สมบัติเชิงกราฟและเชิงทฤษฎีจำนวนของบางฟังก์ชันเหนือฟีลด์จำกัด

นางสาวปรัชญาพร เดิมหลิ่ม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563

GRAPH AND NUMBER THEORETIC PROPERTIES OF CERTAIN MAPS OVER FINITE FIELD

Miss Pratchayaporn Doemlim

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2020

Thesis Title	GRAPH AND NUMBER THEORETIC PROPERTIES OF CERTAIN MAPS OVER FINITE FIELD
By	Miss Pratchayaporn Doemlim
Field of Study	Mathematics
Thesis Advisor	Associate Professor Tuangrat Chaichana, Ph.D.
Thesis Co-advisor	Professor Vichian Laohakosol, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

. . . . Dean of the Faculty of Science

(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

. . . . Chairman

(Professor Yotsanan Meemark, Ph.D.)

. . . . Thesis Advisor

(Associate Professor Tuangrat Chaichana, Ph.D.)

. . . . Thesis Co-advisor

(Professor Vichian Laohakosol, Ph.D.)

. . . . Examiner

(Associate Professor Ouamporn Phuksuwan, Ph.D.)

. . . . External Examiner

(Assistant Professor Pattira Ruengsinsub, Ph.D.)

ปรัชญาพร เดิมหลิ่ม: สมบัติเชิงกราฟและเชิงทฤษฎีจำนวนของบางฟังก์ชันเหนือฟีลด์จำกัด. (GRAPH AND NUMBER THEORETIC PROPERTIES OF CERTAIN MAPS OVER FINITE FIELD) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : รศ.ดร. ตวงรัตน์ ไชยชนะ, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม : ศ.ดร. วิเชียร เลาหโกศล 0 หน้า.

ในวิทยานิพนธ์ฉบับนี้ เราศึกษากราฟเหนือฟีลด์จำกัด $\mathbb{F}_q$ เมื่อ q เป็นกำลังของจำนวนเฉพาะ ที่ได้จากการวนซ้ำของฟังก์ชัน $g(x) = x^p$ เมื่อ p เป็นจำนวนเฉพาะ เราได้แสดงสมบัติบางประการของกราฟนี้ ยกตัวอย่างเช่น กำหนดลักษณะเฉพาะของจุดยอด และหาจำนวนของวงที่มีความยาวเฉพาะ นอกจากนั้นยังหาค่าประมาณทางสถิติบางปริมาณที่เกี่ยวข้องกับความยาวของวง และความยาวหางของกราฟอีกด้วย

ภาควิชา	คณิตศาสตร์และ วิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต	....
สาขาวิชา	คณิตศาสตร์	ลายมือชื่อ อ.ที่ปรึกษาหลัก	....
ปีการศึกษา	2563	ลายมือชื่อ อ.ที่ปรึกษาร่วม	....

612003523: MAJOR MATHEMATICS

KEYWORDS: ITERATIONS, DIRECTED GRAPH, ORBIT, FINITE FIELD

PRATCHAYAPORN DOEMLIM : GRAPH AND NUMBER THEORETIC PROPERTIES OF CERTAIN MAPS OVER FINITE FIELD. ADVISOR : ASSOC PROF. TUANGRAT CHAICHANA, Ph.D., THESIS COADVISOR : PROF. VICHIAN LAOHAKOSOL, Ph.D., 0 pp.

In this thesis, we study the graph over a finite field $\mathbb{F}_q$, where q is a prime power, obtained by iterations of the map $g(x) = x^p$, where p is a prime number. Some properties of the graphs such as a characterization of their vertices and the number of cycles with specific length are showed. Moreover, some statistical estimates about the tail and cycle lengths of the related graphs are established.

Department:	Mathematics and Computer Science	Student's Signature	....
Field of Study:	Mathematics	Advisor's Signature	....
Academic Year:	2020	Co-advisor's signature	....

Acknowledgements

I am greatly indebted to Associate Professor Dr.Tuangrat Chaichana, my thesis advisor for their suggestion and helpful advice in preparing and writing this thesis.

It is difficult to express my gratitude to Professor Dr.Vichian Laohakosol, my thesis co-advisor for his enthusiasm, inspiration and great efforts to explain things clearly and simply.

I would like to express my special thanks to Professor Dr.Yotsanan Meemark, Associate Professor Dr.Ouamporn Phuksuwan and Assistant Professor Dr.Pattira Ruengsinsub, my thesis committees, for their suggestion and comment. I feel very thankful to all my teachers who have taught me all along.

In particular, I wish to express my thankfulness to Development and Promotion of Science and Technology Talents Project (DPST) for financial supports. I wish to thanks my dear friends for giving me good experiences at Chulalongkorn university.

Finally, I would like to express my deep gratitude to my beloved family for their love and encouragement throughout my graduate study.

CONTENTS

Page

Chapter I

PRELIMINARIES

Throughout, let q be a prime power, $\mathbb{F}_q$ the finite field of q elements and $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

1.1 Basic knowledge in Graph Theory

Let $g : \mathbb{F}_q^* \to \mathbb{F}_q^*$ be a function. The **iterates** of g are defined by $g^i(x) = g(g^{i-1}(x))$ for all $i \in \mathbb{N}$, where $g^0(x) = x$. The graph from the iteration of g is defined to be a directed graph $G_g = (V, E)$ whose vertex set is $V \subseteq \mathbb{F}_q^*$ and whose directed edges in E are given by $(x, g(x))$ for all $x \in \mathbb{F}_q^*$. The **reverse graph** of the graph G_g, denoted by $(G_g)_R$, is the graph (V, E_R), where $E_R := \{(x, y) : (y, x) \in E\}$. For general reference on graph theory, we refer to **?**.

Let $x \in \mathbb{F}_q^*$. An **orbit** of x is a directed path in a graph G_g of the map g starting at x, see Figure 1. Since $\mathbb{F}_q$ is finite, there exists the least positive integer $s := s(x)$ such that $g^s(x) \in \{g^0(x), g^1(x), \ldots, g^{s-1}(x)\}$. Let $t := t(x) \in \{0, 1, ..., s-1\}$ be the least non-negative integer such that $g^s(x) = g^t(x)$ and let $c := c(x) = s(x) - t(x)$. We then have c is the smallest positive integer such that $g^t(x) = g^{t+c}(x)$. The **tail** for x is the list of elements $x, g(x), g^2(x), \ldots, g^{t-1}(x)$ in the orbit of x and the **cycle** for x is the list of elements $g^t(x), \ldots, g^{t+c-1}(x)$ in the orbit of x. Note that the **tail length** of x is $t(x)$ and the **cycle length** of x is $c(x)$, see Figure 1.

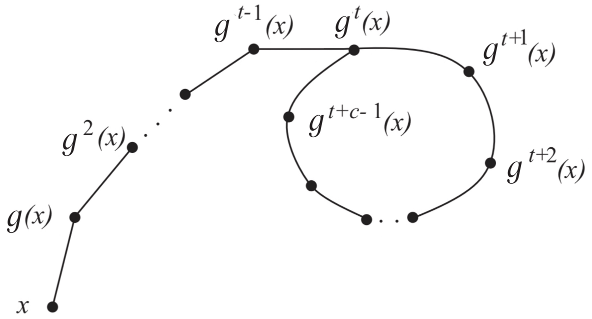
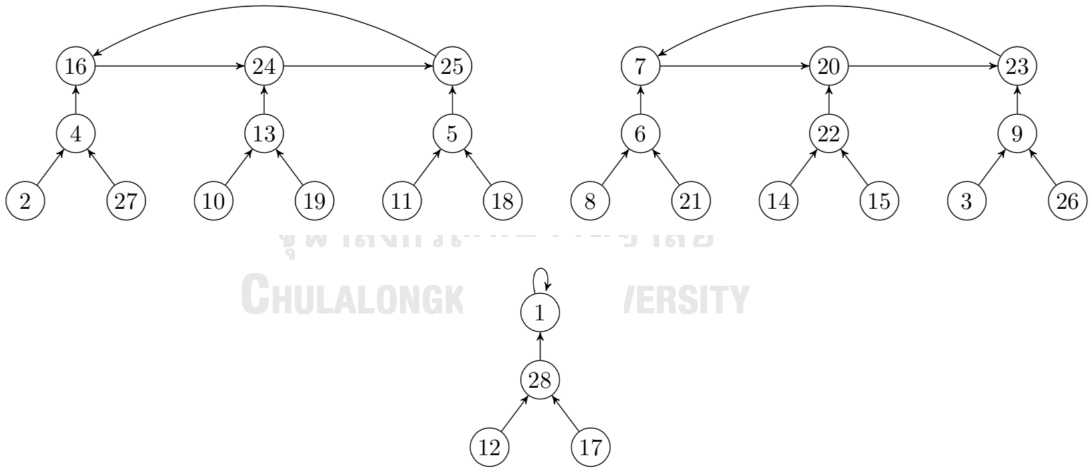


Figure 1. The orbit of x, tail and cycle for x.

Example 1.1.1. The graph from the iteration of $g(x) = x^2$ over $\mathbb{F}_{29}$ is shown as follows.

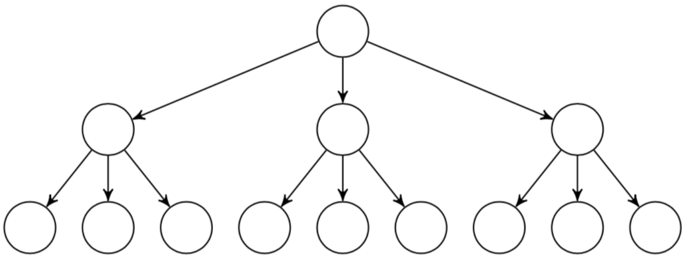


We can see that

x	$t(x)$	$c(x)$	x	$t(x)$	$c(x)$	x	$t(x)$	$c(x)$	x	$t(x)$	$c(x)$
1	0	1	8	2	3	15	2	3	22	1	3
2	2	3	9	1	3	16	0	3	23	0	3
3	2	3	10	2	3	17	2	1	24	0	3
4	1	3	11	2	3	18	2	3	25	0	3
5	1	3	12	2	1	19	2	3	26	2	3
6	1	3	13	1	3	20	0	3	27	2	3
7	0	3	14	2	3	21	2	3	28	1	3

Definition 1.1.2. ? Let $p, h \in \mathbb{N}$. A **complete *p*−tree of height *h***, denoted by B_h, is a directed graph with p^i nodes at depth i, for $0 \leq i \leq h$, with the property that every non-leaf node has exactly p children.

Example 1.1.3. A complete $3-$tree of height 2 is shown as follows.



1.2 Basic knowledge in Number Theory

Definition 1.2.1. ? Let $a, m \in \mathbb{Z}$ with $m > 0$ and gcd$(a, m) = 1$. The order of a modulo m, denote by ord$_m(a)$, is the least positive integer i such that $a^i \equiv 1$ (mod m).

Definition 1.2.2. ? Let p be a prime, and n an integer. The exponent of the largest power of p which divides n is denoted by $v_p(n)$.

Definition 1.2.3. ? Let $\alpha \in \mathbb{F}_q^*$. The **order** of α, denoted by ord(α), is the least positive integer i such that $\alpha^i = 1$.

