National Library of Canada
Bibliothèque nationale du Canada

Acquisitions and Bibliographic Services Branch
Direction des acquisitions et des services bibliographiques

395 Wellington Street
Ottawa, Ontario
K1A 0N4

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

EXPONENTIAL SUMS AND APPLICATIONS

by

Ping Ding

M.Sc., Institute of Mathematics, Chinese Academy of Sciences, 1982

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in the Department

of

Mathematics and Statistics

© Ping Ding 1993

SIMON FRASER UNIVERSITY

February, 1993

All rights reserved. This work may not be
reproduced in whole or in part, by photocopy
or other means, without the written permission of the author.

National Library of Canada
Bibliothèque nationale du Canada

Acquisitions and Bibliographic Services Branch
Direction des acquisitions et des services bibliographiques

395 Wellington Street
Ottawa, Ontario
K1A 0N4

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

ISBN 0-315-91136-0

Canada

APPROVAL

Name: Ping Ding

Degree: Doctor of Philosophy

Title of thesis: Exponential Sums and Applications

Examining Committee:

Chairman: Dr. S. K. Thomason

Dr. A. R. Freedman
Senior Supervisor

Dr. A. H. Lachlan

Dr. B. R. Alspach

Dr. J. L. Berggren

Dr. H. Halberstam
External Examiner
Professor
University of Illinois at Urbana-Champaign

Date Approved: March 11, 1993

PARTIAL COPYRIGHT LICENSE

I hereby grant to Simon Fraser University the right to lend my thesis, project or extended essay (the title of which is shown below) to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me or the Dean of Graduate Studies. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Title of Thesis/Project/Extended Essay

Exponential sums and applications

Author: ______

(signature)

Ping Ding

(name)

Feb 5, 1993

(date)

ABSTRACT

Let q be a positive integer and

$$f(x) = a_k x^k + \dots + a_1 x + a_0 \quad (k \geq 3)$$

be a polynomial with integral coefficients such that $(a_1, \dots, a_k, q) = 1$. Write

$$S(q, f(x)) = \sum_{x=1}^{q} e^{2\pi i f(x)/q} .$$

We proved that

$$|S(q, f(x))| \leq e^{ck} q^{1-1/k}, \quad \text{for } k \geq 3,$$

where c = 1.74. This improves previous results that c = 2 (Qi M. G. and Ding P.) and c = 1.85 (Lu M. G.).

Define t satisfying $p^t \| (ka_k, \dots, 2a_2, a_1)$, where the symbol $\|$ means that t is the highest power of p such that $p^t \mid (ka_k, \dots, 2a_2, a_1)$. Let $\mu_1, \dots, \mu_r$ be the different zeros modulo p of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod{p}, \qquad 0 \leq x < p,$$

and let $m_1, \dots, m_r$ be their multiplicities. Set $\max_{1 \leq i \leq r} m_i = M = M(f)$ and

$$\sum_{i=1}^{r} m_i = m = m(f).$$

Let

$$\tau = \left[\frac{\log k}{\log p}\right].$$

we prove the following result:

If $n \geq 2$ or $n = 1$ and $p \leq k$, then

$$| S(p^n, f(x)) | \leq m p^{\tau/(M+1)} p^{t/(M+1)} p^{n[1 - 1/(M+1)]} .$$

This improves the previous results by using k (Chalk) and $k^{1/2}$ (Ding) to substitute $p^{\tau/(M+1)}$ as $p^\tau \leq k$ and $M \geq 1$. Actually, this result is the best possible as shown by an example at the end of this section.

Let k, s, and q be positive integers.

Let N(q) denote the number of solutions of the congruences

$$\begin{aligned} x_1 + \dots + x_s &\equiv b_1, \\ \dots\dots & \qquad \pmod{q} \qquad (*) \\ (x_1)^k + \dots + (x_s)^k &\equiv b_k, \end{aligned}$$

where $1 \leq x_i \leq q$, $(x_i, q) = 1$, $1 \leq i \leq s$.

Let $q = p^n$ with p a prime, n a positive integer, $k \geq 3$, $s > 2k^2$. Then when $p \geq (k-1)^{2k/(k-2)}$, the congruence (*) is always solvabale. This largely reduces Hua's result $p > 2^{k^2} k^{3k}$ to k^2, approximately.

We denote by $V_a(p^n, f(x))$ the a set of f modulo p^n, that is,

$$V_a(p^n, f(x)) = \{x \bmod p^n:\ f(x) \equiv a \pmod{p^n}\}$$

and put

$$N = N(p^n, f(x)) = \text{Card } V_a(p^n, f(x)).$$

We prove that $N(p^n, f(x)) < (2 + \sqrt{2})\, m\, p^{\tau/(M+1)}\, p^{t/(M+1)}\, p^{n[1 - (1/(M+1))]}$. This improves a previous result of Chalk.

