \text{ primes} \\ q\equiv k \pmod{2^{i+1}}}} q^2 \\ &= \sum_{3\le i\le N_1} 4i\left\{\frac{1}{2^i}\left(\frac{2N^{3/2}}{3\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\right) + O\Big(N^{1+\theta/2}\log N\Big)\right\} \\ &= \left(\frac{2N^{3/2}}{3\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big)\right)\left(4 + O\Big(\frac{\log N}{N}\Big)\right) + O\Big(N^{1+\theta/2}(\log N)^3\Big) \\ &= \frac{8N^{3/2}}{3\log N} + O\Big(\frac{N^{3/2}}{(\log N)^2}\Big). \end{aligned}$$

and

$$A_{12} = \sum_{N_1 < i \le \lfloor \log_2(N-1) \rfloor} \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q^2 \equiv 2^i + 1 \pmod{2^{i+1}}}} iq^2 = \sum_{N_1 < i \le \lfloor \log_2(N-1) \rfloor} i \cdot 4 \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q \equiv k \pmod{2^{i+1}}}} q^2$$

$$\ll \sum_{N_1 < i \le \lfloor \log_2(N-1) \rfloor} 4i \frac{1}{2^i} \left(\frac{N^{3/2}}{\log N} \right)$$

$$= O\Big(N^{1+\theta/2} (\log N)^3 \Big).$$

Finally to compute the second term in (3.16), we proceed along a similar line as making use of Lemma 3.2, to get

$$A_2 = \sum_{1 \le i \le \lfloor \log_2(N-1) \rfloor} \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ 2^i \| (q^2-1)}} i = \sum_{1 \le i \le \lfloor \log_2(N-1) \rfloor} \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q^2 \equiv 2^i + 1 (\mathrm{mod}\ 2^{i+1})}} i$$

$$= \sum_{3 \le i \le \lfloor \log_2(N-1) \rfloor} \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q^2 \equiv 2^i + 1 \pmod{2^{i+1}}}} i = \sum_{3 \le i \le \lfloor \log_2(N-1) \rfloor} i \cdot 4 \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q \equiv k \pmod{2^{i+1}}}} 1$$

$$:= A_{21} + A_{22}.$$

where

$$A_{21} = \sum_{3 \le i \le N_1} 4i \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q \equiv k \pmod{2^{i+1}}}} 1$$

$$= \sum_{3 \le i \le N_1} 4i \left\{ \frac{1}{2^i} \left(\frac{2N^{1/2}}{\log N} + O\Big(\frac{N^{1/2}}{(\log N)^2} \Big) \right) + O\Big(N^{\theta/2} \log N \Big) \right\}$$

$$= \left(\frac{2N^{1/2}}{\log N} + O\Big(\frac{N^{1/2}}{(\log N)^2} \Big) \right) \left(4 + O\Big(\frac{\log N}{N} \Big) \right) + O\Big(N^{\theta/2} (\log N)^3 \Big)$$

$$= \frac{8N^{1/2}}{\log N} + O\Big(\frac{N^{1/2}}{(\log N)^2} \Big),$$

and

$$A_{22} = \sum_{N_1 < i \le \lfloor \log_2(N-1) \rfloor} 4i \sum_{\substack{q \le N^{1/2},\ q \text{ primes} \\ q \equiv k \pmod{2^{i+1}}}} 1.$$

For $n > N_1$, the dominant term is order $N^{\theta/2} \log N$. Thus,

$$A_{22} \ll \sum_{N_1 < i \le \lfloor \log_2(N-1) \rfloor} 4i \cdot N^{\theta/2} \log N$$

$$= O\Big(N^{\theta/2} (\log N)^3 \Big).$$

Collecting all four terms, the desired estimate follows. ∎

Acknowledgements

The authors wish to thank Associate Professor Dr. Teerapat Srichan for several helpful discussion and insights and would like to thank the referees for their comments and suggestions.

References

[1] E. Alkan, Applications of Bombieri–Vinogradov type theorems to power–free integers, Colloq. Math. 164 (2021) 53–75.

[2] T.M. Apostol, Introduction to Analytic Number Theory, Springer, New York, 1976.

[3] E. Bach, J. Shallit, Algorithmic Number Theory, MIT Press, Cambridge, 1996.

[4] G. Chartrand, Introductory Graph Theory, Dover, New York, 1985.

[5] T. Cai, The Book of Numbers, World Scientific, New Jersey, 2017.

[6] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London, 1968.

[7] R. Lidl, N. Niederreiter, Finite Fields, Cambridge University Press, London, 1997.

[8] T.D. Rogers, The graph of the square mapping on the prime fields, Discrete Math. 148 (1996) 317–324.

[9] T. Vasiga, J. Shallit, On the iteration of certain quadratic maps over $GF(p)$, Discrete Math. 277 (2004) 219–240.

[10] R.J. Wilson and J.J. Watkins, Graphs: An Introductory Approach, Wiley, Toronto, 1990.