Theorem 1.2.4. ? *Let $\alpha \in \mathbb{F}_q^*$ and $l \in \mathbb{N}$, $\alpha^l = 1$ if and only if ord$(\alpha) \mid l$.*

Theorem 1.2.5. ? *Let $\alpha \in \mathbb{F}_q^*$ and $k \in \mathbb{N}$. Then ord$(\alpha^k) = \frac{ord(\alpha)}{\gcd(ord(\alpha),k)}$.*

Theorem 1.2.6. ? *If $d|(q-1)$ then there exist $\varphi(d)$ elements of order d, where $\varphi(d)$ is the Euler phi function.*

Theorem 1.2.7. ? *Let F be a field. For $f \in F[x]$, the residue class ring $F[x]/(f)$ is a field if and only if f is irreducible over F.*

Theorem 1.2.8. ? *Let K be a field and F its field extension. Let $\theta \in F$ be algebraic of degree n over K and let g be the minimal polynomial of θ over K. Then $K(\theta)$ is isomorphic to $K[x]/(g)$.*

Theorem 1.2.9. ? *Let F be a finite field. Then F has p^n elements, where the prime p is the characteristic of F and n is the degree of F over its prime subfield.*

Example 1.2.10. We have $\mathbb{F}_8 = \frac{\mathbb{F}_2[x]}{<f(x)>}$ where $f(x) = x^3 + x + 1$ is irreducible. Let α be a root of $x^3 + x + 1$. From Theorem 1.2.8, $\mathbb{F}_8 \cong \{0, 1, \alpha, \alpha^2, \alpha + \alpha^2, 1 + \alpha, 1 + \alpha^2, 1 + \alpha + \alpha^2\}$.

Theorem 1.2.11. ? *For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.*

Definition 1.2.12. ? A generator of cyclic group $\mathbb{F}_q^*$ is called a **primitive element** of $\mathbb{F}_q$.

1.3 Our objectives

In 1996, T.D. Rogers **?** studied some properties of the graphs obtained from iterating the quadratic map $g(x) = x^2$ over $\mathbb{F}_p$, where p is a prime number. The formula of the number of cycles relative to g was derived as follows.

Theorem 1.3.1. **?** *For any positive integer n, let $\gamma(n)$ denote the number of cycles in the graph relative to the quadratic map. Then*

$$\gamma(n) = \sum_{d|m} \frac{\varphi(d)}{ord_d 2}$$

where $n = 2^k m$, m odd. The number of cycles then depends only on the odd factor m of n, so that $\gamma(n) = \gamma(m)$ and $d(m) \leq \gamma(m) \leq \frac{m}{2}$, where $d(m)$ is the number of divisors of m.

In 2004, T. Vasiga and J. Shallit **?** studied some properties of the graph obtained from iterating the quadratic map $g(x) = x^2$ over a finite field $\mathbb{F}_p$, where p is an odd prime. They characterized the vertices of the directed graph $G_{x \to x^2}$ in terms of primitive elements as follows.

Theorem 1.3.2. **?** *Let γ be a primitive root mod p. Then*

(a) $\{a \in \mathbb{F}_p^* : t(a) = 0\} = \{\gamma^i : 0 < i < p$ and $v_2(i) \geq v_2(p-1)\}$;

(b) For $1 \leq k \leq v_2(p-1)$, we have

$$\{a \in \mathbb{F}_p^* : t(a) = k\} = \{\gamma^i : 0 < i < p \text{ and } v_2(i) = v_2(p-1) - k\}.$$

Next, they gave the formulas for the length of tail $t(x)$ and the length of cycle $c(x)$ for particular x in the vertex set V as follows.

Theorem 1.3.3. **?** *For each $x \in \mathbb{F}_p^*$, we have $t(x) = v_2(ord_p x)$ and $c(x)$ =$ord_l 2$, where $ord_p x = 2^e l$ and e, l are non-negative integers with l is odd.*

Theorem 1.3.4. **?** *Let $p - 1 = 2^\tau \rho$, where ρ is odd. For each positive integer divisor d of ρ, the graph G_g; $g(x) = x^2$ contains $\frac{\varphi(d)}{ord_d 2}$ cycles of length $ord_d 2$. There are ρ elements in all these cycles, and off each element in these cycles there hang reversed complete binary trees of height $\tau - 1$ containing $2^\tau - 1$ elements.*

Theorem 1.3.5. **?** *The structure of the digraph $G_{x\to x^2}$ for a prime p when $p = 2^{2^k}+1$, a Fermat prime, is a reversed complete binary tree of height $2^k - 1$ with root -1, attached to a cycle of length 1 on the integer 1. The elements $x \in \mathbb{F}_p$ with $t(x) = a$ for $0 \leq a \leq 2^k$ are given by $3^{e\cdot 2^{2^k-a}}, 0 \leq e < 2^a$, where e is odd.*

Theorem 1.3.6. **?** *When $p = 2^q - 1$, a Mersenne prime, the digraph $G_{x\to x^2}$ consists of cycles whose length divides $q - 1$. Off each element in these cycles there hangs a single element with tail length 1.*

Some statistics about tail and cycle lengths for the iteration of $x \to x^2$ over $\mathbb{F}_p^*$ were also studied in **?**.

Definition 1.3.7. **?** For iterates of $x \to x^2 \mod p$, define

- $TC(p) :=$ total number of cycles;
- $T_0(p) :=$ total number of elements in all cycles, i.e., the number of $a \in \mathbb{F}_p^*$ with $t(a) = 0$;
- $AC(p) :=$ average length of a cycle;
- $C(p) :=$ average value of $c(a)$ for all $a \in \mathbb{F}_p^*$;
- $T(p) :=$ average value of $t(a)$ for all $a \in \mathbb{F}_p^*$.

Then they found the following result.

Theorem 1.3.8. **?** *Let $p - 1 = 2^\tau\rho$, where ρ is odd and consider the iteration of $x \mapsto x^2 \mod p$. Then*

1. $TC(p) = \sum\limits_{d|\rho} \frac{\varphi(d)}{ord_d 2}$;

2. $T_0(p) = \rho$;

3. $AC(p) = \frac{\rho}{TC(p)}$;

4. $C(p) = \frac{1}{\rho}\sum_{d|\rho}\varphi(d)ord_d 2$;

5. $T(p) = \frac{1}{p-1}\sum_{d|p-1}\varphi(d)v_2(d) = \tau - 1 + 2^{-\tau}$.

Next, for a positive integer N, consider some quantities over all odd primes $p \leq N$.

Definition 1.3.9. ? With respect to the iteration of $x \to x^2 \mod p$, define

- $ST_0(N) := \sum_{2<p\leq N} T_0(p)$;
- $ST(N) := \sum_{2<p\leq N}\sum_{1\leq a<p} t_p(a)$.

Definition 1.3.10. ? Let x, k, l be positive integers. Denote $\pi(x, l, k)$ the number of primes $p \leq x$ which are congruent to $k \mod l$.

Definition 1.3.11. ? Let f, g be functions from non-negative real numbers to non-negative real numbers, $f = O(g)$ if there exist constants $c > 0$ and $n_0 \geq 0$ such that $f(n) \leq cg(n)$ for all $n \geq n_0$.

Definition 1.3.12. ? Let function $f(x)$ and $g(x)$, define $f(x) \sim g(x)$ as $x \to \infty$ if and only if

$$\lim_{x\to\infty}\frac{f(x)}{g(x)} = 1.$$

Lemma 1.3.13. ? *Extended Riemann Hypothesis* (ERH) *:*

Let k and l be relatively prime integers. Then for any $\epsilon > 0$, we have

$$\pi(x, l, k) = \frac{li(x)}{\varphi(l)} + O(x^{1/2+\epsilon}),$$

where $li(x) = \frac{x}{\log x}\Big(1 + O(\frac{1}{\log x})\Big)$.

Lemma 1.3.14 (?). *Assume the* ERH. *Then, if the logarithmic integral $li(x)$ is defined by $li(x) = \int_2^x \frac{1}{\log t}dt$ and k, l are integers with* $\gcd(k,l) = 1$, *then*

$$\pi(x,l,k) = \frac{li(x)}{\varphi(l)} + O(\sqrt{x}(\log x + 2\log l)).$$

By assuming ERH, they established the asymptotic estimates for the sums of some average quantities as follows.

Theorem 1.3.15. ? *Assume the* ERH. *Then*

$$ST_0(N) \sim \frac{N^2}{6\log N}.$$

Theorem 1.3.16. ? *Assume the* ERH. *Then*

$$ST(N) \sim \frac{2}{3}\frac{N^2}{\log N}.$$

In this thesis, we study the graphs obtained from the iteration of a certain map $g : x \to x^p$, where p is prime, over $\mathbb{F}_q^*$ extending the ideas of **?** and **?**. In Chapter II, structures of the graphs, characterization of vertices of the graphs in term of primitive elements in $\mathbb{F}_q^*$ and numerical values for the number of cycles with specific length are investigated. In the last chapter, statistical estimates about the tail and cycle lengths such as the approximation $ST_0(N)$ and $ST(N)$ are shown.

Chapter II

STRUCTURE OF A GRAPH $G_{x\to x^p}$

In this chapter, for a fixed prime p, we consider the graph over a finite field $\mathbb{F}_q^*$ where q is a prime power, obtained by the iteration of the map $g : \mathbb{F}_q^* \to \mathbb{F}_q^*$ defined by $g(x) = x^p$. The formulas of the tail length and cycle length of each element in $\mathbb{F}_q^*$ are shown as follows.

Theorem 2.0.17. *Let $\alpha \in \mathbb{F}_q^*$ and ord$(\alpha) = p^e l$ where $e \in \mathbb{N} \cup \{0\}$ and $l \in \mathbb{N}$ with* gcd$(p, l) = 1$. *If $t := t(\alpha)$ is the tail length for α and $c := c(\alpha)$ is the cycle length for α, then $t = v_p($ord$(\alpha))$ and $c =$ord$_l p$.*

Proof. Let $\alpha \in \mathbb{F}_q^*$. We have $g^t(\alpha) = g^{t+c}(\alpha)$. Then $\alpha^{p^t} = \alpha^{p^{t+c}}$ and so

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

Therefore, we obtain $p^e l | p^t(p^c - 1)$. Since gcd$(p^e, p^c - 1) = 1 =$ gcd(l, p^t), $p^e | p^t$ and $l | (p^c - 1)$. We first show that $t = e = v_p(\text{ord}(\alpha))$. Obviously, $e \le t$. If $e < t$, then $p^e < p^t$. Since t is the smallest nonnegative integer such that $g^t(\alpha) = g^{t+c}(\alpha)$, we have $g^e(\alpha) = g^{e+c}(\alpha)$ and so

$$\alpha^{p^e(p^c-1)} = \alpha^{p^{e+c}-p^e} \neq 1$$

which contradicts with the fact that $p^e l | p^t(p^c - 1)$. Hence the first part of the theorem is done. Next, we will show that ord$_l p = c$. Since $l | (p^c - 1)$,

$$p^c = 1(\text{mod } l).$$

Then ord$_l p \le c$. Suppose that there exists $d \in \mathbb{N}$ such that $1 \le d < c$ and

$$p^d = 1(\text{mod } l).$$

Then $l|(p^d-1)$ and so $p^e l | p^t(p^d-1)$. This implies that

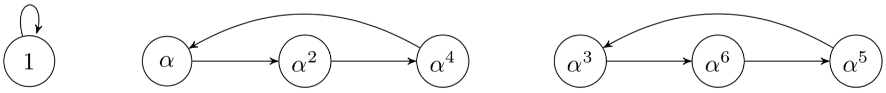
$$\alpha^{p^{t+d}-p^t} = \alpha^{p^t(p^d-1)} = 1.$$

Consequently, $g^{t+d}(\alpha) = g^t(\alpha)$ which contradicts the minimal of c. □

Note that, from the above theorem, $t(\alpha) = v_p(d)$ for some $d|(q-1)$.