Let $k \geq 2$ and $q = g(k) - G(k)$, where $g(k)$ and $G(k)$ are same as in Waring's problem. For each positive integer $r \geq q$ let $u_r' = g(k) + r - q$. Then for every $\varepsilon > 0$ and all $N \geq N(r, \varepsilon)$, we construct a finite set A of k-th powers such that $|A| \leq (r(2+\varepsilon)^r+1)N^{1/(k+r)}$ and every nonnegative integer $n \leq N$ is the sum of u_r' elements of A. Some related results are also obtained. These results improve and generalize Nathanson's results.

For every $\varepsilon > 0$, we construct a set A of squares with $|A| < N^{1/k+\varepsilon}$ for sufficiently large N and every integer n, $\omega \leq n \leq N$, is a sum of $(k + 1)$ nonvanishing squares in A for some positive integer ω and for all $k \geq 4$.

The second result is that for each $k \geq 3$ we construct a set A of squares such that $|A| < k(2+\varepsilon)^k N^{1/k}$ and every integer n, $N^{\varepsilon} < n \leq N$, is a sum of $(k+3)$ distinct elements of A, where ε is a small positive number less than 0.0064.

Acknowledgements

I would like to thank my Senior Supervisor, Dr. A. R. Freedman, for his encouragement, guidance, and patience during the preparation of this thesis.

I also wish to thank the Office of the Dean of Graduate Studies, the Department of Mathematics & Statistics, and Professor A. R. Freedman for their financial support.

TABLE OF CONTENTS

INTRODUCTION

In 1770 E. Waring asserted without proof in his *Meditations Algebraicae* that every natural number is a sum of at most nine positive integral cubes, also a sum of at most 19 biquadrates, and so on. By this it is usually assumed that he believed that for every natural number $k \geq 2$ there exists a number s such that every natural number is a sum of at most s kth powers of natural numbers, and that the least such s, say g(k), satisfies $g(3) = 9$, $g(4) = 19$. It was not until 1770 that $g(2) = 4$ was given, by Lagrange, who built on earlier work of Euler. During the next 139 years, special cases of the problem were solved for k = 3, 4, 5, 6, 7, 8, 10. It was in 1909 that Hilbert solved the problem in the affirmative for all k. His proof was extremely complicated in its detailed arguments.

Many important advances in analytic number theory in the twentieth century have been achieved by either the sieve method or the Hardy-Littlewood circle method. These methods, originating in fundamental work of the second and third decade of this century, have now been developed into a delicate theory which has turned out to be a very powerful tool in the solution of problems from additive and multiplicative number theory. For these methods there are two excellent books respectively, one is Halberstam and Richert's «Sieve methods» [19], and other is Vaughan's «The Hardy-Littlewood method» [42].

Vinogradov made great technical improvements to Hardy-Littlewood's method in 1930s and proved Goldbach's problem for odd numbers, that is, every sufficiently large odd number is a sum of three primes. His method requires estimating the exponential sums for primes. Some other problems in number theory also need to estimate various exponential sums. Therefore, Hua L. K. placed the estimation of complete exponential sums as the fundamental lemma in his book «Additive theory of prime numbers» [26].

In Chapter 1 we give two estimations of complete exponential sums which improve previous results. In the first section, we consider the complete trigonometric sums defined by

$$S(q, f(x)) = \sum_{x=1}^{q} e^{2\pi i f(x)/q},$$

where q is a positive integer and

$$f(x) = a_k x^k + \dots + a_1 x + a_0,$$

$a_1, \dots, a_k$ are integers such that $(a_1, \dots, a_k, q) = 1$. Hua [25] first established that

$$S(q, f(x)) << q^{1 - 1/k + \varepsilon},$$

where ε is a small positive number and the symbol "<<" is Vinogradov's one, that is,

$$f << g$$

means that there is a constant C which may depend on some variables such that

$$|f| \leq Cg.$$

Hua's result is important since the main order (1 - 1/k) is the best possible. In 1953, Necheav [34] gave an explicit estimate

$$|S(q, f(x))| \leq e^{2^k} q^{1 - 1/k},$$

and since then, by the efforts of a few mathematicians, the coefficient e^{2^k} here went down rapidly to $e^{6.1k}$, by Chen J. R. [11] in 1977, and to $e^{1.85k}$, by Lu M. G. [30] in 1985. Our main result in the first section is to establish

