การแจกแจงแบบเอกรูปของภาคเศษส่วนของ a^n/n

นายปณิธาน โมทอง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2557

Uniform Distribution of Fractional Parts of a^n/n

Mr. Panithan Mothong

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2014

Thesis Title	UNIFORM DISTRIBUTION OF FRACTIONAL PARTS OF a^n/n
By	Mr. Panithan Mothong
Field of Study	Mathematics
Thesis Advisor	Assistant Professor Keng Wiboonton, 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 Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

.... Chairman

(Associate Professor Yotsanan Meemark, Ph.D.)

.... Thesis Advisor

(Assistant Professor Keng Wiboonton, Ph.D.)

.... Examiner

(Assistant Professor Tuangrat Chaichana, Ph.D.)

.... External Examiner

(Aram Tangboonduangjit, Ph.D.)

ปณิธาน โมทอง : การแจกแจงแบบเอกรูปของภาคเศษส่วนของ a^n/n (UNIFORM DISTRIBUTION OF FRACTIONAL PARTS OF a^n/n)
อ. ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ.ดร.เก่ง วิบูลย์ธัญญ์, 28 หน้า.

กำหนดให้ $a \geq 2$ เป็นจำนวนเต็ม เราพิสูจน์ว่าภาคเศษส่วนของลำดับ $\{a^n/n\}_{n\in\mathcal{B}}$ เป็นการแจกแจงแบบเอกรูป โดยที่ $\mathcal{B} := \{pq : p, q$ เป็นจำนวนเฉพาะ และ $a^q \leq pq\}$

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต..

ลายมือชื่อ อ.ที่ปรึกษาหลัก.......................................

สาขาวิชา คณิตศาสตร์

ปีการศึกษา 2557

5572029023 : MAJOR MATHEMATICS

KEYWORDS : UNIFORM DISTRIBUTION MODULO ONE/ PRIME NUMBERS/ EXPONENTIAL SUMS

PANITHAN MOTHONG : UNIFORM DISTRIBUTION OF FRACTIONAL PARTS OF a^n/n. ADVISOR : ASST. PROF. KENG WIBOONTON, Ph.D., 28pp.

Let $a \geq 2$ be an integer. We prove that the sequence $\{a^n/n\}_{n\in\mathcal{B}}$ is uniformly distributed modulo 1, where $\mathcal{B} := \{pq : p, q \text{ primes}, \ a^q \leq pq\}$.

Department : ...Mathematics and..... ...Computer Science...

Field of Study : ......Mathematics......

Academic Year : ....2014.............

Student's Signature : ....

Advisor's Signature : ....

.

TO COMPOSE

To compose is to be
the little you were created as
and let white birds out
in the dark night.
To live is to be
the great thing that you are
and stand alone and wonder
and hear birds fly in
from unknown worlds.

Tor Jonsson

ACKNOWLEDGEMENTS

I am very grateful to my thesis advisor, Assistant Professor Dr. Keng Wiboonton, for all his help and advice. Our conversations were always helpful and encouraging to me. I would like to thank my thesis committee: Associate Professor Dr. Yotsanan Meemark, Assistant Professor Dr. Tuangrat Chaichana and Dr. Aram Tangboonduangjit, for their comments and suggestions.

Finally, I thank my parents for giving me the foundation necessary for this undertaking and for always having unbounded faith in my abilities.

CONTENTS

NOTATION

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
$\mathbb{R}$	the set of real numbers
$\mathbf{e}(x)$	$\mathrm{e}^{2\pi ix}$ for all $x \in \mathbb{R}$
$[x]$	the greatest integer $\leq x$
$\{x\}$	$x - [x]$
$\lambda(I)$	the length of an interval I
$\mathrm{ord}_q a$	the multiplicative order of a in $\mathbb{Z}/q\mathbb{Z}$
(u, v)	the greatest common divisor of integers u and v
$\pi(x)$	the number of primes smaller than or equal to x
$\pi(x; k, r)$	the number of primes smaller than or equal to x in the arithmetic progression $r \pmod{k}$
$\phi(n)$	the number of positive integers smaller than or equal to n that are relatively prime to n
$\nu_p(n) = k$	the largest positive integer k with $p^k \mid n$ and $p^{k+1} \nmid n$
Λ	von Mangoldt function
$\theta(x)$	$\sum_{p \leq x} \log p$

CHAPTER I

INTRODUCTION

In this chapter, we attempt to give a general introduction to uniform distribution modulo 1.

Throughout this thesis, we use $\mathbf{e}(x) = \mathrm{e}^{2\pi i x}$ for all $x \in \mathbb{R}$.

For a real number x, let $[x]$ denote the *integral part* of x, that is, the greatest integer $\leq x$; and let $\{x\} = x - [x]$ be the *fractional part* of x, or the residue of x modulo 1. We note that the fractional part of any real number is contained in the *unit interval* $I = [0, 1)$.

Let $\Gamma = (\gamma_n)_{n=1}^{\infty}$ be a sequence of real numbers. For a positive integer N and a subset E of $[0, 1)$, let the *counting function* $A(E; N; \Gamma)$ be defined by

$$A(E; N; \Gamma) = |\{\ n \in \mathbb{N} : 1 \leq n \leq N \ \text{ and } \ \{\gamma_n\} \in E\}|.$$

The sequence $\Gamma = (\gamma_n)_{n=1}^{\infty}$ of real numbers is said to be *uniformly distributed modulo 1* (abbreviated **u.d. mod 1**) if for every pair a, b of real numbers with $0 \leq a < b \leq 1$ we have

$$\lim_{N \to \infty} \frac{A([a, b); N; \Gamma)}{N} = b - a. \tag{1.1}$$

Let $c_{[a,b)}$ be the *characteristic function* of the interval $[a, b) \subseteq I$; i.e.,

$$c_{[a,b)}(x) = \begin{cases} 1, & x \in [a, b), \\ 0, & x \notin [a, b). \end{cases}$$

If $\Gamma = (\gamma_n)_{n=1}^{\infty}$ is u.d. mod 1, then (1.1) can be written in the form

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} c_{[a,b)}(\{\gamma_n\}) = \int_0^1 c_{[a,b)}(x)dx. \tag{1.2}$$

Let $a < b$ be real numbers. A *partition* P of the interval $[a, b]$ is a finite subset of real numbers $x_0, ..., x_n$ such that

$$a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b.$$

We write $P = \{x_0, x_1, ..., x_n\}$.