Example 2.0.18. Consider the graph of $g(x) = x^2$ for $q = 8$.

Here $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ where $\alpha \in \mathbb{F}_8^*$ saitisfying $\alpha^3 + \alpha + 1 = 0$.



By Theorem **??**, the tail length and the cycle length for all $x \in \mathbb{F}_8^*$, are shown as follows.

x	ord$(x) = 2^e l$	$t(x) = v_2($ord$(x))$	$c(x) =$ord$_l 2$
1	$1 = 2^0 \cdot 1$	0	1
α	$7 = 2^0 \cdot 7$	0	3
α^2	$7 = 2^0 \cdot 7$	0	3
α^3	$7 = 2^0 \cdot 7$	0	3
α^4	$7 = 2^0 \cdot 7$	0	3
α^5	$7 = 2^0 \cdot 7$	0	3
α^6	$7 = 2^0 \cdot 7$	0	3

Example 2.0.19. Consider the graph of $g(x) = x^3$ over $\mathbb{F}_{109}^*$.

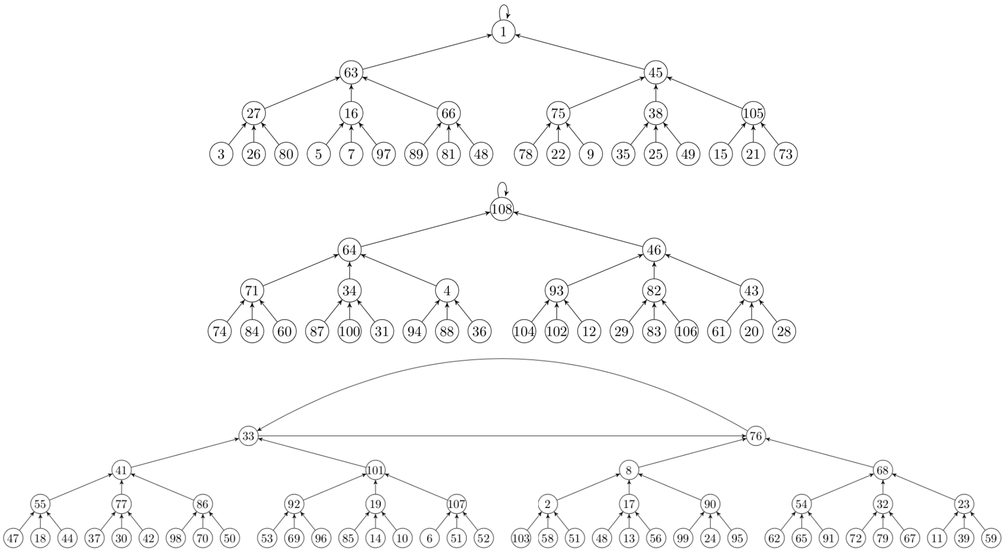


Figure 2. The graph of $g(x) = x^3$ over $\mathbb{F}_{109}^*$.

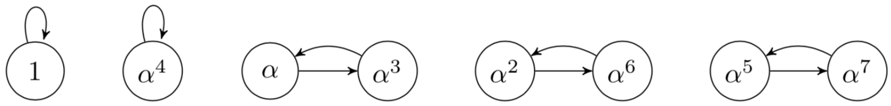
By Theorem **??**, we compute the tail length and the cycle length of each element in $\mathbb{F}_{109}^*$, as shown in the following table.

x	ord(x)	$t(x)$	$c(x)$	x	ord(x)	$t(x)$	$c(x)$	x	ord(x)	$t(x)$	$c(x)$
1	1	0	1	37	108	3	2	73	27	3	1
2	36	2	2	38	9	2	1	74	54	3	1
3	27	3	1	39	108	3	2	75	9	2	1
4	18	2	1	40	108	3	2	76	4	0	2
5	27	3	1	41	12	1	2	77	36	2	2
6	108	3	2	42	108	3	2	78	27	3	1
7	27	3	1	43	18	2	1	79	108	3	2
8	12	1	2	44	108	3	2	80	27	3	1
9	27	3	1	45	3	1	1	81	27	3	1
10	108	3	2	46	6	1	1	82	18	2	1
11	108	3	2	47	108	3	2	83	54	3	1
12	54	3	1	48	27	3	1	84	54	3	1
13	108	3	2	49	27	3	1	85	108	3	2
14	108	3	2	50	108	3	2	86	36	2	2
15	27	3	1	51	108	3	2	87	54	3	1
16	9	2	1	52	108	3	2	88	54	3	1
17	36	2	2	53	108	3	2	89	27	3	1
18	108	3	2	54	36	2	2	90	36	2	2
19	36	2	2	55	36	2	2	91	108	3	2
20	54	3	1	56	108	3	2	92	36	2	2
21	27	3	1	57	108	3	2	93	18	2	1
22	27	3	1	58	108	3	2	94	54	3	1
23	36	0	3	59	108	3	2	95	108	3	2
24	108	3	2	60	54	3	1	96	108	3	2
25	27	3	1	61	54	3	1	97	27	3	1

x	ord(x)	$t(x)$	$c(x)$	x	ord(x)	$t(x)$	$c(x)$	x	ord(x)	$t(x)$	$c(x)$
26	27	3	1	62	108	3	2	98	108	3	2
27	9	2	1	63	3	1	1	99	108	3	2
28	54	3	1	64	6	1	1	100	54	3	1
29	54	3	1	65	108	3	2	101	12	1	2
30	108	3	2	66	9	2	1	102	54	3	1
31	54	3	1	67	108	3	2	103	108	3	2
32	36	2	2	68	12	1	2	104	54	3	1
33	4	0	2	69	108	3	2	105	9	2	1
34	18	2	1	70	108	3	2	106	54	3	1
35	27	3	1	71	18	2	1	107	36	2	2
36	54	3	1	72	108	3	2	108	2	0	1

Example 2.0.20. Consider the graph of $g(x) = x^3$ for $q = 9$.

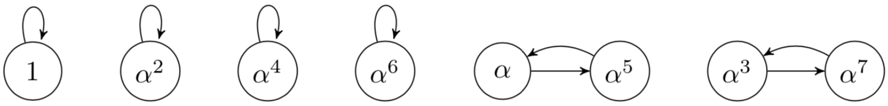
Here, $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ where $\alpha \in \mathbb{F}_9^*$ satisfying $\alpha^2 + 1 = 0$.



By Theorem **??**, the tail length and the cycle length for all $x \in \mathbb{F}_9^*$ are as in the following table.

x	ord$(x) = 3^e l$	$t(x) = v_3($ord$(x))$	$c(x) =$ord$_l 3$
1	$1 = 3^0 \cdot 1$	0	1
α	$8 = 3^0 \cdot 8$	0	2
α^2	$4 = 3^0 \cdot 4$	0	2
α^3	$8 = 3^0 \cdot 8$	0	2
α^4	$2 = 3^0 \cdot 2$	0	1
α^5	$8 = 3^0 \cdot 8$	0	2
α^6	$4 = 3^0 \cdot 4$	0	2
α^7	$8 = 3^0 \cdot 8$	0	2

Example 2.0.21. Consider the graph of $g(x) = x^5$ for $q = 9$.

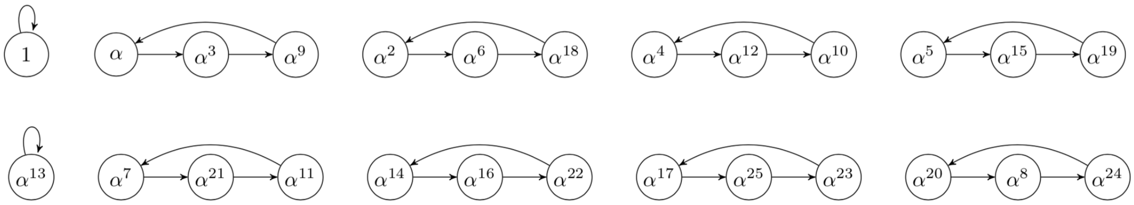


By Theorem **??**, the tail length and the cycle length for all $x \in \mathbb{F}_9^*$ are as in the following table.

x	ord$(x) = 5^e l$	$t(x) = v_5($ord$(x))$	$c(x) =$ord$_l 5$
1	$1 = 5^0$	0	1
α	$8 = 5^0 \cdot 8$	0	2
α^2	$4 = 5^0 \cdot 4$	0	1
α^3	$8 = 5^0 \cdot 8$	0	2
α^4	$2 = 5^0 \cdot 2$	0	1
α^5	$8 = 5^0 \cdot 8$	0	2
α^6	$4 = 5^0 \cdot 4$	0	1
α^7	$8 = 5^0 \cdot 8$	0	2

Example 2.0.22. Consider the graph of $g(x) = x^3$ for $q = 27$.

Here, $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ where $\alpha \in \mathbb{F}_{27}^*$ satisfying $\alpha^3 + 2\alpha^2 + 1 = 0$.



By Theorem **??**, the tail length and the cycle length for all $x \in \mathbb{F}_{27}^*$ are as in the following table.

x	ord(x)	$t(x)$	$c(x)$	x	ord(x)	$t(x)$	$c(x)$
α	26	0	3	α^{14}	13	0	3
α^2	13	0	3	α^{15}	26	0	3
α^3	26	0	3	α^{16}	13	0	3
α^4	13	0	3	α^{17}	26	0	3
α^5	26	0	3	α^{18}	13	0	3
α^6	13	0	3	α^{19}	26	0	3
α^7	26	0	3	α^{20}	13	0	3

x	ord(x)	$t(x)$	$c(x)$	x	ord(x)	$t(x)$	$c(x)$
α^8	13	0	3	α^{21}	26	0	3
α^9	26	0	3	α^{22}	13	0	3
α^{10}	13	0	3	α^{23}	26	0	3
α^{11}	26	0	3	α^{24}	13	0	3
α^{12}	13	0	3	α^{25}	26	0	3
α^{13}	2	0	1	$\alpha^{26} = 1$	1	0	1

The next theorem provides the characterization of vertices of the graph in terms of primitive elements in $\mathbb{F}_q^*$.

Theorem 2.0.23. *Let γ be a primitive element of $\mathbb{F}_q^*$. Then*

1. $\{a \in \mathbb{F}_q^* : t(a) = 0\} = \{\gamma^i : 1 \leq i \leq q-1$ *and* $v_p(i) \geq v_p(q-1)\}$*;*

2. For $1 \leq k \leq v_p(q-1)$*, we have*

$$\{a \in \mathbb{F}_q^* : t(a) = k\} = \{\gamma^i : 1 \leq i \leq q-1 \text{ and } v_p(i) = v_p(q-1) - k\}.$$

Proof. Let $q - 1 = p^\tau \rho$, where $\gcd(p, \rho) = 1$.

1. Let $a \in \mathbb{F}_q^*$ with $t(a) = 0$. Then $a = \gamma^i$ for some $1 \leq i \leq q-1$, and there is $l \geq 1$ such that

$$a = g^0(a) = g^{l+0}(a) = a^{p^l}$$

Then we have $a^{p^l-1} = 1$ and so $(\gamma^i)^{p^l-1} = 1$. Therefore $p^\tau\rho | i(p^l - 1)$. Since $\gcd(p^\tau, \rho) = 1$, $p^\tau | i$. Hence $v_p(i) \geq \tau = v_p(q-1)$.