$$|S(q, f(x))| \leq e^{1.74k} q^{1 - 1/k},$$

which is the best one up to now. One possible application of this result is to the estimations of $g(\phi)$ if further difficulties could be overcome, where g(x) is well-known in Waring's problem and ϕ is a polynomial with integral coefficients. The induction procedure in the first section starts from 2n + 1 instead of 2n + 2 and the difficulties are dealt with by individual cases. As Stechin [41] already established an asymptotic inequality

$$\left|\sum_{x=1}^{q} e^{2\pi i f(x)/q}\right| \leq e^{k + O(k/\log k)} q^{1 - 1/k}, \qquad \text{for } k \to \infty,$$

it is obvious that one of the cruxes is to obtain good estimates for relatively small k, qualitatively say, at present hand, for $5 \leq k \leq 64$. We deal with small k according to $k \in (2^i, 2^{i+1}]$ for $2 \leq i \leq 5$. If we write $q = p^n$, where p is a prime and n is a positive integer, then another crux is to get good estimates for small p. We shall give careful estimations for

$p = 2$ and 3. We also sufficiently use the properties of t_j for small prime p. One of the principle difficulties in the second section is induction. To overcome the difficulty we introduce a parameter τ which allows us to apply induction on n according to $n \le 2\tau$ or $n > 2\tau$.

In Chapter 2 we consider some applications of exponential sums to congruences. Let k, s , and q be positive integers. Let N(q) denote the number of solutions to the system of congruences

$$\begin{aligned} x_1 + \dots + x_s &\equiv b_1, \\ \dots\dots & \qquad\qquad (\text{mod } q) \\ (x_1)^k + \dots + (x_s)^k &\equiv b_k, \end{aligned}$$

where $1 \le x_i \le q$, $(x_i, q) = 1$, $1 \le i \le s$. In the first section we shall prove that for $q = p^n$, where p is a prime and n a positive integer, if

$$p \ge b(k),$$

then the above system of congruences is always solvable for $s \ge 2k^2$, where

$$b(k) \approx k^2,$$

which reduces Hua's condition (cf. [26]) that

$$p > 2^{k^2} k^{3k}.$$

The precise upper bounds to

$$\left|\sum_{x=1}^{p^n} e^{2\pi i f(x)/p^n}\right|, \qquad \text{where p is a prime and n is a positive integer,}$$

for $k < p \le (k - 1)^{2k/(k - 2)}$ at hand are not good enough to enable us to reduce the conditions so that we can't directly apply our results in Chapter 1 The second section is a simple application of the second section in Chapter 1 which improves Chalk's result [9].

In Chapter 3 by considering the differences between g(k) and G(k), where g(k) is as above and G(k) denotes the minimal value of r such that every sufficiently large integer is the sum of r kth powers, we first construct a finite set with relatively small cardinality such that every positive integer $n \leq N$ is the sum of certain elements in this set for sufficiently large N. Three theorems are proven here. Those results improve Nathanson's. Unfortunately, we can't obtain an infinite version for this question at present. Our idea is to cut the interval [1, N] into finitely many pieces. We then start from the lowest interval and translate higher interval to lower one. The second part of Chapter 3 deals with the small sets for nonvanishing squares and distinct squares. The idea is similar to the first section but the difficulty for distinct squares is to show that if n is expressed as a sum of some elements in the constructed small set A then those elements must be distinct.

CHAPTER 1. ESTIMATION OF EXPONENTIAL SUMS

§1.1 Estimate of complete trigonometric sums.

1. INTRODUCTION.

Let q be a positive integer and

$$f(x) = a_k x^k + \dots + a_1 x + a_0 \quad (k \geq 3) \tag{1.1}$$

be a polynomial with integral coefficients such that $(a_1, \dots, a_k, q) = 1$. Write

$$S(q, f(x)) = \sum_{x=1}^{q} e^{2\pi i f(x)/q}, \tag{1.2}$$

where $i = \sqrt{-1}$.

In 1940, Hua L. K. [25] first proved that

$$S(q, f(x)) = O(q^{(1-1/k)+\varepsilon}),$$

and about 1947 improved this to

$$S(q, f(x)) = O(q^{1-1/k}),$$

where the constant implied by "O" depends only on k. This is an important result because the main order (1 - 1/k) is the best possible. Afterwards, some work done on this problem is as follows:

1953	Nechaev V. I. [34]	$\lvert S(q, f(x))\rvert \leq e^{2^k} q^{1-1/k}$,
1959	Chen J. R. [10]	$\lvert S(q, f(x))\rvert \leq e^{3k^{2+6/k}} q^{1-1/k}$,
1975	Nechaev V. I. [35]	$\lvert S(q, f(x))\rvert \leq e^{5k^2/\log k} q^{1-1/k}$,
1977	Chen J. R. [11]	$\lvert S(q, f(x))\rvert \leq e^{6.1k} q^{1-1/k}$,
1984	Lu M. G. [30]	$\lvert S(q, f(x))\rvert \leq e^{3k} q^{1-1/k}$,
1985	Ding P. & Qi M. G. [13]	$\lvert S(q, f(x))\rvert \leq e^{2k} q^{1-1/k}$,