A real-valued function f defined on $[a, b]$ is called a *step function* provided there is a partition $P = \{x_0, x_1, ..., x_n\}$ of $[a, b]$ and numbers $f_1, f_2, ..., f_n \in \mathbb{R}$ such that for $1 \leq i \leq n$,

$$f(x) = \sum_{i=1}^{n} f_i c_{[x_{i-1},x_i)}(x).$$

Let $a < b$ be real numbers, let $f : [a, b] \to \mathbb{R}$ be a bounded function, and let $P = \{x_0, x_1, ..., x_n\}$ be a partition of $[a, b]$. We define the *upper Riemann sum* $U(f, P)$ by

$$U(f, P) := \sum_{i=1}^{n} \left(\sup_{x\in[x_{i-1},x_i)} f(x) \right) (x_i - x_{i-1}).$$

We also define the *lower Riemann sum* $L(f, P)$ by

$$L(f, P) := \sum_{i=1}^{n} \left(\inf_{x\in[x_{i-1},x_i)} f(x) \right) (x_i - x_{i-1}).$$

Let $a < b$ be real numbers, let $f : [a, b] \to \mathbb{R}$ be a bounded function. We define the *upper Riemann integral* $\overline{\int_a^b} f$ of f on $[a, b]$ by

$$\overline{\int_a^b} f := \inf\{U(f, P) : P \text{ is a partition of } [a, b]\}.$$

We also define the *lower Riemann integral* $\underline{\int_a^b} f$ of f on $[a, b]$ by

$$\underline{\int_a^b} f := \sup\{L(f, P) : \ P \text{ is a partition of } [a, b]\}.$$

Let $a < b$ be real numbers, let $f : [a, b] \to \mathbb{R}$ be a bounded function. If $\overline{\int_a^b} f = \underline{\int_a^b} f$ we say that f is *Riemann integrable* on $[a, b]$, and we define

$$\int_a^b := \overline{\int_a^b} f = \underline{\int_a^b} f.$$

The following proposition is taken from [6].

Proposition 1.1. *The sequence* $\Gamma = (\gamma_n)_{n=1}^{\infty}$ *of real numbers is u.d.* mod 1 *if and only if for every real-valued continuous function* f *defined on the closed unit interval* $\bar{I} = [0, 1]$ *we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{\gamma_n\}) = \int_0^1 f(x)dx. \tag{1.3}$$

Proof. Let $\Gamma = (\gamma_n)_{n=1}^{\infty}$ be u.d. mod 1, and let

$$g(x) = \sum_{i=1}^{k} g_i c_{[a_{i-1}, a_i)}(x)$$

be a step function on $\bar{I}$, where $0 = a_0 < a_1 < \cdots < a_k = 1$ and $g_1, g_2, ..., g_k \in \mathbb{R}$. Since

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} c_{[a,b)}(\{\gamma_n\}) = \int_0^1 c_{[a,b)}(x)dx,$$

we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \sum_{i=0}^{k-1} g_i c_{[a_i, a_{i+1})}(\{\gamma_n\}) = \int_0^1 g(x)dx.$$

Now we suppose that f is a real-valued continuous function defined on $\bar{I}$. Given $\epsilon > 0$, there exist two step functions f_1 and f_2 such that

$$f_1(x) \leq f(x) \leq f_2(x) \quad \text{for all} \quad x \in \bar{I} \quad \text{and} \quad \int_0^1 (f_2(x) - f_1(x))\, dx \leq \epsilon,$$

by the definition of the Riemann integral. Then we see that

$$\begin{aligned}
\int_0^1 f(x)dx - \epsilon &\leq \int_0^1 f_1(x)dx \\
&= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f_1(\{\gamma_n\}) \\
&\leq \liminf_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{\gamma_n\}) \\
&\leq \limsup_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{\gamma_n\}) \\
&\leq \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f_2(\{\gamma_n\}) \\
&= \int_0^1 f_2(x)dx \\
&\leq \int_0^1 f(x)dx + \epsilon.
\end{aligned}$$

Since ϵ is arbitrarily small and f is a continuous function, we see that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{\gamma_n\}) = \int_0^1 f(x)dx.$$

Conversely, let $\Gamma = (\gamma_n)_{n=1}^{\infty}$ be a sequence, and suppose that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{\gamma_n\}) = \int_0^1 f(x)dx$$

holds for every real-valued continuous function f on $\bar{I}$. Given $[a, b) \subseteq I$ and $\epsilon > 0$.

Then there exist two continuous functions, g_1 and g_2, such that

$$g_1(x) \leq c_{[a,b)}(x) \leq g_2(x) \quad \text{for all} \quad x \in \bar{I} \quad \text{and} \quad \int_0^1 (g_2(x) - g_1(x))\, dx \leq \epsilon.$$

Then we see that

$$\begin{aligned} b - a - \epsilon &\leq \int_0^1 g_2(x)dx - \epsilon \\ &\leq \int_0^1 g_1(x)dx = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} g_1(\{\gamma_n\}) \\ &\leq \liminf_{N\to\infty} \frac{A([a,b);N;\Gamma)}{N} \\ &\leq \limsup_{N\to\infty} \frac{A([a,b);N;\Gamma)}{N} \\ &\leq \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} g_2(\{\gamma_n\}) = \int_0^1 g_2(x)dx \\ &\leq \int_0^1 g_1(x)dx + \epsilon \\ &\leq b - a + \epsilon. \end{aligned}$$

Since ϵ is arbitrarily small, we obtain

$$\lim_{N\to\infty} \frac{A([a,b);N;\Gamma)}{N} = b - a.$$

□

Corollary 1.2. *The sequence $\Gamma = (\gamma_n)_{n=1}^{\infty}$ of real numbers is u.d.* mod 1 *if and only if for every complex-valued continuous function f on $\mathbb{R}$ with period* 1 *we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\gamma_n) = \int_0^1 f(x)dx. \tag{1.4}$$

Proof. Using Proposition 1.1 to the real and imaginary part of f, we see that (1.3) also holds for complex-valued function f. Since f is a function with period 1, that is $f(\{\gamma_n\}) = f(\gamma_n)$, we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\gamma_n) = \int_0^1 f(x)dx.$$

Conversely, we need only note that in the second part of the proof of Proposition 1.1 the functions g_1 and g_2 can be chosen in such a way that they satisfy the additional requirements

$$g_1(0) = g_1(1) \quad \text{and} \quad g_2(0) = g_2(1),$$

so that (1.4) can be applied to the periodic extensions of g_1 and g_2 to $\mathbb{R}$. □

We will use the following theorem in the proof of Proposition 1.4, (see [9].)

Proposition 1.3. (Weierstrass Approximation Theorem) *Any $2\pi-$periodic continuous function, $f : \mathbb{R} \to \mathbb{C}$ and an arbitrary $\epsilon > 0$ there exists a trigonometric polynomial p such that*

$$|f(x) - p(x)| < \epsilon$$

for all x in $[0, 2\pi]$.