Conversely, consider $\gamma^i \in \mathbb{F}_q^*$, where $1 \leq i \leq q-1$ and $v_p(i) \geq v_p(q-1) = \tau$. We get $p^\tau | i$. Choose $l = \mathrm{ord}_\rho p$. Then $p^l \equiv 1 \pmod{\rho}$; that is, $\rho | (p^l - 1)$. Therefore $p^\tau\rho | i(p^l - 1)$. Thus $(\gamma^i)^{p^l-1} = 1$. Now we have $\gamma^{ip^l} = \gamma^i$. It follows that $g^l(\gamma^i) = g^0(\gamma^i)$. By the definition of the length of tail, $t(\gamma^i) = 0$.

2. Let $k \in \mathbb{N}$ be such that $1 \leq k \leq v_p(q-1)$. Let $a \in \mathbb{F}_q^*$ with $t(a) = k$. Then $a = \gamma^i$ for some $1 \leq i \leq q-1$ and there exists $l > 0$ such that

$$g^k(a) = g^{k+l}(a) \text{ and } g^{k-1}(a) \neq g^{k-1+l}(a).$$

Then we have

$$(\gamma^i)^{p^k} = (\gamma^i)^{p^{k+l}} \text{ and } (\gamma^i)^{p^{k-1}} \neq (\gamma^i)^{p^{k-1+l}}.$$

Consequently, we get

$$(\gamma^i)^{p^{k+l}-p^k} = 1 \text{ and } (\gamma^i)^{p^{k-1+l}-p^{k-1}} \neq 1.$$

Then $(q-1)|ip^k(p^l-1)$ and $(q-1)ip^{k-1}(p^l-1)$.

We claim that $p^\tau ip^{(k-1)}$. To prove claim, write $i = p^r w$, where gcd$(p,w) = 1$. Suppose that $p^\tau|ip^{(k-1)}$. Then $p^\tau|p^r wp^{k-1}$. Since gcd$(p,w) = 1$, $p^\tau|p^r p^{k-1}$. From $p^\tau \rho|p^r wp^k(p^l-1)$ and gcd$(\rho, p) = 1$, we have $\rho|w(p^l-1)$. Therefore $p^\tau \rho|p^r wp^{k-1}(p^l-1)$; that is, $(q-1)|ip^{k-1}(p^l-1)$ which is a contradiction. Note that $p^\tau|ip^k$.

By claim, we get $v_p(p^\tau) = v_p(ip^k)$. Now we obtain $\tau = v_p(i) + k$ and so

$$v_p(i) = \tau - k = v_p(q-1) - k.$$

Conversely, consider $\gamma^i \in \mathbb{F}_q^*$ where $1 \leq i \leq q-1$ and $v_p(i) = v_p(q-1) - k$. Then we have

$$v_p(ip^k) = v_p(q-1) = v_p(p^\tau \rho).$$

Therefore $p^\tau|ip^k$ but $p^\tau ip^{k-j}$ for all $1 \leq j \leq k$. By the first claim, there exists $l \geq 1$ such that $\rho|(p^l-1)$. Then $(q-1)|ip^k(p^l-1)$ and $(q-1)ip^{k-j}(p^l-1)$ for all $1 \leq j \leq k$. So $(\gamma^i)^{p^k(p^l-1)} = 1$ and $(\gamma^i)^{p^{k-j}(p^l-1)} \neq 1$ for all $1 \leq j \leq k$. We then have $g^k(\gamma^i) = g^{k+l}(\gamma^i)$ and $g^{k-1}(\gamma^i) \neq g^{k-1+l}(\gamma^i)$. Hence k is the smallest such that $g^k(\gamma^i) = g^{k+l}(\gamma^i)$. By the definition of the tail length $t(\gamma^i) = k$. □

Theorem 2.0.24. *Let* $q-1=p^\tau\rho$*, where* $\tau\in\mathbb{N}\cup\{0\}$ *and* $\rho\in\mathbb{N}$ *with* $\gcd(p,\rho)=1$.

1. *The total number of elements in all cycles is* ρ*.*

2. *For each positive integer divisor* d *of* ρ*,* $G_{x\to x^p}$ *contains* $\frac{\varphi(d)}{ord_d p}$ *cycles of length* $ord_d p$*.*

3. *Off each element in these cycles there hang reversed complete binary* $p-$*tree of height* $\tau-1$ *containing* $\frac{p^\tau-1}{p-1}$ *elements.*

Proof. Let γ be a primitive element over $\mathbb{F}_q^*$. Let $x\in\mathbb{F}_q^*$ and $q-1=p^\tau\rho$ with $\gcd(p,\rho)=1$.

1. If x is in the cycle, we have $t(x)=0$. By Theorem **??** (1), $x=\gamma^i$ where $1\leq i\leq q-1$ and $v_p(i)\geq v_p(q-1)=\tau$. So x must be of the form $x=\gamma^{jp^\tau}$, where $1\leq j\leq\rho$. Hence the total number of elements in all cycles is ρ.

2. Note that $\text{ord}(\gamma^{p^\tau})=\frac{p^\tau\rho}{\gcd(p^\tau,p^\tau\rho)}=\rho$. From (1) we have

$$\{\gamma^i:1\leq i\leq q-1 \text{ and } v_p(i)\geq v_p(q-1)\}=<\gamma^{p^\tau}>,$$

a cyclic group of order ρ. We know that if $d|\rho$, there are $\varphi(d)$ elements of order d. Note that $\text{ord}(\gamma^{p^\tau\frac{\rho}{d}})=\frac{\rho}{\gcd(\rho,\frac{\rho}{d})}=d$. Then, for all $1\leq j<d$ and $\gcd(j,d)=1$, then $\text{ord}(\gamma^{\frac{p^\tau\rho}{d}})^j=\frac{d}{\gcd(j,d)}=d$. Therefore, the elements of order d are given by $\gamma^{jp^\tau\frac{\rho}{d}}$ for $1\leq j<d$ and $\gcd(j,d)=1$. Since $\text{ord}(\gamma^{jp^\tau\frac{\rho}{d}})=p^0d$, by Theorem **??**, $c(\gamma^{jp^\tau\frac{\rho}{d}})=\text{ord}_dp$. Hence for all $d|\rho$, $G_{x\to x^p}$ contains $\frac{\varphi(d)}{\text{ord}_dp}$ cycles of length ord_dp.

3. An element $x\in\mathbb{F}_q^*$ with $t(x)=1$, which $x^p=\gamma^{jp^\tau}$ in cycle is one of those of the form $\gamma^{jp^{\tau-1}}$ where $1\leq j\leq p-1$. In general, if γ^i is an element with tail length t $(1\leq t\leq\tau)$, the element with tail length $t+1$ are

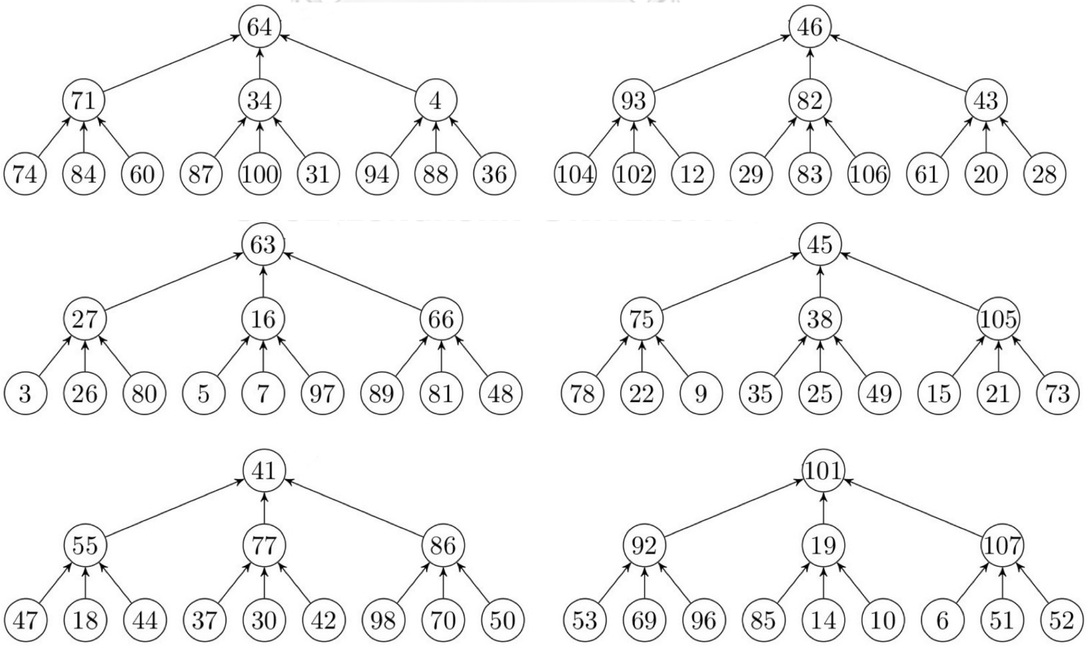
$$\gamma^{\frac{i+j(q-1)}{p}} \text{ for } 0\leq j\leq p-1.$$

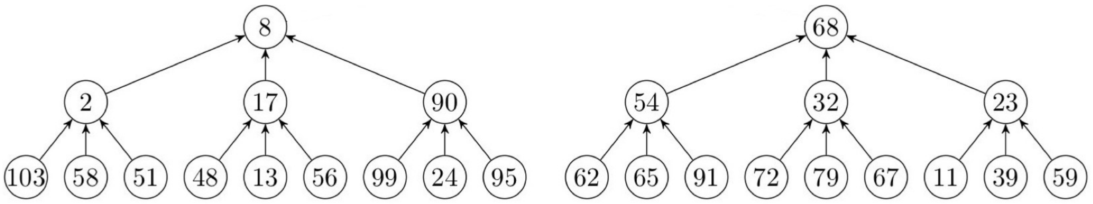
Since the longest tail length is τ, we have the reversed complete binary $p-$tree of height $\tau - 1$ containing $1 + p + p^2 + ... + p^{\tau-1} = \frac{p^\tau - 1}{p-1}$ elements. □

Example 2.0.25. The graph of $g(x) = x^3$ over $\mathbb{F}_{109}^*$. We have $108 = 3^3 4$ with $\rho = 4$. Moreover, it is easily seen from Figure 2 that the total number of elements in all cycles is $\rho = 4$. The table shows the number of cycles of length ord$_d$3 for each $d|\rho$.

d	$\varphi(d)$	$c = ord_d 3$	cycle
1	1	1	1
2	1	1	1
4	2	2	1

From Figure 2, off each element in the cycles there hang reversed complete 3-tree of height 2 containing $\frac{3^3-1}{3-1} = 13$ elements as in the following figure.




8
2
17
90
103
58
51
48
13
56
99
24
95
68
54
32
23
62
65
91
72
79
67
11
39
59

Chapter III

SOME STATISTICAL RESULTS

3.1 Averages of some quantities

In this section, we consider some statistics about tail and cycle lengths for the iteration of the map $x \to x^p$ over $\mathbb{F}_q^*$.

Definition 3.1.1. With respect to the iteration of $x \to x^p$, we define

- $TC(q) :=$ total number of cycles;
- $T_0(q) :=$ total number of elements in all cycles, i.e., the number of $a \in \mathbb{F}_q^*$ with $t(a) = 0$;
- $AC(q) :=$ average length of a cycle;
- $C(q) :=$ average value of $c(a)$ for all $a \in \mathbb{F}_q^*$;
- $T(q) :=$ average value of $t(a)$ for all $a \in \mathbb{F}_q^*$.