1985 Lu M. G. [31] $|S(q, f(x))| \le e^{1.85k} q^{1-1/k}$,

where each inequality holds for fixed $k \ge 3$ and all f, and in 1977, Stechin S. B. [41] established that

$$|S(q, f(x))| \le e^{k+O(k/\log k)} q^{1-1/k}, \quad \text{for } k \to \infty.$$

We now prove the following

Theorem 1.1.

$$|S(q, f(x))| \le e^{1.74k} q^{1-1/k}, \quad \text{for } k \ge 3.$$

2. BASIC LEMMAS.

Lemma 1.1. For positive integers k and real y,

$$k^{(y-1)/k} \le y \qquad (2 \le y \le k-1), \tag{1.3}$$

and

$$(k-2)^{1/k} \le y^{1/(y+1)}. \qquad (5 \le k, 2 \le y \le k-1) \tag{1.4}$$

Proof. We first prove (1.3).

$$k^{(y-1)/k} \le y \quad (2 \le y \le k-1)$$

iff

$$k^{1/k} \le y^{1/(y-1)},$$

that is,

$$\frac{\log k}{k} \le \frac{\log y}{y-1}.$$

The right hand side is decreasing for $y \ge 2$ and there is at least

$$\frac{\log(k-1)}{k-2} \ge \frac{\log k}{k}$$

if $k \ge 3$.

We now establish (1.4). Obviously it suffices to prove

$$(k-2)^{(y+1)/k} \le y, \qquad \text{for } k \ge 5 \text{ and } 2 \le y \le k-1, \tag{1.5}$$

that is,

$$(k-2)^{1/k} \le y^{1/(y+1)},$$

or

$$\frac{\log(k-2)}{k} \le \frac{\log y}{y+1}. \tag{1.6}$$

For $y \ge 3.6$, $\frac{\log y}{y+1}$ is decreasing, and so

$$\frac{\log y}{y+1} \ge \frac{\log(k-1)}{k} > \frac{\log(k-2)}{k}$$

as required. This leaves $2 \le y \le 3.6$, when

$$\frac{\log y}{y+1} \ge \frac{\log 2}{3} = 0.2310\ldots .$$

On the other hand,

$$\frac{\log(k-2)}{k} = 0.2197\ldots \qquad \text{at } k = 5,$$

$$\frac{\log 2}{3} \quad \text{at } k = 6,$$

and is $\le 0.229919\ldots$ for $k \ge 7$. Hence (1.6) follows, so that (1.5) and (1.4). This completes the proof.

Now let $f(x)$ be as in (1.1) with q equal to a power of a prime p.

Define t to be that exponent satisfying $p^t \| (ka_k, \ldots, 2a_2, a_1)$, where $p^t \| A$ means $p^t \mid A$ but $p^{t+1} \nmid A$. By $(a_1, \ldots, a_k, p) = 1$, we deduce that $p^t \le k$. Let $\mu_1, \ldots, \mu_r$ be the different solutions modulo p of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod{p}, \quad 0 \le x < p, \tag{1.7}$$

and let $m_1, \ldots, m_r$ be their multiples. Put

$$m_1 + \ldots + m_r = m. \tag{1.8}$$

Clearly $r \le m \le k - 1$.

Let σ_j satisfy $p^{\sigma_j} \| (f(py + \mu_j) - f(\mu_j))$, and set

$$g_{\mu_j}(y) = p^{-\sigma_j} (f(py + \mu_j) - f(\mu_j)). \tag{1.9}$$

Define t_j satisfying $p^{t_j} \| g'_{\mu_j}(y)$. As before, $p^{t_j} \le k$.