One of the most important facts of the theory of uniformly distributed modulo 1 is the following result, (see [6].)

Proposition 1.4. (Weyl's criterion) *The sequence $\Gamma = (\gamma_n)_{n=1}^{\infty}$ is u.d. mod 1 if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbf{e}(h\gamma_n) = 0, \quad \textit{for all nonzero integers } h. \tag{1.5}$$

Proof. The necessity follows from Corollary 1.2.

Now suppose that $\Gamma = (\gamma_n)_{n=1}^{\infty}$ satisfies

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbf{e}(h\gamma_n) = 0,$$

for $h \in \mathbb{Z} \setminus \{0\}$. Then we will show that (1.4) holds for every complex-valued continuous function f on $\mathbb{R}$ with period 1. Let $\epsilon > 0$. By the Weierstrass approximation theorem, there exists a trigonometric polynomial $p(x)$, that is, a finite linear combination of function of the type $\mathbf{e}(hx)$, $h \in \mathbb{Z}$, with complex coefficients, such that

$$\sup_{0\leq x\leq 1} |f(x) - p(x)| \leq \epsilon. \tag{1.6}$$

Now we have

$$\begin{aligned}\left|\int_0^1 f(x)dx - \frac{1}{N}\sum_{n=1}^{N} f(\gamma_n)\right| \leq &\left|\int_0^1 (f(x) - p(x))\, dx\right| \\ &+ \left|\int_0^1 p(x)dx - \frac{1}{N}\sum_{n=1}^{N} p(\gamma_n)\right| \\ &+ \left|\frac{1}{N}\sum_{n=1}^{N} (f(\gamma_n) - p(\gamma_n))\right|.\end{aligned}$$

The first and the third terms on the right are both $\leq \epsilon$ whatever the value of N because of (1.6). By taking N sufficiently large, the second term on the right is $\leq \epsilon$ because of (1.5). We see that

$$\left|\int_0^1 f(x)dx - \frac{1}{N}\sum_{n=1}^{N} f(\gamma_n)\right| \leq 3\epsilon.$$

Since ϵ is arbitrarily small, we have $\Gamma = (\gamma_n)_{n=1}^{\infty}$ is u.d. mod 1. □

One of the most well-known examples of a u.d. mod 1 sequence using Weyl's criterion is the following result.

Example 1.1. Let γ be an irrational number. Then the sequence $(n\gamma)_{n=1}^{\infty}$ is u.d. mod 1. To show this, let h be a nonzero integer. Since γ is an irrational, $h\gamma$ is not an integer and so $1 - \mathbf{e}(h\gamma)$ is nonzero. Then for each N, we have

$$\begin{aligned} \left| \frac{1}{N} \sum_{n=1}^{N} \mathbf{e}(hn\gamma) \right| &= \frac{1}{N} \frac{|\mathbf{e}(h\gamma) - \mathbf{e}(h(N+1)\gamma)|}{|1 - \mathbf{e}(h\gamma)|} \\ &\leq \frac{1}{N} \frac{2}{|1 - \mathbf{e}(h\gamma)|}. \end{aligned}$$

Since

$$\lim_{N \to \infty} \frac{1}{N} \frac{2}{|1 - \mathbf{e}(h\gamma)|} = 0,$$

by Weyl's criterion, we have the sequence $(n\gamma)_{n=1}^{\infty}$ is u.d. mod 1.

Example 1.2. Weyl generalized the above example to the following result. Let $p(n)$ be a polynomial with real coefficients such that a coefficient, other than the constant term, is irrational. Then $(p(n))_{n=1}^{\infty}$ is u.d. mod 1. (Theorem 3.2 of [6].)

Example 1.3. Let $\gamma = 0.123456789101112131415...$ in decimal notation. Suppose that γ is periodic with period length n. But in $\gamma = 0.123456789101112131415...$ there are $2n$ consecutive zeros an infinite number of times. So the period can only have n zeros, which is a contradiction. Then γ is irrational. Therefore, by Example 1.1, the sequence $(n\gamma)_{n=1}^{\infty}$ is u.d. mod 1.

Example 1.4. The sequence $(ne)_{n=1}^{\infty}$ is u.d. mod 1 according to Example 1.1. However, the subsequence $(n!e)_{n=1}^{\infty}$ has 0 as the only limit point. We have

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{n!} + \frac{e^{\alpha}}{(n+1)!}, \quad 0 < \alpha < 1,$$

so that $n!e = k + \frac{e^{\alpha}}{(n+1)}$, for some $k \in \mathbb{N}$. Hence, for $n \geq 2$, we get $\{n!e\} = \frac{e^{\alpha}}{(n+1)} < \frac{e}{n+1}$. Since $\frac{e}{n+1} \to 0$ as n tends to infinity, we have $(\{n!e\})_{n=1}^{\infty}$ is not dense in $[0, 1)$. We can show that if the sequence is u.d. mod 1, then its fractional parts is dense in I. So the sequence $(n!e)_{n=1}^{\infty}$ is not u.d. mod 1.

Let $\Gamma_N = (\gamma_n)_{n=1}^N$ be a finite sequence of the first N terms of Γ. The number

$$D_N := D_N(\Gamma) = \sup_{[a,b)\subseteq[0,1]} \left| \frac{A([a,b);N;\Gamma_N)}{N} - (b-a) \right|$$

is called the *discrepancy* of the given sequence.

The pertinence of the concept of the discrepancy in the theory of u.d. mod 1 is revealed by the following criterion.

Proposition 1.5. *The sequence* $\Gamma = (\gamma_n)_{n=1}^\infty$ *is u.d.* mod 1 *if and only if*

$$\lim_{N\to\infty} D_N(\Gamma) = 0.$$

Proof. The sufficiency is obvious because of (1.1).