Then we have the following results.

Theorem 3.1.2. *Let* $q-1 = p^\tau \rho$ *where* $\gcd(p, \rho) = 1, \tau \geq 0$. *We have*

1. $TC(q) = \sum\limits_{d|\rho} \frac{\varphi(d)}{ord_d p}$;
2. $T_0(q) = \rho$;
3. $AC(q) = \frac{\rho}{TC(q)}$;
4. $C(q) = \frac{1}{\rho} \sum\limits_{d|\rho} \varphi(d) ord_d p$;

5. $T(q) = \frac{1}{q-1}\sum\limits_{d|q-1}\varphi(d)v_p(d) = \tau - \frac{p^\tau-1}{p^\tau(p-1)}$.

Proof. 1. By Theorem **??** (2), for each positive divisor d of ρ, the graph $G_{x\to x^p}$ contains $\frac{\varphi(d)}{\text{ord}_d p}$ cycles. Then

$$TC(q) = \sum_{d|\rho}\frac{\varphi(d)}{\text{ord}_d p}.$$

2. It follows directly from Theorem **??** (1) that

$$T_0(q) = \rho.$$

3. By Definition **??** and (2), we have

$$AC(q) = \frac{T_0(q)}{TC(q)} = \frac{\rho}{TC(q)}.$$

4. By Definition **??**, we have

$$C(q) = \frac{1}{q-1}\sum_{\alpha\in\mathbb{F}_q^*}c(\alpha).$$

Note that for each positive divisor d of ρ, the corresponding subgraphs have the same cycle lengths. Let $d \in \mathbb{N}$ be such that $d|\rho$. Consider a subgraph corresponding to d, by Theorem **??** (2), there are ord$_d p$ elements in each cycle. Each element in the cycle has $\frac{p^\tau-1}{p-1}$ elements in the $p-$tree reversed graph and $p-1$ elements of height 0. Then there are ord$_d p + (p-1)\frac{p^\tau-1}{p-1}ord_d p$ elements in this subgraph. By Theorem **??** (1) there are $\frac{\varphi(d)}{\text{ord}_d p}$ subgraphs whose cycle length is ord$_d p$. This implies that

$$\begin{aligned} C(q) &= \frac{1}{q-1}\sum_{d|\rho}\frac{\varphi(d)}{\text{ord}_d p}\text{ord}_d p\Big(\text{ord}_d p + (p-1)\frac{p^\tau-1}{p-1}\text{ord}_d p\Big) \\ &= \frac{1}{p^\tau\rho}p^\tau\sum_{d|\rho}\varphi(d)\text{ord}_d p \\ &= \frac{1}{\rho}\sum_{d|\rho}\varphi(d)\text{ord}_d p \end{aligned}$$

5. By Theorem **??**, we have $t(\alpha) = v_p(d)$, for some $d|(q-1)$. Then

$$\begin{aligned}
T(q) &= \frac{1}{q-1}\sum_{\alpha\in\mathbb{F}_q^*} t(\alpha) = \frac{1}{q-1}\sum_{d|q-1}\varphi(d)v_p(d) = \frac{1}{q-1}\sum_{d|p^\tau\rho}\varphi(d)v_p(d)\\
&= \frac{1}{q-1}\sum_{d|\rho}\sum_{0\le i\le\tau}\varphi(dp^i)v_p(dp^i)\\
&= \frac{1}{q-1}\sum_{d|\rho}\sum_{0\le i\le\tau}\varphi(d)\varphi(p^i)(v_p(d)+v_p(p^i))\\
&= \frac{1}{q-1}\sum_{d|\rho}\varphi(d)\sum_{0\le i\le\tau}\varphi(p^i)\cdot i\\
&= \frac{1}{q-1}\sum_{d|\rho}\varphi(d)(p-1)\sum_{0\le i\le\tau}p^{i-1}\cdot i\\
&= \frac{1}{q-1}\rho(p-1)\sum_{0\le i\le\tau}p^{i-1}\cdot i\\
&= \frac{1}{p^\tau}(p-1)\frac{d}{dp}\Big(\sum_{0\le i\le\tau}p^i\Big)\\
&= \frac{1}{p^\tau}(p-1)\frac{d}{dp}\Big(\frac{p^{\tau+1}-1}{p-1}\Big)\\
&= \frac{1}{p^\tau}(p-1)\frac{(p-1)(\tau+1)p^\tau-(p^{\tau+1}-1)}{(p-1)^2}\\
&= \frac{1}{p^\tau}\frac{(p-1)(\tau p^\tau+p^\tau)-(p^{\tau+1}-1)}{(p-1)}\\
&= \frac{1}{p^\tau}\Big(\tau p^\tau-\frac{p^\tau-1}{p-1}\Big)\\
&= \tau-\frac{p^\tau-1}{p^\tau(p-1)}.
\end{aligned}$$

□

3.2 Asymptotic estimates of some quantities

In this section, we consider sums of average quantities over all primes $q \le N$ where $N \in \mathbb{N}$.

Definition 3.2.1. With respect to the iteration of map $x \to x^p$ over $\mathbb{F}_q^*$, we define

- $ST_0(N) := \sum_{q\le N} T_0(q)$;

- $ST(N) := \sum_{q \le N} \sum_{1 \le a < q} t_q(\alpha)$, where $t_q(\alpha)$ is a tail length of α over $\mathbb{F}_q^*$.

Next, we assume the extended Riemann hypothesis (ERH) and recall the following lemma.

Lemma 3.2.2. **?** *Assume the* ERH. *Let* k, l *be integers with* $\gcd(k, l) = 1$. *Then*

$$\sum_{\substack{p \le x \\ p \equiv k \ (mod\ l) \\ p \text{ is prime}}} p = \frac{1}{\varphi(l)} \Big(\frac{x^2}{2 \log x} \Big) \Big(1 + O\Big(\frac{1}{\log x} \Big) \Big) + O(x^{3/2}(\log x + 2 \log l)).$$

We now consider the behaviour of $ST_0(N)$ and $ST(N)$ as follows.

Theorem 3.2.3. *Assume the* ERH. *Then*

$$ST_0(N) \sim \frac{1}{2(p^2-1)} \frac{N^2}{\log N}.$$

Proof. We know that $ST_0(N) := \sum_{q \le N} T_0(q)$. From Theorem **??**, $T_0(q) = \frac{q-1}{p^{v_p(q-1)}}$. We then have

$$\begin{aligned} ST_0(N) &= \sum_{q \le N} T_0(q) \\ &= \sum_{q \le N} \frac{q-1}{p^{v_p(q-1)}} \\ &= \sum_{0 \le i \le \log_p N} \sum_{\substack{q \le N \\ p^i || (q-1)}} \frac{q-1}{p^i}. \end{aligned}$$

Claim 1. For each $i \in \mathbb{N}_0$, if $p^i || (q-1)$,then there exists $r \in \mathbb{N}$ such that $r < p$ and $q - 1 \equiv rp^i \pmod{p^{i+1}}$.

Proof of Claim 1. Let i be a non-negative integer.

Assume that $p^i || (q-1)$. Then $p^i | (q-1)$ and $p^{i+1}(q-1)$. So there exists $l \in \mathbb{N}$ such that $q - 1 = p^i l$. Since $p^{i+1}(q-1)$, there are $k, r \in \mathbb{N}_0$ such that $1 \le r < p$ and $l = pk + r$. Then

$$q - 1 = p^i(pk + r) = p^{i+1}k + rp^i.$$

Hence we have $q-1\equiv rp^i \pmod{p^{i+1}}$ as required.

Now we have

$$\begin{aligned}ST_0(N) &= \sum_{0\le i\le \log_p N}\ \sum_{\substack{q\le N\\ q\equiv rp^i+1 \pmod{p^{i+1}}}} \frac{q-1}{p^i}\\ &= \sum_{0\le i\le \log_p N}\frac{1}{p^i}\sum_{\substack{q\le N\\ q\equiv rp^i+1 \pmod{p^{i+1}}}}(q-1)\\ &= \sum_{0\le i\le \log_p N}\frac{1}{p^i}\Big(\sum_{\substack{q\le N\\ q\equiv rp^i+1 \pmod{p^{i+1}}}} q-\sum_{\substack{q\le N\\ q\equiv rp^i+1 \pmod{p^{i+1}}}} 1\Big).\end{aligned}$$

Note that, by Lemma **??**,

$$\begin{aligned}\sum_{\substack{q\le N\\ q\equiv rp^i+1 \pmod{p^{i+1}}}} q =&\frac{1}{\varphi(p^{i+1})}\Big(\frac{N^2}{2\log N}\Big)\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)+O(N^{3/2}(\log N+2\log(p^{i+1})))\\ =&\frac{1}{\varphi(p^{i+1})}\Big(\frac{N^2}{2\log N}\Big)\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)+O(N^{3/2}(\log N)\end{aligned}$$

and by Definition **??**,

$$\sum_{\substack{q\le N\\ q\equiv rp^i+1 \pmod{p^{i+1}}}} 1=\pi(N,p^{i+1},rp^i+1).$$

We have, by using Lemma **??**, that

$$\begin{aligned}\pi(N,p^{i+1},rp^i+1) =&\frac{1}{\varphi(p^{i+1})}\Big(\frac{N}{\log N}+O\Big(\frac{N}{(\log N)^2}\Big)\Big)+O(\sqrt{N}(\log N+2\log(p^{i+1})))\\ =&\frac{1}{\varphi(p^{i+1})}\Big(\frac{N}{\log N}+O\Big(\frac{N}{(\log N)^2}\Big)\Big)+O(\sqrt{N}\log N).\end{aligned}$$

We have $\varphi(p^{i+1}) = p^i(p-1)$. Then

$$\begin{aligned}
ST_0(N) = &\sum_{1\le i\le \log_p N} \frac{1}{p^i}\Big[\frac{1}{\varphi(p^{i+1})}\Big(\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)+O(N^{3/2}(\log N))\\
&-\Big(\frac{1}{\varphi(p^{i+1})}\Big(\frac{N}{\log N}+O\Big(\frac{N}{(\log N)^2}\Big)\Big)+O(\sqrt{N}\log N)\Big)\Big]\\
=&\sum_{0\le i\le \log_p N} \frac{1}{p^i}\Big[\frac{1}{p^i(p-1)}\Big(\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)+O(N^{3/2}\log N)\Big]\\
=&\sum_{0\le i\le \log_p N} \frac{1}{p^{2i}(p-1)}\Big(\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\Big)\\
=&\frac{1}{p-1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\sum_{0\le i\le \log_p N}\frac{1}{p^{2i}}.
\end{aligned}$$

Claim 2. $\sum_{0\le i\le \log_p N}\frac{1}{p^{2i}} = \frac{1}{p+1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)$.