Lemma 1.2. [31] Let p be a prime, and μ_j a simple root of $p^{-t}f'(x) \equiv 0 \pmod p$. Then

$$\sigma_j = t + 2 \text{ and } t_j = 0 \quad \text{when } p > 2$$

and

$$\sigma_j = t + 1 \text{ and } t_j = 1 \quad \text{when } p = 2.$$

Lemma 1.3. [31] If t = 0, then

$$g_{\mu_j}(y) \equiv p^{-\sigma_j}(pyf'(\mu_j) + (py)^2\frac{f''(\mu_j)}{2!} + \dots + (py)^{m_j+1}\frac{f^{(m_j+1)}(\mu_j)}{(m_j+1)!}) \pmod p \qquad (1.10)$$

If $m_j = 1$ and $t \geq 1$, then

i) when $p \geq 5$,

$$g_{\mu_j}(y) \equiv p^{-\sigma_j}(\,pyf'(\mu_j) + (py)^2\frac{f''(\mu_j)}{2!}) \pmod p, \qquad (1.11)$$

ii) when p = 3,

$$g_{\mu_j}(y) \equiv 3^{-\sigma_j}(\,3yf'(\mu_j) + (3y)^2\frac{f''(\mu_j)}{2!} + (3y)^3\frac{f'''(\mu_j)}{3!}) \pmod 3, \qquad (1.12)$$

and iii) when p = 2,

$$g_{\mu_j}(y) \equiv 2^{-\sigma_j}(2y)^2\frac{f''(\mu_j)}{2!} \pmod 2. \qquad (1.13)$$

Lemma 1.4. [26] Let p be a prime and $f(x) = a_kx^k + \dots + a_1x + a_0$ a polynomial with integral coefficients such that $p \nmid (a_k, \dots, a_1)$. Let μ be a root of the congruence

$$f'(x) \equiv 0 \pmod{p^{t+1}}, \quad 0 \leq x < p, \qquad (1.14)$$

and let σ satisfy $p^{\sigma} \,\|\, (\,f(px + \mu) - f(\mu)\,)$, then

$$1 \leq \sigma \leq k. \qquad (1.15)$$

Lemma 1.5. [13] Let μ_j be a root with multiplicity m_j of the congruence

$$f'(x) \equiv 0 \pmod{p^{t+1}}, \quad 0 \leq x < p,$$

and σ_j satisfy $p^{\sigma_j} \,\|\, (\,f(px + \mu_j) - f(\mu_j)\,)$, then

$$2 \le \sigma_j \le m_j + t + 1. \tag{1.16}$$

Let $g_{\mu_j}(y)$ satisfy (1.9) and $p^{t_j} \| g'_{\mu_j}(y)$, then

$$\sigma_j + t_j \le m_j + t + 1, \tag{1.17}$$

and the number of solutions of the congruence

$$g'_{\mu_j}(y) \equiv 0 \pmod{p^{t_j+1}} \qquad (0 \le y < p)$$

does not exceed m_j.

Lemma 1.6. [26] Set

$$S_{\mu_j,p^n} = \sum_{\substack{x=1 \\ x \equiv \mu_j \,(\mathrm{mod}\, p)}}^{p^n} e_{p^n}(f(x)), \tag{1.18}$$

where $e_q(f(x)) = e^{2\pi i f(x)/q}$.

Then

$$|S_{\mu_j,p^n}| \begin{cases} \le p^{n-1} & \text{for all } n \ge 1 \\ = p^{\sigma_j - 1}|S(p^{n-\sigma_j}, g_{\mu_j}(y))| & \text{if } n > \sigma_j \end{cases} \tag{1.19}$$

Lemma 1.7. Let f(x) be as in (1.1). When $n \ge 2t+2$, we have

$$|S(p^n, f(x))| \le \sum_{j=1}^{r} |S_{\mu_j,p^n}| . \tag{1.20}$$

If p is an odd prime and f(x) satisfies the above conditions with $t \ge 1$, then when $n = 2t+1$, (1.20) holds. If $p = 2$ and $t \ge 2$, then (1.20) also holds for $n = 2t+1$. If p is an odd prime and $t \ge 2$, then (1.20) still holds for $n = 2t$.

Proof. We only give a proof for the case p is an odd prime, $t \ge 2$, and $n = 2t$. For the other cases refer to [13].

We make substitution $x = y + zp^{n-t-1}$ in $S(p^n, f(x))$, where y and z run independently through

$$y = 1, \dots, p^{n-t-1}; \; z = 0, \dots, p^{t+1} - 1.$$

When $n = 2t$,

$$S(p^n, f(x)) = \sum_{x=1}^{p^n} e_{p^n}(f(x))$$
$$= \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^n}(p^{n-t-1}zf'(y) + \frac{1}{2}p^{2(n-t-1)}z^2f''(y) + \dots)$$
$$= \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)),$$

since

$$\sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)) = \begin{cases} p^{t+1} & \text{if } p^{t+1} | f'(y) \\ 0 & \text{otherwise} \end{cases}.$$

(1.20) then follows.

Let $H_k(x) = \alpha_k x^k + \dots + \alpha_1 x$ be a polynomial with rational coefficients. If there is an integer q such that $e^{2\pi i H_k(x+q)} = e^{2\pi i H_k(x)}$ for all x, then we say that $H_k(x)$ has *period* q. The smallest positive period of $H_k(x)$ is called its *order*. Let $B_k(q)$ denote the class of polynomials with degree k and period q and $B_k^*(q)$ denote the subclass of polynomials with degree k and order q.