To show the necessity, we choose an integer $m \geq 2$. For $0 \leq k \leq m-1$, let

$$I_k = \left[\frac{k}{m}, \frac{k+1}{m}\right).$$

Since Γ is u.d. mod 1, there exists $M = M(m) \in \mathbb{N}$ such that for $N \geq M$ and for every $k = 0, 1, ..., m-1$, we have

$$\frac{1}{m}\left(1 - \frac{1}{m}\right) \leq \frac{A(I_k;N;\Gamma)}{N} \leq \frac{1}{m}\left(1 + \frac{1}{m}\right). \tag{1.7}$$

Let $J = [\alpha, \beta) \subseteq I$. Clearly there exist intervals J_1 and J_2, finite unions of intervals I_k, such that

$$J_1 \subseteq J \subseteq J_2, \quad \lambda(J) - \lambda(J_1) < \frac{2}{m}, \quad \text{and} \quad \lambda(J_2) - \lambda(J) < \frac{2}{m},$$

where λ is the length of an interval. It follows from (1.7) that we have for all $N \geq M$,

$$\lambda(J_1)\left(1 - \frac{1}{m}\right) \leq \frac{A(J_1;N;\Gamma)}{N} \leq \frac{A(J;N;\Gamma)}{N} \leq \frac{A(J_2;N;\Gamma)}{N} \leq \lambda(J_2)\left(1 + \frac{1}{m}\right).$$

Consequently, we obtain

$$\left(\lambda(J) - \frac{2}{m}\right)\left(1 - \frac{1}{m}\right) < \frac{A(J;N;\Gamma)}{N} < \left(\lambda(J) + \frac{2}{m}\right)\left(1 + \frac{1}{m}\right).$$

Then, by using $\lambda(J) \le 1$,

$$-\frac{3}{m} - \frac{2}{m^2} < \frac{A(J;N;\Gamma)}{N} - \lambda(J) < \frac{3}{m} + \frac{2}{m^2} \quad \text{for all} \quad N \ge M. \tag{1.8}$$

Since the bounds in (1.8) are independent of J, we arrive at

$$D_N(\Gamma) \le \frac{3}{m} + \frac{2}{m^2}$$

for all $N \ge M$. But $\frac{3}{m} + \frac{2}{m^2}$ can be made arbitrarily small, so the proof is complete. □

We use the Landau's symbol O as well as the Vinogradov's symbols $\ll$ and $\gg$. Recall that

$$f(n) = O(g(n)), \quad f(n) \ll g(n), \quad \text{and} \quad g(n) \gg f(n)$$

are all equivalent to the fact that there is $c \in \mathbb{R}$ such that

$$\text{for all} \quad n \ge N, \quad \text{the inequality} \quad |f(n)| \le cg(n) \quad \text{holds.}$$

We say $f(x) = o\left(g(x)\right)$ as x tends to infinity if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

We also use $f(x) \sim g(x)$ as x tends to infinity if

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

One of our main tools is the classical *Erdős-Turán Inequality* that relates the uniformity of distribution to exponential sums, by bounding the discrepancy of a sequence in terms of its exponential moments. (See [3].)

Lemma 1.6. (Erdős-Turán Inequality) *For any integer $L \geq 1$ and for the discrepancy D_N of the sequence Γ, we have*

$$D_N \ll \frac{1}{L} + \frac{1}{N} \sum_{1 \leq |h| \leq L} \frac{1}{|h|} \left| \sum_{n=1}^{N} \boldsymbol{e}(h\gamma_n) \right| .$$

For every positive integer $a \geq 2$, let $f_a,\ h_a$ be the arithmetic functions defined by

$$f_a(n) = \frac{a^{n-1} - 1}{n} \quad \text{and} \quad h_a(n) = \frac{a^n - a}{n} \qquad (n \geq 1).$$

Note that f_a and h_a are integer if n is a prime number and $n \nmid a$.

In [1], W.D. Banks, M.Z. Garaev, F. Luca amd I.E. Shparlinski proved the following.

(i) For any nonzero integer b such that $\log|b| = o\left(\sqrt{\log N \log\log N}\right)$, the following inequality holds :

$$\sum_{\substack{1 \leq n \leq N \\ n \text{ composite}}} \left| \sum_{\substack{1 \leq a \leq n \\ (a,n)=1}} \mathbf{e}\left(bf_a(n)\right) \right| \leq N^2 \mathrm{e}^{-(0.5+o(1))\sqrt{\log N \log\log N}} .$$

(ii) For any nonzero integer b such that $|b| < (\log\log\log N)^3$ the bound

$$\sum_{\substack{1 \leq n \leq N \\ n \text{ composite}}} \left| \sum_{\substack{1 \leq a \leq n \\ (a,n)=1}} \mathbf{e}\left(bh_a(n)\right) \right| \ll \frac{N^2 \log\log\log\log N}{\log\log\log N}$$

holds as $N \to \infty$.

These results imply that the fractional parts $\{f_a(n)\}_{n=1}^{\infty}$ and $\{h_a(n)\}_{n=1}^{\infty}$ are uniformly distributed modulo 1, on average over $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Let $a \geq 2$ be an integer. J. Cilleruelo, A. Kumchev, F. Luca, J. Rue, and I.E. Shparlinski [2] defined the set $\mathcal{A} = \{\ pq : \ p, q \text{ primes},\ q \leq (\log p)/(\log a)\ \}$ and put $\mathcal{A}(N) = \mathcal{A} \cap [1, N]$. They also proved that the discrepancy D_N of the sequence $(a^n/n)_{n \in \mathcal{A}(N)}$ is

$$D_N = O\left(\frac{\log\log\log\log N}{\log\log\log N}\right),$$

implying that the sequence is uniformly distributed modulo 1.

However, the statement that the sequence $(a^n/n)_{n=1}^{\infty}$ is uniformly distributed modulo 1 still be a conjecture. In this thesis, we prove that the sequence (a^n/n) is uniformly distributed modulo 1 when we restrict n to a certain subset of the positive integers. This restriction is on the set $\mathcal{B}$ where

$$\mathcal{B} = \{pq \ : \ p, q \text{ primes},\ a^q \leq pq\}$$

and we set $\mathcal{B}(N) = \mathcal{B} \cap [1, N]$ for each positive integer N.

The structure of this thesis is as follows. In chapter II, we give some basic preliminaries in analytic number theory which are used to prove our lemmas. In chapter III, we prove some lemmas and our main result.

CHAPTER II
PRELIMINARIES

In this chapter, we give some basic preliminaries which are needed for this work.

Throughout this thesis, p and q always denote prime numbers. For two integers u and v, their greatest common divisor is denoted by (u, v).

As usual, for relatively prime integers a and q we denote by $\text{ord}_q a$ the multiplicative order of a in $\mathbb{Z}/q\mathbb{Z}$.

For a real number $x > 1$, we use $\pi(x)$ for the number of primes $p \leq x$, and for coprime positive integers k and r we use $\pi(x; k, r)$ for the number of primes smaller than or equal to x in the arithmetic progression $r \pmod{k}$.

We also denote by $\phi(n)$ the Euler function and by $\nu_p(n) = k$ if $p^k | n$ and $p^{k+1} \nmid n$.

We use the asymptotic estimate that follows from the prime number theorem about counting prime numbers, (see [5].)