Proof of Claim 2. We have

$$\begin{aligned}
\sum_{0\le i\le \log_p N}\frac{1}{p^{2i}} &= \frac{\Big(1-\frac{1}{N^2}\cdot\frac{1}{p^2}\Big)}{1-\frac{1}{p^2}}\\
&= \frac{p^2-\frac{1}{N^2}}{p^2-1}\\
&= \frac{(p-1)}{p^2-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\\
&= \frac{1}{p+1}\Big(1+O\Big(\frac{1}{N}\Big)\Big).
\end{aligned}$$

Hence, by Claim 2, we have

$$\begin{aligned}
ST_0(N) =&\frac{1}{p-1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\frac{1}{p+1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\\
=&\frac{1}{p-1}\frac{1}{p+1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\Big(1+O\Big(\frac{1}{N}\Big)\Big).
\end{aligned}$$

Consider the following limit, we have

$$\begin{aligned}
\lim_{N\to\infty}\frac{ST_0N}{\frac{1}{(p-1)(p+1)}\frac{N^2}{2\log N}} &= \lim_{N\to\infty}\frac{\frac{1}{p-1}\frac{1}{p+1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\Big(1+O\Big(\frac{1}{N}\Big)\Big)}{\frac{1}{2(p^2-1)}\frac{N^2}{\log N}}\\
&= 1.
\end{aligned}$$

Therefore

$$ST_0(N) \sim \frac{1}{2(p^2-1)}\frac{N^2}{\log N}$$

as desired. □

Now, we turn to $ST(N)$.

Theorem 3.2.4. *Assume the* ERH. *Then*

$$ST(N) \sim \frac{p+2}{2(p-1)^2(p+1)}\frac{N^2}{\log N}.$$

Proof. By Theorem **??** (5), we have

$$\begin{aligned}
ST(N) &= \sum_{q\le N}\sum_{1\le a<q} t_q(a) \\
&= \sum_{q\le N}(q-1)\Big[v_p(q-1) - \frac{1}{p-1} + \frac{p^{-v_p(q-1)}}{p-1}\Big] \\
&= \sum_{q\le N} qv_p(q-1) - \sum_{q\le N}\frac{q}{p-1} + \sum_{q\le N}\frac{qp^{-v_p(q-1)}}{p-1} \\
&\quad - \sum_{q\le N} v_p(q-1) + \sum_{q\le N}\frac{1}{p-1} - \sum_{q\le N}\frac{p^{-v_p(q-1)}}{p-1} \\
&= \sum_{q\le N} qv_p(q-1) - \frac{1}{p-1}\sum_{q\le N} q - \sum_{q\le N} v_p(q-1) + \frac{1}{p-1}\sum_{q\le N} 1 \\
&\quad + \frac{1}{p-1}\sum_{q\le N}\frac{q-1}{p^{v_p(q-1)}}.
\end{aligned}$$

We have

$$\frac{1}{p-1}\sum_{q\le N}\frac{q-1}{p^{v_p(q-1)}} = \frac{1}{p-1}ST_0(N) \sim \frac{1}{2(p-1)^2(p+1)}\frac{N^2}{\log N}.$$

Consider

$$\begin{aligned}\sum_{q\le N} qv_p(q-1) &= \sum_{1\le i\le \log_p N} \Big(\sum_{\substack{q\le N\\ q\equiv 1 \pmod{p^i}}} q\Big)\\ &= \sum_{1\le i\le \log_p N} \Big(\frac{1}{\varphi(p^i)}\Big(\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\\ &\quad + O(N^{3/2}(\log N + 2\log p^i)\Big)\\ &= \sum_{1\le i\le \log_p N} \Big(\frac{1}{p^{i-1}(p-1)}\Big(\frac{N^2}{2\log N}\Big)\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\\ &=\frac{1}{p-1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\sum_{1\le i\le \log_p N}\frac{1}{p^{i-1}}.\end{aligned}$$

Claim 1.

$$\sum_{1\le i\le \log_p N}\frac{1}{p^{i-1}} = \frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big).$$

Proof of Claim 1. We have

$$\begin{aligned}\sum_{1\le i\le \log_p N}\frac{1}{p^{i-1}} &= \frac{1-\frac{1}{N}}{1-\frac{1}{p}}\\ &= \frac{\frac{N-1}{N}}{\frac{p-1}{p}}\\ &= \frac{p}{p-1}\Big(1-\frac{1}{N}\Big)\\ &= \frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big).\end{aligned}$$

Then, by Claim 1, we have

$$\sum_{q\le N} qv_p(q-1) = \frac{1}{p-1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big).$$

Consider

$$
\begin{aligned}
\sum_{q\le N} v_p(q-1) &= \sum_{1\le i\le \log_p N}\Big(\sum_{\substack{q\le N\\ q\equiv 1 \pmod{p^i}}} 1\Big)\\
&= \sum_{1\le i\le \log_p N} \pi(N,p^i,1)\\
&= \sum_{1\le i\le \log_p N} \Big(\frac{li(N)}{\varphi(p^i)} + O(\sqrt{N}(\log N + 2\log p^i))\Big) \qquad \text{by Lemma } \mathbf{??}\\
&= li(N)\sum_{1\le i\le \log_p N} \frac{1}{p^{i-1}(p-1)} + O(\sqrt{N}(\log N^2)).
\end{aligned}
$$

Thus, by Claim 1 and $li(N)=\frac{N}{\log N}\Big(1+O\Big(\frac{1}{\log(N)}\Big)\Big)$, we have

$$\sum_{q\le N} v_p(q-1) = \frac{N}{\log N}\Big(1+O\Big(\frac{1}{\log(N)}\Big)\Big)\frac{1}{p-1}\Big(\frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big).$$

By [1,p.28–29], $\sum_{q\le N} q \sim \frac{N^2}{2\log N}$ and by [**??**], $\sum_{q\le N} 1 \sim \frac{N}{\log N}$.

Now, we get

$$
\begin{aligned}
ST(N) =& \sum_{q\le N} q v_p(q-1) - \frac{1}{p-1}\sum_{q\le N} q - \sum_{q\le N} v_p(q-1) + \frac{1}{p-1}\sum_{q\le N} 1\\
&+ \frac{1}{p-1}\frac{1}{2(p^2-1)}\frac{N^2}{\log N}\\
=& \frac{1}{p-1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{\log N}\Big)\Big)\frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big) - \frac{1}{p-1}\frac{N^2}{2\log N}\\
&- \frac{1}{p-1}\frac{N}{\log N}\Big(1+O\Big(\frac{1}{\log(N)}\Big)\Big(\frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big) + \frac{1}{p-1}\frac{N}{\log N}\\
&+ \frac{1}{2(p-1)^2(p+1)}\frac{N^2}{\log N}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
\lim_{N\to\infty}\frac{ST(N)}{\frac{p+2}{2(p-1)^2(p+1)}\frac{N^2}{\log N}} =& \lim_{N\to\infty}\frac{\frac{1}{p-1}\frac{N^2}{2\log N}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\frac{p}{p-1}\Big(1+O\frac{1}{N}\Big) - \frac{1}{p-1}\frac{N^2}{2\log N}}{\frac{p+2}{2(p-1)^2(p+1)}\frac{N^2}{\log N}}\\
&+ \lim_{N\to\infty}\frac{-\frac{1}{p-1}\Big(1+O\Big(\frac{1}{\log(N)}\Big)\frac{N}{\log N}\Big(\frac{p}{p-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big) + \frac{1}{p-1}\frac{N}{\log N}}{\frac{p+2}{2(p-1)^2(p+1)}\frac{N^2}{\log N}}\\
&+ \lim_{N\to\infty}\frac{+\frac{1}{2(p-1)^2(p+1)}\frac{N^2}{\log N}}{\frac{p+2}{2(p-1)^2(p+1)}\frac{N^2}{\log N}}\\
=& \ 1.
\end{aligned}
$$

Therefore,

$$ST(N) \sim \frac{p+2}{2(p-1)^2(p+1)} \frac{N^2}{\log N}.$$

□

Next, we consider sums of average quantities over all primes q that $q^2 \leq N$.

Definition 3.2.5. With respect to the iteration of the map $x \to x^p$ over $\mathbb{F}_{q^2}^*$, we define

- $ST_0(N) := \sum_{q^2 \leq N} T_0(q^2)$, where $T_0(q^2)$ is the number of elements in cycles over $\mathbb{F}_{q^2}^*$.

We first consider the graph obtained by iteration of $x \to x^p$, where $p = 2$.

Theorem 3.2.6. *Assume the* ERH. *Then*

$$ST_0(N) \sim \frac{1}{18} \frac{N^{3/2}}{\log N}.$$

Proof. Write $q^2 - 1 = 2^\tau \cdot \rho$ where $\tau = v_2(q^2 - 1)$ and $\gcd(2, \rho) = 1$. We have, using Theorem **??** (2), that

$$T_0(q^2) = \frac{q^2 - 1}{2^{v_2(q^2-1)}}.$$

Therefore

$$ST_0(N) = \sum_{q^2 \leq N} \frac{q^2 - 1}{2^{v_2(q^2-1)}} = \sum_{q \leq N^{1/2}} \frac{q^2 - 1}{2^{v_2(q^2-1)}}$$
$$= \sum_{0 \leq i \leq \log_2 N} \sum_{\substack{q \leq N^{1/2} \\ 2^i || (q^2-1)}} \frac{q^2 - 1}{2^i}.$$

<u>Claim 1.</u> For each $i \in \mathbb{N}_0$. If $2^i || (q^2 - 1)$, then $q^2 - 1 \equiv 2^i \pmod{2^{i+1}}$.

Proof of Claim 1. Let i be a non-negative integer.

Assume that $2^i||(q^2-1)$. Then $2^i|(q^2-1)$ and $2^{i+1}(q^2-1)$. So there exists $l \in \mathbb{N}$ such that $q^2-1 = 2^i(2l+1)$ which gives

$$q^2-1 = 2^{i+1}l + 2^i.$$

Hence $q^2-1 \equiv 2^i \pmod{2^{i+1}}$. This completes the proof of Claim 1.

By Claim 1, we have

$$\begin{aligned} ST_0(N) &= \sum_{0\le i\le \log_2 N} \sum_{\substack{q\le N^{1/2} \\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} \frac{q^2-1}{2^i} \\ &= \sum_{0\le i\le \log_2 N} \frac{1}{2^i} \sum_{\substack{q\le N^{1/2} \\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} (q^2-1) \\ &= \sum_{0\le i\le \log_2 N} \frac{1}{2^i}\Big(\sum_{\substack{q\le N^{1/2} \\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2 - \sum_{\substack{q\le N^{1/2} \\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} 1\Big). \end{aligned} \tag{3.2.1}$$

Next, we will find the estimates the sum Eq. (**??**).

We first consider the congruence $q^2 \equiv 2^i+1 \pmod{2^{i+1}}$ for all nonnegative integers i.

Case $i=0$. The congruence becomes $q^2 \equiv 2 \pmod 2$. The only solution for this case is $q=2$.

Case $i=1$. The congruence $q^2 \equiv 3 \pmod 4$ has no solution.

Case $i=2$. The congruence $q^2 \equiv 5 \pmod 8$ has no solution.