Lemma 1.8. [40] Put

$$M_k(q) = \max_{H(x) \in B_k^*(q)} \left| \frac{1}{q} \sum_{x=1}^{q} e^{2\pi i H_k(x)} \right|. \tag{1.21}$$

Then we have

$$M_2(q) \le q^{-1/2}, \tag{1.22}$$

and

$$M_3(q) \le q^{-0.1142}. \tag{1.23}$$

Lemma 1.9. Let p = 2 , f(x) satisfy (1.1), and $2^t \,\|\, f'(x)$. If n = 2t +1 and t = 1, then

$$|S(p^n, f(x))| \le 2^{n-1/2}. \tag{1.24}$$

Proof. By substitution $x = y + 2z$ ($y = 1, 2$; $z = 0, 1, 2, 3$) and notice that $n = 3$, $t = 1$, (1.24) follows from (1.22) immediately.

$$
\begin{aligned}
|S(p^n, f(x))| &= \sum_{y=1}^{2} e_{2^n}(f(y)) \sum_{z=0}^{3} e_2\left(z\frac{f'(y)}{2} + \frac{1}{2}z^2 f''(y)\right) \\
&\le 2(2^2 \cdot 2^{-1/2}) = 2^{3-1/2} \\
&= 2^{n-1/2}.
\end{aligned}
$$

Lemma 1.10. Let $f(x)$, t, and m be defined as before. If $t = 0$ and $k \ge 5$, then, for all odd prime $p \le k$,

$$|S(p^3, f(x))| \le m p^{(2/k)-1} p^{3(1-1/k)}.$$

Proof. Lemmas 1.7 and 1.6 give that

$$|S(p^3, f(x))| \le \sum_{j=1}^{r} |S_{\mu_j,p^3}|,$$

and

$$
|S_{\mu_j,p^3}| \begin{cases} \le p^2 & \text{if } \sigma_j \ge 3 \\ = p^{\sigma_j - 1}|S(p^{3-\sigma_j}, g_{\mu_j}(y))| & \text{if } \sigma_j < 3. \end{cases}
$$

When $m_j = 1$, it follows from Lemma 1.2 that $\sigma_j = t + 2 = 2$ and $t_j = 0$. Hence

$$|S_{\mu_j,p^3}| = p|S(p, g_{\mu_j}(y))|.$$

By (1.11),

$$g_{\mu_j}(y) \equiv p^{-2}\left(pyf'(\mu_j) + (py)^2 \frac{f''(\mu_j)}{2!} \right) \pmod p.$$

Thus, by Lemma 1.8,

$$|S_{\mu_j,p^3}| \le p^{3/2} = p^{(3/k)-(3/2)} p^{3(1-1/k)} < p^{(2/k)-1} p^{3(1-1/k)}.$$

When $m_j \ge 2$,

$$
\begin{aligned}
|S_{\mu_j,p^3}| &\le p^2 = p^{(3/k)-1} p^{3(1-1/k)} \le m_j p^{(3/k)-1} 2^{-1} p^{3(1-1/k)} \\
&\le m_j k^{1/k} 2^{-1} p^{(2/k)-1} p^{3(1-1/k)} \le m_j p^{(2/k)-1} p^{3(1-1/k)}.
\end{aligned}
$$

This completes the proof since $\sum_{j=1}^{r} m_j = m$.

Lemma 1.11. If $p = 2$ and $m_j = 2$, then we have $t_j = 1$.

Proof. If $p = 2$, then

$$f(2y + \mu_j) - f(\mu_j) = 2yf'(\mu_j) + (2y)^2\frac{f''(\mu_j)}{2!} + + (2y)^3\frac{f'''(\mu_j)}{3!} + \dots .$$

If $h \geq 4$, then $2^{h-2} \geq h$. Thus the number of factor 2s of h does not exceed h - 2. This implies that when $h \geq 4$, $2^{t+2} \mid 2^h\frac{f^{(h)}(\mu_j)}{h}$. Further, when $m_j = 2$, we obtain $2^{t+3} \mid 2f'(\mu_j)$, $2^{t+3} \parallel 2^2f''(\mu_j)$, and $2^{t+3} \mid 2^2f'''(\mu_j)$. This implies that $2 \parallel g'_{\mu_j}(y)$. Consequently, $t_j = 1$, as required.