Theorem 2.1. (Prime Number Theorem) *As $x \to \infty$, we have*

$$\pi(x) \sim \frac{x}{\log x}.$$

We also use the asymptotic estimate that follows from the Siegel-Walfisz theorem about primes in arithmetic progressions, (see [5].)

Theorem 2.2. (Siegel-Walfisz Theorem) *Let $k \geq 1$ and $A > 0$. We have*

$$\pi(x; k, r) = \frac{\pi(x)}{\phi(k)} + O\left(\frac{x}{\log^A x}\right) \tag{2.1}$$

for any $x \geq 2$ and $(k, r) = 1$.

We also need the bound given by the Brun-Titchmarsh Theorem, (see [5].)

Theorem 2.3. (Brun-Titchmarsh Theorem) *For* $(k, r) = 1$ *and* $x \geq k$*, we have*

$$\pi(x; k, r) \ll \frac{x}{\phi(k) \log(x/k)}. \tag{2.2}$$

Lemma 2.4. (Abel's Summation Formula) *Let* $y < x$*, and let* f *be a function having a continuous derivative on* $[y, x]$*. Then*

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt \tag{2.3}$$

where the integers $a(n)$ *are given, and where*

$$A(x) := \sum_{n\leq x} a(n). \tag{2.4}$$

The *von Mangoldt function*, denoted by $\Lambda(n)$, is defined as

$$\Lambda(n) = \begin{cases} \log p, & \text{if} \quad n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 2.5. *We have*

$$\sum_{n\leq x} \Lambda(n) = x + O\left(\frac{x}{\log x}\right).$$

Proof. Take

$$a(n) = \begin{cases} 1, & \text{if} \quad n \text{ is prime number,} \\ 0, & \text{otherwise,} \end{cases}$$

that is, $a(n)$ is the characteristic function of the set of prime numbers. Moreover, take

$$f(x) := \log x.$$

We obtain

$$\begin{aligned}
\sum_{n\leq x}\Lambda(n) &= \sum_{p\leq x}\Lambda(p) + \sum_{p\leq x^{1/2}}\Lambda(p^2) + \sum_{p\leq x^{1/3}}\Lambda(p^3) + ... \\
&= \sum_{n\leq x} a(n)f(n) + \sum_{p\leq x^{1/2}}\Lambda(p^2) + \sum_{p\leq x^{1/3}}\Lambda(p^3) + ... \\
&= \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt + O\left(\sum_{2\leq k\leq \log_2 x}\pi(x^{1/k})\log x\right) \\
&= x + O\left(\pi(x) + \int_2^x td\frac{\pi(t)}{t}\right) + O\left(x^{1/2}\log^2 x\right) \\
&= x + O\left(\frac{x}{\log x}\right),
\end{aligned}$$

where we use Abel's summation formula in the third equality. □

We also note that

$$\theta(x) = \sum_{p\leq x}\log p = x + O\left(\frac{x}{\log x}\right). \quad (2.5)$$

We recall the Mertens' Theorem for the sum of reciprocals of the primes $p \leq x$ in the following crude form. Typically, the proof involves Mertens' proof, starts with estimate

$$\sum_{p\leq x}\frac{1}{p^{1+\eta}}$$

where $\eta > 0$. Then letting $\eta \to 0$ gives Mertens' theorem. Here we present an alternative proof which start estimate the summation function of $\Lambda(n)$, then translates into estimates of

$$\sum_{p\leq x}\frac{\log p}{p} \quad \text{and} \quad \sum_{p\leq x}\frac{1}{p}.$$

Theorem 2.6. (Mertens' Theorem) *There exists a constant $C > 0$ such that*

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + C + O\left(\frac{1}{\log x}\right). \quad (2.6)$$

Proof. Take $a(n) := 1$ and $f(x) := \log x$. By Abel's Summation formula, we have

$$\begin{aligned}\sum_{n\leq x} \log n &= [x]\log x - 2\log 2 + \log 2 - \int_2^x \frac{t-\{t\}}{t} dt \\ &= x\log x - \{x\}\log x - 2\log 2 + \log 2 - \int_2^x 1 - \frac{\{t\}}{t} dt \\ &= x\log x - x + O(\log x).\end{aligned}$$

We observe, however, that

$$\begin{aligned}x\log x - x + O(\log x) &= \sum_{n\leq x} \log n = \sum_{n\leq x}\sum_{p|n} \nu_p(n)\log p \\ &= \sum_{n\leq x}\sum_{p|n}\sum_{i\leq \nu_p(n)} \log p \\ &= \sum_{n\leq x}\sum_{p^i|n} \Lambda(p^i) \\ &= \sum_{n\leq x}\sum_{d|n} \Lambda(d) \\ &= \sum_{d\leq x} \Lambda(d)\left[\frac{x}{d}\right] \\ &= \sum_{d\leq x} \Lambda(d)\left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) \\ &= x\sum_{d\leq x}\frac{\Lambda(d)}{d} + O\left(\sum_{d\leq x}\Lambda(d)\right) \\ &= x\sum_{d\leq x}\frac{\Lambda(d)}{d} + O(x),\end{aligned}$$

where the last step follows from Lemma 2.5. Combining with the previous equation, we deduce that

$$\sum_{d\leq x}\frac{\Lambda(d)}{d} = \log x + O(1). \tag{2.7}$$

Next we show that $\sum_{d\le x}\frac{\Lambda(d)}{d}=\sum_{p\le x}\frac{\Lambda(p)}{p}+O(1)$:

$$\begin{aligned}\sum_{d\le x}\frac{\Lambda(d)}{d}&=\sum_{p\le x}\frac{\log p}{p}+\sum_{p\le x^{1/2}}\frac{\log p}{p^2}+\sum_{p\le x^{1/3}}\frac{\log p}{p^3}+\cdots\\&=\sum_{p\le x}\frac{\log p}{p}+O\left(\sum_{p\le x^{1/2}}\frac{\log p}{p^2}\left(\frac{1}{1-\frac{1}{p}}\right)\right)\\&=\sum_{p\le x}\frac{\log p}{p}+O(1).\end{aligned}$$

Hence $A(x)=\sum_{p\le x}\frac{\log p}{p}=\sum_{d\le x}\frac{\Lambda(d)}{d}+O(1)$. It follows from (2.7), we have

$$A(x)=\sum_{p\le x}\frac{\log p}{p}=\log x+O(1).$$

Using Abel's Summation formula, we have

$$\begin{aligned}\sum_{p\le x}\frac{1}{p}=\sum_{p\le x}\frac{\log p}{p}\frac{1}{\log p}&=\frac{A(x)}{\log x}+\int_2^x\frac{A(t)}{t\,(\log t)^2}\,dt\\&=\frac{\log x+O(1)}{\log x}+\int_2^x\frac{\log t+O(1)}{t\,(\log t)^2}\,dt\\&=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{1}{t\,(\log t)}\,dt+O\left(\int_2^x\frac{1}{t\,(\log t)^2}\,dt\right)\\&=1+O\left(\frac{1}{\log x}\right)+\log\log x-\log\log 2+O\left(\frac{1}{\log x}-\frac{1}{\log 2}\right)\\&=\log\log x+C+O\left(\frac{1}{\log x}\right).\end{aligned}$$

□

We will use the following lemma in the proof of Theorem 2.8, (see [8].)