Case $i \ge 3$. Since $i \ge 3$,we have $2^i \equiv 0 (\bmod 8)$. Then $2^i+1 \equiv 1 (\bmod 8)$. So $q^2 \equiv 2^i+1 \pmod{2^{i+1}}$ has 4 solutions. We know that

$$(2^{i-1}+1)^2 = 2^{2i-2}+2^i+1 \equiv 2^i+1 \pmod{2^{i+1}},$$

and we set $q_1 \equiv 2^{i-1}+1 (\bmod 2^{i+1})$. Therefore, the other solutions are

$$\begin{aligned} -q_1 &\equiv -2^{i-1}-1 \equiv 2^{i-1}+2^i-1 \pmod{2^{i+1}}, \\ q_1+2^i &\equiv 2^{i-1}+2^i+1 \pmod{2^{i+1}} \\ \text{and} -(q_1+2^i) &\equiv -2^{i-1}-2^i-1 \equiv 2^{i-1}-1 \pmod{2^{i+1}}. \end{aligned}$$

Consequenetly, if $i \geq 3$, we get

$$\begin{aligned}\sum_{\substack{q \leq N^{1/2} \\ q^2 \equiv 2^i + 1 \pmod{2^{i+1}}}} q^2 &= \sum_{\substack{q \leq N^{1/2} \\ q \equiv 2^{i-1} + 1 \pmod{2^{i+1}}}} q^2 + \sum_{\substack{q \leq N^{1/2} \\ q \equiv 2^{i-1} - 1 \pmod{2^{i+1}}}} q^2 \\ &+ \sum_{\substack{q \leq N^{1/2} \\ q \equiv 2^{i-1} + 2^i + 1 \pmod{2^{i+1}}}} q^2 + \sum_{\substack{q \leq N^{1/2} \\ q \equiv 2^{i-1} + 2^i - 1 \pmod{2^{i+1}}}} q^2\end{aligned}$$

<u>Claim 2.</u> Let f be a real valued function. Then

$$\sum_{\substack{q \leq N \\ q \equiv k \pmod{l} \\ \gcd(k,l)=1}} f(q) = \frac{1}{\varphi(l)} \int_2^x \frac{f(t)}{\log(t)} + f(x)\epsilon(x) - \int_2^x f'(t)\epsilon(t)\, dt + O(1).$$

Proof of Claim 2. Let

$$a(n) = \begin{cases} 1\ ;\ n \text{ is prime, } n \equiv k \pmod{l}, \gcd(k,l) = 1 \\ 0\ ;\ \text{otherwise.} \end{cases}$$

So,

$$A(x) = \sum_{n \leq x} a(n) = \sum_{\substack{n \leq x \\ n \equiv k \pmod{l} \\ \gcd(k,l)=1}} 1 = \pi(x, l, k).$$

Then, by Stieljes integral, we have

$$\begin{aligned}\sum_{\substack{q \leq N \\ q \equiv k \pmod{l} \\ \gcd(k,l)=1}} f(q) = \sum_{1 < n \leq x} a(n) f(n) &= \int_1^x f(t)\ dA(t) \\ &= \int_1^2 f(t)\ dA(t) + \int_2^x f(t)\ dA(t) \\ &= \int_2^x f(t)\ d\pi(t, l, k) + O(1).\end{aligned}$$

By Lemma **??**,

$$\begin{aligned}\pi(x, l, k) &= \frac{li(x)}{\varphi(l)} + O(x^{1/2}(\log x + 2\log(l))) \\ &= \frac{li(x)}{\varphi(l)} + \epsilon(x),\end{aligned}$$

where $\epsilon(x) := O(x^{1/2}(\log x + 2\log(l)))$. Then

$$\sum_{\substack{q\le N\\ q\equiv k \pmod l\\ \gcd(k,l)=1}} f(q) = \int_2^x f(t)\,d\Big(\frac{li(t)}{\varphi(l)} + \epsilon(t)\Big) + O(1)$$

$$= \int_2^x f(t)\,d\frac{li(t)}{\varphi(l)} + \int_2^x f(t)\,d\epsilon(t) + O(1).$$

Note that

$$\int_2^x f(t)\,d\epsilon(t) = f(t)\epsilon(t)|_2^x - \int_2^x f'(t)\epsilon(t)\,dt + O(1)$$

and $li(x) = \int_2^x \frac{1}{\log t}dt + O(1)$. Hence,

$$\sum_{\substack{q\le x\\ q\equiv k \pmod l\\ \gcd(k,l)=1}} f(q) = \frac{1}{\varphi(l)}\int_2^x \frac{f(t)}{\log(t)}dt + f(x)\epsilon(x) - \int_2^x f'(t)\epsilon(t)\,dt + O(1).$$

Then we have Claim 2. By putting $f(a) = a^2$ for all $a \ge 2$ and Claim 2, for all positive integers k, l with $\gcd(k,l) = 1$, we have

$$\sum_{\substack{q\le x\\ q\equiv k \pmod l}} q^2 = \frac{1}{\varphi(l)}\int_2^x \frac{t^2}{\log(t)}dt + x^2\epsilon(x) - \int_2^x 2t\epsilon(t)\,dt + O(1).$$

By [**??**, p.28], we have

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

This implies that,

$$\int_2^x \frac{t^2}{\log(t)}dt = \int_{2^3}^{x^3} \frac{du}{\log u}$$

$$= \int_2^{x^3} \frac{du}{\log u} - \int_2^8 \frac{du}{\log u}$$

$$= \frac{x^3}{\log x^3} + O\Big(\frac{x^3}{(\log x^3)^2}\Big) + O(1)$$

$$= \frac{x^3}{\log x^3} + O\Big(\frac{x^3}{(\log x^3)^2}\Big).$$

So, we obtain the following approximation.

$$\begin{aligned}\sum_{\substack{q\le x\\ q\equiv k \pmod{l}}} q^2 &= \frac{1}{\varphi(l)}\Big[\frac{x^3}{\log x^3} + O\Big(\frac{x^3}{(\log x^3)^2}\Big)\Big] + x^2 O(x^{1/2}(\log x + 2\log(l)))\\ &\quad - \int_2^x 2tO(t^{1/2}(\log t + 2\log(l)))\,dt + O(1)\\ &= \frac{1}{\varphi(l)}\Big[\frac{x^3}{\log x^3} + O\Big(\frac{x^3}{(\log x^3)^2}\Big)\Big] + x^2 O(x^{1/2}(\log x + 2\log(l))) + O(1)\\ &= \frac{1}{\varphi(l)}\Big[\frac{x^3}{\log x^3} + O\Big(\frac{x^3}{(\log x^3)^2}\Big)\Big] + x^2 O(x^{1/2}(\log x + 2\log(l))).\end{aligned}$$

By letting $x = N^{1/2}$, $l = 2^{i+1}$ $(i \ge 3)$ and $\gcd(k,2) = 1$, we have

$$\sum_{\substack{q\le N^{1/2}\\ q\equiv k \pmod{2^{i+1}}}} q^2 = \frac{1}{\varphi(2^{i+1})}\Big[\frac{N^{3/2}}{\log N^{3/2}} + O\Big(\frac{N^{3/2}}{(\log N^{3/2})^2}\Big)\Big] + NO(N^{1/4}(\log N^{1/2} + 2\log(2^{i+1}))).$$

Since the sum does not depend on k , we have

$$\begin{aligned}\sum_{\substack{q\le N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2 &= 4\sum_{\substack{q\le N^{1/2}\\ q\equiv k \pmod{2^{i+1}}}} q^2,\\ &= 4\Big[\frac{1}{\varphi(2^{i+1})}\Big[\frac{N^{3/2}}{\log N^{3/2}} + O\Big(\frac{N^{3/2}}{(\log N^{3/2})^2}\Big)\Big]\\ &\quad + NO(N^{1/4}(\log N^{1/2} + 2\log(2^{i+1})))\Big].\end{aligned}$$

Consider the estimates of the second term in the Eq. (**??**)

$$\begin{aligned}\sum_{\substack{q\le N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} 1 &= 4\sum_{\substack{q\le N^{1/2}\\ q\equiv k \pmod{2^{i+1}}}} 1\\ &= 4\pi(N^{1/2}, 2^{i+1}, k)\\ &= 4\Big[\frac{li(N^{1/2})}{\varphi(2^{i+1})} + O(N^{1/4}(\log N^{1/2} + 2\log(2^{i+1})))\Big]\\ &= 4\Big[\frac{1}{\varphi(2^{i+1})}\Big(\frac{N^{1/2}}{\log N^{1/2}} + O\Big(\frac{N^{1/2}}{(\log N^{1/2})^2}\Big)\Big)\\ &\quad + O(N^{1/4}(\log N^{1/2} + 2\log(2^{i+1})))\Big].\end{aligned}$$

We have $\varphi(2^{i+1}) = 2^i$. Then, by Eq. (**??**), we have

$$\begin{aligned}
ST_0(N) =& \sum_{0\le i\le \log_2 N} \frac{1}{2^i}\Big(\sum_{\substack{q\le N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2 - \sum_{\substack{q\le N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} 1\Big)\\
=&\Big(4+\sum_{1\le i\le \log_2 N} \frac{1}{2^i} \sum_{\substack{q\le N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} q^2\Big) - \Big(1+\sum_{1\le i\le \log_2 N} \frac{1}{2^i} \sum_{\substack{q\le N^{1/2}\\ q^2\equiv 2^i+1 \pmod{2^{i+1}}}} 1\Big)\\
=& \sum_{3\le i\le \log_2 N} \frac{4}{2^i}\Big[\sum_{\substack{q\le N^{1/2}\\ q\equiv k \pmod{2^{i+1}}}} q^2 - \sum_{\substack{q\le N^{1/2}\\ q\equiv k \pmod{2^{i+1}}}} 1\Big] + 3\\
=& \sum_{3\le i\le \log_2 N} \frac{4}{2^i}\Big[\frac{1}{\varphi(2^{i+1})}\Big(\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big)\\
&+ NO(N^{1/4}(\log N^{1/2} + 2\log(2^{i+1})))\\
&-\Big(\frac{1}{\varphi(2^{i+1})}\Big(\frac{N^{1/2}}{\log N^{1/2}} + O\Big(\frac{N^{1/2}}{(\log N^{1/2})^2}\Big)\Big)\Big)\\
&+ O(N^{1/4}(\log N^{1/2} + 2\log(2^{i+1})))\Big)\Big] + 3\\
=& \sum_{3\le i\le \log_2 N} \frac{4}{2^{2i}}\Big[\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big] + 3\\
=&\Big[\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big] \sum_{3\le i\le \log_2 N} \frac{4}{2^{2i}}.
\end{aligned}$$

Claim 3. $\sum_{3\le i\le \log_2 N}\frac{1}{2^{2i}}=\frac{1}{48}\Big(1+O\Big(\frac{1}{N}\Big)\Big)$.

Proof of Claim 3. We have

$$\begin{aligned}\sum_{3\le i\le \log_2 N}\frac{1}{2^{2i}}&=\frac{\frac{1}{4^3}\Big(1-\frac{4^2}{N^2})\Big)}{1-\frac{1}{4}}\\&=\frac{1}{4^3}\cdot\frac{4}{3}\Big(1-\frac{16}{N^2}\Big)\\&=\frac{1}{48}\Big(1+O\Big(\frac{1}{N}\Big)\Big).\end{aligned}$$

This completes the proof of Claim 3.

Hence

$$\begin{aligned}ST_0(N)=&4\Big(\frac{1}{48}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big)\Big(\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\\=&\frac{1}{18}\frac{N^{3/2}}{\log N}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big).\end{aligned}$$

Since

$$\lim_{N\to\infty}\frac{ST_0N}{\frac{1}{18}\frac{N^{3/2}}{\log N}}=\lim_{N\to\infty}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)=1,$$

we get

$$ST_0(N)\sim\frac{1}{18}\frac{N^{3/2}}{\log N}.$$

□

When p is an odd prime, we have the following result.