Lemma 1.12. [11] If f(x) is defined as (1.1) and $p > k$ is a prime, then for $n \geq 1$, we have

$$|S(p^n, f(x))|\, p^{-n(1-1/k)} \leq \begin{cases} 1 & \text{if } p > (k-1)^{2k/(k-2)} \\ (k-1)p^{-(1/2)+(1/k)} & \text{if } (k-1)^2 < p \leq (k-1)^{2k/(k-2)} \\ p^{1/k} & \text{if } (k-1)^{k/(k-2)} < p \leq (k-1)^2 \\ (k-1)p^{(3/k)-1} & \text{if } k < p \leq (k-1)^{k/(k-2)} \end{cases}$$

Lemma 1.13. [38, 39] Define as usual

$$\pi(x) = \sum_{p \leq x} 1, \quad \text{and} \quad \theta(x) = \sum_{p \leq x} \log p \ .$$

Then

$$\theta(x) < 1.001102x, \qquad \text{if } x > 0; \tag{1.25}$$

$$|\theta(x) - x| < 8.6853x/\log^2 x, \qquad \text{if } x > 1; \tag{1.26}$$

$$\pi(x) < \frac{x}{\log x}\left(1 + \frac{1.5}{\log x}\right), \qquad \text{if } x > 1; \tag{1.27}$$

$$\pi(x) < 1.2551\frac{x}{\log x}, \qquad \text{if } x > 1. \tag{1.28}$$

3. FUNDAMENTAL ESTIMATIONS.

Lemma 1.14. Let $k \geq 5$ be an integer and $5 \leq p \leq k$ be a prime. Then for $n \geq 1$, we have

$$|S(p^n, f(x))| \leq \begin{cases} (k-1)p^{(2t(p)/k)-1}p^{n(1-1/k)} & \text{if } p \leq (k-1)^{k/(k+1)} \\ (k-1)p^{(3/k)-1}p^{n(1-1/k)} & \text{if } (k-1)^{k/(k+1)} < p \leq k \end{cases},$$

where $t(p) = \left[\frac{\log k}{\log p}\right] \geq 1$.

Proof. The second inequality of the lemma follows immediately from Lemma 4.3 of [31]. Here we only give a proof of the first inequality.

First case: $p \leq (k-1)^{k/(k+1)}$. Note that $t \leq t(p)$ since $p^t \leq k$. Also, if $p \leq k^{1/2}$, then $t(p) \geq 2$.

For $n < 2t(p)$, we obtain trivially that

$$\begin{aligned} |S(p^n, f(x))| &\leq p^n = p^{n/k}p^{n(1-1/k)} < p^{2t(p)/k}p^{n(1-1/k)} \\ &\leq (k-1)p^{2t(p)/k - 1}p^{n(1-1/k)}. \end{aligned}$$

For $n \geq 2t(p)$, we employ induction on n to show that

$$|S(p^n, f(x))| \leq mp^{2t(p)/k - 1}p^{n(1-1/k)}. \tag{1.29}$$

We first prove that (1.29) holds for $n = 2t(p)$. If $t = 0$, then $n \geq 2t + 2$; and if $1 \leq t < t(p)$, then $n \geq 2t + 2$. By Lemmas 1.6 and 1.7 we have

$$\begin{aligned} |S(p^n,f(x))| &\leq \sum_{j=1}^{r} |S_{\mu_j,p^n}| \leq rp^{n-1} = rp^{2t(p)/k - 1}p^{n(1-1/k)} \\ &\leq mp^{2t(p)/k - 1}p^{n(1-1/k)}. \end{aligned} \tag{1.30}$$

If $t = t(p)$, then $t \geq 2$. Set $x = y + p^{n-t-1}z$, where y and z run independantly through

$$y = 1, \ldots, p^{n-t-1};\ z = 0, \ldots, p^{t+1} - 1.$$

Thus, for $n = 2t$, with $t \geq 2$, we have

$$\begin{aligned} |S(p^n,f(x))| &= \left| \sum_{x=1}^{p^n} e_{p^n}(f(x)) \right| = \left| \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)) \right| \\ &\leq \sum_{j=1}^{r} \left| p^{t+1} \sum_{\substack{y=1 \\ y \equiv \mu_j \pmod p}}^{p^{n-t-1}} e_{p^n}(f(y)) \right| \end{aligned}$$

$$= \sum_{j=1}^{r} \Big| \sum_{\substack{y=1 \\ y \equiv \mu_j \, (\mathrm{mod}\, p)}}^{p^n} e_{p^n}(f(y)) \Big|$$

$$\le rp^{n-1} \le mp^{2t(p)/k - 1}p^{n(1-1/k)}. \tag{1.31}$$

Hence, for $n = 2t(p)$, (1.29) follows from (1.30) and (1.31).