Lemma 2.7. *For $x\ge 2$, we have $\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}=e^{\gamma}\log x+O(1)$, where γ is the Euler's constant.*

We also use the following well-known lower bound for $\phi(n)$, (see [8].)

Theorem 2.8. *For all* $n \geq 3$,

$$\phi(n) \geq \frac{n}{\log\log n}\left(e^{-\gamma} + O(1/\log\log n)\right), \tag{2.8}$$

where γ *is the Euler's constant and there are infinitely many* n *for which the equality of the above relation holds.*

Proof. Let $\mathcal{E} = \{\ n \in \mathbb{N} |\ \ \frac{\phi(n)}{n} < \frac{\phi(m)}{m}\ \text{ for all positive integers }\ m < n\}$. If $n \in \mathcal{E}$ has k prime factors, let n^* be the product of the first k prime factors. If $n \neq n^*$, then $n^* < n$ and $\frac{\phi(n^*)}{n^*} < \frac{\phi(n)}{n}$, which is impossible. Hence $\mathcal{E}$ consists entirely of n of the form

$$n = \prod_{p \leq y} p \quad \text{for some} \quad y. \tag{2.9}$$

Then for $n \in \mathcal{E}$, there exists y so that $\log n = \sum_{p \leq y} \log p = \theta(y)$. Then by Corollary 2.7, we have

$$\frac{\phi(n)}{n} = \prod_{p \leq y}\left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log y} + O\left(\frac{1}{(\log y)^2}\right).$$

Since $\log\log n = \log(\theta(y)) = \log y + O(1)$ by (2.5), we have for $n \in \mathcal{E}$

$$\phi(n) = \frac{ne^{-\gamma}}{\log\log n}\left\{1 + O\left(\frac{1}{\log\log n}\right)\right\}.$$

If $n \notin \mathcal{E}$ then there exists an $m < n$ such that $m \in \mathcal{E}$ and $\frac{\phi(m)}{m} < \frac{\phi(n)}{n}$. Therefore

$$\begin{aligned} \frac{\phi(n)}{n} > \frac{\phi(m)}{m} &= \frac{e^{-\gamma}}{\log\log m}\left\{1 + O\left(\frac{1}{\log\log m}\right)\right\} \\ &\geq \frac{e^{-\gamma}}{\log\log n}\left\{1 + O\left(\frac{1}{\log\log n}\right)\right\}. \end{aligned}$$

Note that $\phi(n) = \frac{ne^{-\gamma}}{\log\log n}\left\{1 + O\left(\frac{1}{\log\log n}\right)\right\}$ holds for all n of the type (2.9), so the proof is complete. □

CHAPTER III

MAIN RESULT

In this chapter, we prove some lemmas and show that the sequence $(a^n/n)_{n\in\mathcal{B}}$ is uniformly distributed modulo 1 where

$$\mathcal{B} = \{pq \ : \ p, q \text{ primes}, \ a^q \leq pq\}.$$

The following lemma is an asymptotic estimate of the number of elements in $\mathcal{B}(N)$ where $\mathcal{B}(N) = \mathcal{B} \cap [1, N]$ for each positive integer N.

Lemma 3.1. *We have*

$$|\mathcal{B}(N)| \sim \frac{N \log\log\log N}{\log N}.$$

Proof. We observe that if $pq \in \mathcal{B}(N)$ then

$$\frac{a^q}{q} \leq p \leq \frac{N}{q}.$$

Let Q be the largest prime q such that $a^q \leq N$. So $Q \sim \frac{\log N}{\log a}$. Then by prime number theorem, we have

$$\sum_{q\leq Q} \pi\left(\frac{a^q}{q}\right) \ll \sum_{q\leq Q} \frac{a^q}{q^2} \ll \frac{a^Q}{Q^2} \ll \frac{N}{\log^2 N}.$$

Thus, we have

$$|\mathcal{B}(N)| = \sum_{q\leq Q} \pi\left(\frac{N}{q}\right) - \pi\left(\frac{a^q}{q}\right) = \sum_{q\leq Q} \pi\left(\frac{N}{q}\right) + O\left(\frac{N}{\log^2 N}\right).$$

Use prime number theorem again, then

$$\sum_{q\le Q}\pi\left(\frac{N}{q}\right)\sim\sum_{q\le Q}\frac{N}{q\log(N/q)}$$
$$\sim\frac{N}{\log N}\sum_{q\le Q}\frac{1}{q}.$$

Using Mertens' theorem, we have

$$\sum_{q\le Q}\pi\left(\frac{N}{q}\right)\sim\frac{N\log\log\log N}{\log N}.$$

Therefore,

$$|\mathcal{B}(N)|\sim\frac{N\log\log\log N}{\log N}.$$

□

For a pair of primes $p>q$ we define $u_q(p)$ by the condition

$$u_q(p)p\ \equiv\ 1\ (\mathrm{mod}\ q),\quad 1\le u_q(p)\le q-1. \tag{3.1}$$

For $\alpha,\beta\in\mathbb{R}$, we also write $\alpha\ \equiv\ \beta\ (\mathrm{mod}\ 1)$ if $\alpha-\beta\in\mathbb{Z}$.

Lemma 3.2. *For primes $p>q$, we have*

$$\frac{a^{pq}}{pq}\equiv\frac{(a^p-a)}{q}u_q(p)+\frac{a^q}{pq}\ (mod\ 1).$$

Proof. By (3.1), we have

$$\frac{a^{p-1}-1}{p}\equiv\left(a^{p-1}-1\right)u_q(p)\ (\mathrm{mod}\ q),$$

and then

$$\begin{aligned}\frac{a^{pq}}{pq} &= \frac{a^{(p-1)(q-1)}a^{p+q-1}}{pq}\\ &\equiv \frac{a^{p+q-1}}{pq}\\ &\equiv \frac{a^q}{q}\frac{(a^{p-1}-1)}{p} + \frac{a^q}{pq}\\ &\equiv \frac{a}{q}(a^{p-1}-1)u_q(p) + \frac{a^q}{pq}\\ &\equiv \frac{(a^p-a)}{q}u_q(p) + \frac{a^q}{pq} \pmod 1.\end{aligned}$$

□

The following lemmas will be used to prove our main result.