Theorem 3.2.7. *Assume the* ERH. *Then*

$$ST_0(N)\sim\frac{4p^2}{3(p-1)^2(p+1)}\frac{N^{3/2}}{\log N}.$$

Proof. Write $q^2-1=p^\tau\cdot\rho$ where $\tau=v_p(q^2-1)$ and $\gcd(p,\rho)=1$. We, using Theorem **??** (2), have that

$$T_0(q^2)=\frac{q^2-1}{p^{v_p(q^2-1)}}.$$

Then, by Definition 3.2.9, we have

$$\begin{aligned} ST_0(N) &= \sum_{q^2 \leq N} T_0(q^2) \\ &= \sum_{q^2 \leq N} \frac{q^2-1}{p^{v_p(q^2-1)}} \\ &= \sum_{q \leq N^{1/2}} \frac{q^2-1}{p^{v_p(q^2-1)}} \\ &= \sum_{0 \leq i \leq \log_p N} \sum_{\substack{q \leq N^{1/2} \\ p^i || (q^2-1)}} \frac{q^2-1}{p^i}. \end{aligned}$$

<u>Claim 1.</u> For each $i \in \mathbb{N}_0$, if $p^i || (q^2-1)$, then there exists $0 < r < p$ such that $q^2 - 1 \equiv rp^i \pmod{p^{i+1}}$.

Proof of Claim 1. Let i be a non-negative integer and assume that $p^i || (q^2-1)$. Then $p^i | (q^2-1)$ and $p^{i+1}(q^2-1)$. So there exist $l \in \mathbb{N}$ and $0 < r < p$ such that $q^2 - 1 = p^i(pl + r) = p^{i+1}l + p^i r$. Then

$$q^2 - 1 \equiv rp^i \pmod{p^{i+1}}$$

as desired.

Hence, by Claim 1, we have

$$\begin{aligned} ST_0(N) &= \sum_{0 \leq i \leq \log_p N} \sum_{\substack{q \leq N^{1/2} \\ q^2 - 1 \equiv rp^i \pmod{p^{i+1}}}} \frac{q^2-1}{p^i} \\ &= \sum_{0 \leq i \leq \log_p N} \frac{1}{p^i} \sum_{\substack{q \leq N^{1/2} \\ q^2 \equiv rp^i + 1 \pmod{p^{i+1}}}} (q^2 - 1) \\ &= \sum_{0 \leq i \leq \log_p N} \frac{1}{p^i} \Big(\sum_{\substack{q \leq N^{1/2} \\ q^2 \equiv rp^i + 1 \pmod{p^{i+1}}}} q^2 - \sum_{\substack{q \leq N^{1/2} \\ q^2 \equiv rp^i + 1 \pmod{p^{i+1}}}} 1 \Big). \end{aligned} \tag{3.2.2}$$

Next, consider the congruence $q^2 \equiv rp^i + 1 \pmod{p^{i+1}}$ for all $i \geq 0$.

If $i = 0$, we will consider the solution of congruence $q^2 \equiv r + 1 \pmod{p}$. We have $\left(\frac{r+1}{p}\right) = 1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre's symbol, if and only if $q^2 \equiv r + 1 \pmod{p}$

has 2 solutions. Then

$$\sum_{\substack{q \le N^{1/2} \\ q^2 \equiv r+1 \pmod{p}}} q^2 = 2 \sum_{\substack{q \le N^{1/2} \\ q \equiv (r+1)^{1/2} \pmod{p} \\ \left(\frac{r+1}{p}\right)=1}} q^2.$$

Now we may assume that $i \ge 1$.

<u>Case</u> r is odd, we have

$$\Big(\frac{p-r}{2}p^i - 1\Big)^2 = \Big(\frac{p-r}{2}\Big)^2 p^{2i} - (p-r)p^i + 1 \equiv rp^i + 1 \pmod{p^{i+1}}.$$

So, $q \equiv \frac{p-r}{2}p^i - 1 \pmod{p^{i+1}}$ or $q \equiv -\frac{p-r}{2}p^i + 1 = \frac{p+r}{2}p^i + 1 \pmod{p^{i+1}}$.

Consequently, we get

$$\sum_{\substack{q \le N^{1/2} \\ q^2 \equiv rp^i+1 \pmod{p^{i+1}}}} q^2 = \sum_{\substack{q \le N^{1/2} \\ q \equiv \frac{p-r}{2}p^i - 1 \pmod{p^{i+1}}}} q^2 + \sum_{\substack{q \le N^{1/2} \\ q \equiv \frac{p+r}{2}p^i + 1 \pmod{p^{i+1}}}} q^2.$$

<u>Case</u> r is even, we have

$$\Big(\frac{r}{2}p^i + 1\Big)^2 = \Big(\frac{r}{2}\Big)^2 p^{2i} + rp^i + 1 \equiv rp^i + 1 \pmod{p^{i+1}}.$$

So, $q \equiv \frac{r}{2}p^i + 1 \pmod{p^{i+1}}$ or $q \equiv -\frac{r}{2}p^i - 1 = (p - \frac{r}{2})p^i - 1 \pmod{p^{i+1}}$.

This implies that

$$\sum_{\substack{q \le N^{1/2} \\ q^2 \equiv rp^i+1 \pmod{p^{i+1}}}} q^2 = \sum_{\substack{q \le N^{1/2} \\ q \equiv \frac{r}{2}p^i + 1 \pmod{p^{i+1}}}} q^2 + \sum_{\substack{q \le N^{1/2} \\ q \equiv (p-\frac{r}{2})p^i - 1 \pmod{p^{i+1}}}} q^2.$$

By the same proof as in Theorem **??**, for all positive k with $\gcd(k,p) = 1$, we have

$$\sum_{\substack{q \le N^{1/2} \\ q \equiv k \pmod{p^{i+1}}}} q^2 = \frac{1}{\varphi(p^{i+1})}\Big(\frac{N^{3/2}}{\log N^{3/2}} + O\Big(\frac{N^{3/2}}{(\log N^{3/2})^2}\Big)\Big)$$

$$+ NO(N^{1/4}(\log N^{1/2} + 2\log(p^{i+1}))).$$

Since the estimate of the sum does not depend on k, we have

$$\sum_{\substack{q \le N^{1/2} \\ q^2 \equiv rp^i+1 \pmod{p^{i+1}}}} q^2 = 2 \sum_{\substack{q \le N^{1/2} \\ q \equiv k \pmod{p^{i+1}}}} q^2 \quad (i \ge 0).$$

Similarly, for all $i \geq 0$, we have

$$\begin{aligned}
\sum_{\substack{q\leq N^{1/2}\\ q^2\equiv rp^i+1 \pmod{p^{i+1}}}} 1 &= 2\sum_{\substack{q\leq N^{1/2}\\ q\equiv k \pmod{p^{i+1}}}} 1\\
&= 2\pi(N^{1/2},p^{i+1},k)\\
&= 2\Big[\frac{1}{\varphi(p^{i+1})}\Big(\frac{N^{1/2}}{\log N^{1/2}}+O\Big(\frac{N^{1/2}}{(\log N^{1/2})^2}\Big)\Big)\\
&\quad + O(N^{1/4}(\log N^{1/2}+2\log(p^{i+1})))\Big].
\end{aligned}$$

We have $\varphi(p^{i+1}) = p^i(p-1)$. Then, by Eq. (**??**), we have

$$\begin{aligned}
ST_0(N) &= \sum_{0\leq i\leq \log_p N}\frac{1}{p^i}\Big(\sum_{\substack{q\leq N^{1/2}\\ q^2\equiv rp^i+1 \pmod{p^{i+1}}}} q^2 - \sum_{\substack{q\leq N^{1/2}\\ q^2\equiv rp^i+1 \pmod{p^{i+1}}}} 1\Big)\\
&= \sum_{0\leq i\leq \log_p N}\frac{1}{p^i}\Big[2\sum_{\substack{q\leq N^{1/2}\\ q\equiv k \pmod{p^{i+1}}}} q^2 - 2\sum_{\substack{q\leq N^{1/2}\\ q\equiv k \pmod{p^{i+1}}}} 1\Big]\\
&= \sum_{0\leq i\leq \log_p N}\frac{2}{p^i}\Big[\sum_{\substack{q\leq N^{1/2}\\ q\equiv k \pmod{p^{i+1}}}} q^2 - \sum_{\substack{q\leq N^{1/2}\\ q\equiv k \pmod{p^{i+1}}}} 1\Big]\\
&= \sum_{0\leq i\leq \log_p N}\frac{2}{p^i}\Big[\frac{1}{\varphi(p^{i+1})}\Big[\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big]\\
&\quad + NO(N^{1/4}(\log N^{1/2}+2\log(p^{i+1})))\\
&\quad - \Big(\frac{1}{\varphi(p^{i+1})}\Big(\frac{N^{1/2}}{\log N^{1/2}}+O\Big(\frac{N^{1/2}}{(\log N^{1/2})^2}\Big)\Big)\\
&\quad + O(N^{1/4}(\log N^{1/2}+2\log(p^{i+1})))\Big)\Big]\\
&= \sum_{1\leq i\leq \log_p N}\frac{2}{(p-1)p^{2i}}\Big[\Big(\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big]\\
&=\frac{2}{(p-1)}\Big[\Big(\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big]\sum_{0\leq i\leq \log_p N}\frac{1}{p^{2i}}.
\end{aligned}$$

Claim 2. $\sum_{0\leq i\leq \log_p N}\frac{1}{p^{2i}} = \frac{p^2}{p^2-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)$.

Proof of Claim 2. We have

$$\begin{aligned}\sum_{0\leq i\leq \log_p N}\frac{1}{p^{2i}} &= \frac{\Big(1-\frac{1}{N^2}\frac{1}{p^2})\Big)}{1-\frac{1}{p^2}}\\ &= \frac{p^2}{p^2-1}\Big(1-\frac{1}{p^2N^2}\Big)\\ &= \frac{p^2}{p^2-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big).\end{aligned}$$

Now, we ready to find the estimate of $ST_0(N)$.

Consider

$$\begin{aligned}ST_0(N) =&\frac{2}{(p-1)}\Big[\Big(\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big]\frac{p^2}{p^2-1}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\\ =&\frac{2p^2}{(p^2-1)(p-1)}\frac{N^{3/2}}{\log N^{3/2}}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big(1+O\Big(\frac{1}{N}\Big)\Big)\\ =&\frac{4p^2}{3(p^2-1)((p-1)}\frac{N^{3/2}}{\log N}\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\Big)\Big(1+O\Big(\frac{1}{N}\Big)\Big).\end{aligned}$$

Thus,

$$\begin{aligned}\lim_{N\to\infty}\frac{ST_0N}{\frac{4p^2}{3(p^2-1)(p-1)}\frac{N^{3/2}}{\log N}} &= \lim_{N\to\infty}\Big(1+O\Big(\frac{1}{N}\Big)\Big)\Big(1+O\Big(\frac{1}{\log N^{3/2}}\Big)\\ &= 1,\end{aligned}$$

which gives

$$ST_0(N)\sim\frac{4p^2}{3(p^2-1)(p-1)}\frac{N^{3/2}}{\log N}$$

as required. □

REFERENCES

Bach, E. and Shallit, J.: *Algorithmic Number Theory*, MIT Press, Cambridge, 1996.

Chartrand, G.: *Introductory Graph Theory*, Dover, New York, 1985.

Hardy, G. H. and Wright, E. M.: *An Introduction to the Theory of Numbers*, 4th ed., Oxford University Press, London, 1968.

Lidl, R. and Niederreite, H.: *Finite Fields*, Cambridge University Press, London, 1997.

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

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

Wilson, R. J. and Watkins, J. J.: *Graphs; An Introductory Approach*, Jon Wiley & Sons Inc., Toronto, 1990.

VITA

Name	: Miss Pratchayaporn Doemlim
Date of Birth	: 9 May 1996
Place of Birth	: Trang, Thailand
Education	: B.Sc. (First-Class Degree Honors), Mathematics, Walailak University, 2017
Scholarships	: Development and Promotion of Science and Technology Talents Project (DPST)