Lemma 3.3. *For every fixed nonzero integer constant h, $a \geq 2$, and prime number q, we have*

$$s(a,h,q) := \sum_{1\leq u\leq q-1} \sum_{\substack{1\leq v\leq q-2\\ (v,q-1)=1}} \boldsymbol{e}\left(\frac{h(a^v-a)u}{q}\right) \leq \begin{cases} \frac{2q(q-1)}{\mathrm{ord}_q a}, & \text{if } (q,ah)=1,\\ \phi\left(q(q-1)\right), & \text{if } (q,ah)>1.\end{cases}$$

Proof. The case $(q, ah) > 1$ is obvious.

Now suppose $(q, ah) = 1$. We have

$$\sum_{u=1}^{q-1} \mathbf{e}\left(\frac{h(a^v-a)u}{q}\right) = \sum_{u=1}^{q-1} \mathbf{e}\left(\frac{ah(a^{v-1}-1)u}{q}\right) = \begin{cases} -1, & \text{if } q \nmid a^{v-1}-1\\ q-1, & \text{if } q | a^{v-1}-1.\end{cases}$$

Let

$$V = \{1 \leq v \leq q-2 : (v, q-1) = 1,\ a^{v-1} \equiv 1 \pmod q\}.$$

Thus

$$s(a,h,q) = -\left(\phi(q-1) - |V|\right) + (q-1)|V| = -\phi(q-1) + q|V|.$$

Since $m = \mathrm{ord}_q a$ is the smallest positive integer such that $a^m \equiv 1 \pmod q$, then for each $v \in V$, we can write $v = mk + 1$ for some $k = 0, 1, ..., \frac{q-1}{m} - 1$.

Hence,

$$|s(a, h, q)| \leq \phi(q-1) + \frac{q(q-1)}{\mathrm{ord}_q a} \leq \frac{2q(q-1)}{\mathrm{ord}_q a}.$$

□

Lemma 3.4. *For q primes and $N > q^2$ and $Q = \log N / \log a$, we have*

$$S_0 := \sum_{q \leq Q} \frac{\pi(N/q)}{\phi(q(q-1))} s(a, h, q) \ll \frac{N}{\log N} \left(1 + \sum_{q|h} \frac{1}{q} \right).$$

Proof. By Lemma 3.3, we have

$$\begin{aligned} |S_0| &\leq 2N \sum_{\substack{q \leq Q \\ q \nmid ah}} \frac{q(q-1)}{q\phi(q(q-1)) \log(N/q) \mathrm{ord}_q a} + N \sum_{\substack{q \leq Q \\ q|ah}} \frac{\phi(q(q-1))}{q\phi(q(q-1)) \log(N/q)} \\ &\ll \frac{N}{\log N} \sum_{q \leq Q} \frac{1}{\phi(q-1)\mathrm{ord}_q a} + \frac{N}{\log N} \sum_{\substack{q \leq Q \\ q|ah}} \frac{1}{q}. \end{aligned}$$

Using $\mathrm{ord}_q a \geq \log q / \log a$ and the lower bound (2.8), $\phi(n) \gg \frac{n}{\log \log n}$, we have

$$\sum_{q \leq Q} \frac{1}{\phi(q-1)\mathrm{ord}_q a} \ll \sum_{q} \frac{\log \log q}{q \log q} = O(1).$$

Hence

$$S_0 \ll \frac{N}{\log N} \left(1 + \sum_{q|h} \frac{1}{q} \right).$$

□

Lemma 3.5. *For N sufficiently large and $Q = \log N / \log a$, we have*

$$\tilde{S}(h, N) := \sum_{pq \in \mathcal{B}(N)} \boldsymbol{e}\left(\frac{h(a^p - a)u_q(p)}{q} \right) \ll \frac{N}{\log N} \left(1 + \sum_{q|h} \frac{1}{q} \right).$$

Proof. First we fix a prime number q and a pair of integers u, v with $1 \leq u, v \leq q-1$ and $(u, q) = (v, q-1) = 1$. By the Chinese Remainder Theorem, we see that all prime p which satisfy

$$up \equiv 1 \pmod{q}, \quad p \equiv v \pmod{q-1},$$

belong to a certain arithmetic progression $z_q(u,v) \pmod{q(q-1)}$. Thus,

$$\begin{aligned}\tilde{S}(h,N) = \sum_{q \le \frac{\log N}{\log a}} \sum_{u=1}^{q-1} \sum_{\substack{v=1\\(v,q-1)=1}}^{q-2} \mathbf{e}\left(\frac{h(a^v - a)u_q(p)}{q}\right)\\ \times \left[\pi\left(\frac{N}{q}; q(q-1), z_q(u,v)\right) - \pi\left(\frac{a^q}{q}; q(q-1), z_q(u,v)\right)\right].\end{aligned}$$

Using (2.1) (with $A = 2$) and (2.2) and noticing that the sum over u and v contains $\phi\left(q(q-1)\right)$ terms, we obtain

$$\tilde{S}(h,N) = S_0 + O(S_1 + S_2),$$

where

$$S_0 = \sum_{q \le Q} \frac{\pi(N/q)}{\phi(q(q-1))} s(a,h,q) \ll \frac{N}{\log N}\left(1 + \sum_{q|h} \frac{1}{q}\right),$$

$$S_1 = \sum_{q \le \log N/\log a} \frac{a^q}{q^2} \ll \frac{a^Q}{Q^2} \ll \frac{N}{Q^2} \ll \frac{N}{\log^2 N}, \quad \text{and}$$

$$S_2 = \sum_{q \le \log N/\log a} \frac{N}{q(\log N/q)^2} \ll \frac{N}{\log^2 N} \sum_{q \le \log N} \frac{1}{q} \ll \frac{N \log\log\log N}{\log^2 N}.$$

Therefore

$$\tilde{S}(h,N) \sim S_0 \ll \frac{N}{\log N}\left(1 + \sum_{q|h} \frac{1}{q}\right).$$

□

We will use the following theorem in the proof of Theorem 3.7, (see [4].)

Theorem 3.6. *Let* $0 < \theta < 1$. *Then, for* $x^\theta \le y \le x$, *we have*

$$\pi(x) - \pi(x-y) \le (2-\delta)\frac{y}{\log y}$$

for some $\delta = \delta(\theta) > 0$, *provided that* x *is sufficiently large in terms of* θ.

We are now able to prove the main theorem of this thesis. Basically, our idea in the proof follow the one in the proof of the result in [2].

Theorem 3.7. *The discrepancy* D_N *of the sequence* $(a^n/n)_{n\in\mathcal{B}(N)}$ *is*

$$D_N = O\left(\frac{1}{\log\log\log\log N}\right).$$

Hence, the sequence $(a^n/n)_{n\in\mathcal{B}}$ *is u.d. mod 1.*

Proof. Recall that $\mathcal{B} = \{pq \ : \ p, q \text{ primes}, \ a^q \le pq\}$ and we set $\mathcal{B}(N) = \mathcal{B} \cap [1, N]$ for each positive integer N. Then by Lemma 3.2, we have

$$\begin{aligned} S(h,N) &:= \sum_{pq\in\mathcal{B}(N)} \mathbf{e}\left(\frac{ha^{pq}}{pq}\right) \\ &= \sum_{pq\in\mathcal{B}(N)} \mathbf{e}\left(h\left(\frac{(a^p-a)u_q(p)}{q} + \frac{a^q}{pq}\right)\right) \\ &= \tilde{S}(h,N) + E, \end{aligned}$$

where

$$\tilde{S}(h,N) = \sum_{pq\in\mathcal{B}(N)} \mathbf{e}\left(\frac{h(a^p-a)u_q(p)}{q}\right) \ll \frac{N}{\log N}\left(1 + \sum_{q|h}\frac{1}{q}\right) \qquad \text{(by Lemma 3.5)}$$

and

$$
\begin{aligned}
|E| &\ll \sum_{pq\in\mathcal{B}(N)} \left|1-\mathbf{e}\left(\frac{ha^q}{pq}\right)\right| \\
&\ll \sum_{pq\in\mathcal{B}(N)} \left\{\frac{|h|a^q}{pq}\right\} \\
&\ll \sum_{a^q\le N/q} \frac{|h|a^q}{q}\sum_{p\le N}\frac{1}{p} + \sum_{q\le\frac{\log N}{\log a}}\ \sum_{\frac{a^q}{q}\le p\le a^q} |h|\left\{\frac{a^q}{pq}\right\}.
\end{aligned}
$$

Using Mertens' theorem, we have

$$
\begin{aligned}
|E| &\ll \sum_{a^q\le N/q} \frac{|h|a^q}{q}\log\log N + \sum_{q\le\frac{\log N}{\log a}}\ \sum_{\frac{a^q}{q}\le p\le a^q} |h| \\
&\ll \frac{|h|N\log\log N}{\log^2 N} + |h|\sum_{q\le\frac{\log N}{\log a}} \pi(a^q)-\pi\left(\frac{a^q}{q}\right).
\end{aligned}
$$

Using Theorem 3.6 with $\theta = 0.5$, we obtain

$$
\begin{aligned}
|E| &\ll \frac{|h|N\log\log N}{\log^2 N} + |h|\sum_{q\le\frac{\log N}{\log a}} \frac{a^q-a^q/q}{\log(a^q(1-1/q))} \\
&\ll \frac{|h|N\log\log N}{\log^2 N} + |h|\sum_{q\le\frac{\log N}{\log a}} \frac{a^q(1-1/q)}{q\log a} \\
&\ll \frac{|h|N\log\log N}{\log^2 N} + |h|\sum_{q\le\frac{\log N}{\log a}} \frac{a^q}{q} \\
&\ll \frac{|h|N\log\log N}{\log^2 N} + |h|\frac{N}{\log N} \\
&\ll |h|\frac{N}{\log N}.
\end{aligned}
$$

Substituting the bound of $\tilde{S}(h,N)$ and E, we get

$$
S(h,N) \ll \frac{|h|N}{\log N} + \frac{N}{\log N}\left(1+\sum_{q|h}\frac{1}{q}\right).
$$

Let $L = \frac{\log\log\log N}{\log\log\log\log N}$ and $M = |\mathcal{B}(N)|$. Then apply Lemma 1.6 to obtain the bound of the discrepancy D_N of the sequence $\mathcal{B}(N)$ as follows:

$$\begin{aligned}
D_N &\ll \frac{1}{L} + \frac{1}{M} \sum_{0<|h|\le L} \frac{|S(h,N)|}{|h|} \\
&\ll \frac{1}{L} + \frac{LN}{M\log N} + \frac{N\log L}{M\log N} + \frac{N}{M\log N} \sum_{0<|h|\le L} \frac{1}{|h|} \sum_{q|h} \frac{1}{q} \\
&\ll \frac{\log\log\log\log N}{\log\log\log N} + \frac{\log N}{N\log\log\log\log N}\frac{N}{\log N} \\
&\quad + \frac{\log N \log L}{(\log\log\log N)\log N} + \frac{1}{\log\log\log N} \sum_{q} \frac{1}{q} \sum_{0<|l|\le L/q} \frac{1}{|ql|} \\
&\ll \frac{\log\log\log\log N}{\log\log\log N} + \frac{1}{\log\log\log\log N} + \frac{\log L}{\log\log\log N} \\
&\ll \frac{1}{\log\log\log\log N}.
\end{aligned}$$

This completes the proof of the theorem. □

REFERENCES

[1] Banks, W.D. Garaev, M.Z. Luca, F. and Shparlinski, I. E.: Uniform distribution of fractional parts related to pseudoprimes, *Canad. J. Math.*, **61** (2009), 481–502.

[2] Cilleruelo, J. Kumchev, A. Luca, F. Rué, J. and Shparlinski, I. E.: On the fractional parts of a^n/n, *Bull. London. Math. Soc.*, **45** (2013), 249–256.

[3] Drmota, M. and Tichy, R.: *Sequences, discrepancies and applications*, Springer, Berlin, 1997.

[4] Friedlander, J. and Iwaniec, H.: *Opera de cribro*, American Mathematical Society, 2010.

[5] Iwaniec, H. and Kowalski, E.: *Analytic number theory*, American Mathematical Society, 2004.

[6] Kuipers, L. and Niederreiter, H.: *Uniform distribution of sequences*, Dover publication, New York, 2006.

[7] Matomăki, K.: Large differences between consecutive primes, *Q. J. Math. (Oxford)*, **58** (2007), 489–518.

[8] Montgomery, H.L. and Vaughan, R.C.: *Multiplicative number theory I. Classical theory*, Cambridge University Press, New York, 2007.

[9] Pinkus, A.: Density in Approximation Theory, *Surveys in Approximation Theory.*, **1** (2005), 1–45.

VITA

Name	Mr. Panithan Mothong
Date of Birth	5 August 1989
Place of Birth	Ubon Ratchathani, Thailand
Education	B.Sc. (Mathematics)(Second Class Honours), Mahidol University, 2012