Assume (1.29) holds for all integers in $[2t(p), n - 1]$, where $n > 2t(p)$. Define

$A_1 = \{j : n \le \sigma_j\}$,

$A_2 = \{j : 1 \le n - \sigma_j \le 2t_j \}$,

$A_3 = \{j : 2t_j + 1 \le n - \sigma_j \le 2t(p) \}$,

and

$A_4 = \{j : n - \sigma_j \ge 2t(p) + 1 \}$.

Since $\{1, 2, \ldots, r\}$ is the disjoint union of the A_is, we have

$$\sum_{i=1}^{4} \sum_{j \in A_i} m_j = m. \tag{1.32}$$

1). $j \in A_1$. Since $n > 2t(p) \ge 2t + 2$, it follows from Lemmas 1.6 and 1.5 that

$$|S_{\mu_j,p^n}| \le p^{n-1} = p^{n/k - 1}p^{n(1-1/k)} \le p^{\sigma_j/k - 1}p^{n(1-1/k)}$$
$$\le p^{(m_j + t + 1 - t_j)/k - 1}p^{n(1-1/k)}. \tag{1.33}$$

If $m_j = 1$, then

$$|S_{\mu_j,p^n}| \le p^{(t+2)/k - 1}p^{n(1-1/k)} \le p^{2t(p)/k - 1}p^{n(1-1/k)}. \tag{1.34}$$

If $m_j \ge 2$, then by Lemma 1.1 we obtain

$$|S_{\mu_j,p^n}| \le m_j p^{t/k - 1}p^{n(1-1/k)} \le m_j p^{2t(p)/k - 1}p^{n(1-1/k)}. \tag{1.35}$$

By (1.34) and (1.35), we obtain immediately

$$\sum_{j \in A_1} |S_{\mu_j,p^n}| \le \sum_{j \in A_1} m_j p^{2t(p)/k - 1}p^{n(1-1/k)}. \tag{1.36}$$

2). $j \in A_2$. In this case we must have $t_j \ge 1$. It follows from Lemmas 1.6 and 1.5 that

$$|S_{\mu_j,p^n}| \le p^{n-1} = p^{n/k - 1}p^{n(1-1/k)} \le p^{(\sigma_j + 2t_j)/k - 1}p^{n(1-1/k)}$$
$$\le p^{(m_j + t + 1 + t_j)/k - 1}p^{n(1-1/k)}. \tag{1.37}$$

If $m_j = 1$, then by Lemma 1.2, $t_j = 0$, contradicting $t_j \geq 1$. Thus, $m_j \geq 2$. In view of Lemma 1.1, we have

$$|S_{\mu_j,p^n}| \leq m_j p^{(t+t_j)/k - 1} p^{n(1-1/k)} \leq m_j p^{2t(p)/k - 1} p^{n(1-1/k)},$$

whence

$$\sum_{j\in A_2} |S_{\mu_j,p^n}| \leq \sum_{j\in A_2} m_j p^{2t(p)/k - 1} p^{n(1-1/k)}. \tag{1.38}$$

3). $j \in A_3$. We first consider the case $n - \sigma_j = 2t_j + 1$ and $t_j = 0$.

By Lemma 1.6,

$$|S_{\mu_j,p^n}| = p^{\sigma_j - 1}|S(p^{2t_j+1}, g_{\mu_j}(y))| = p^{\sigma_j - 1}|S(p, g_{\mu_j}(y))|. \tag{1.39}$$

When $m_j = 1$, by Lemma 1.2, $\sigma_j = t + 2$. It then follows from Lemmas 1.3 and 1.8 that

$$\begin{aligned} |S_{\mu_j,p^n}| &\leq p^{\sigma_j - 1 + 1/2} = p^{(n/k) - (3/2)} p^{n(1-1/k)} = p^{(\sigma_j+1)/k - (3/2)} p^{n(1-1/k)} \\ &= p^{(t+3)/k - (3/2)} p^{n(1-1/k)} < p^{2t(p)/k - 1} p^{n(1-1/k)}. \end{aligned} \tag{1.40}$$

When $m_j \geq 2$, we obtain, by Lemmas 1.6, 1.5 and 1.1,

$$\begin{aligned} |S_{\mu_j,p^n}| &\leq p^{n-1} = p^{(n/k) - 1} p^{n(1-1/k)} = p^{(\sigma_j+1)/k - 1} p^{n(1-1/k)} \\ &= p^{(m_j+t+2)/k - 1} p^{n(1-1/k)} \leq m_j p^{(t+1)/k - 1} p^{n(1-1/k)} \\ &< m_j p^{2t(p)/k - 1} p^{n(1-1/k)}. \end{aligned} \tag{1.41}$$

Assume either $2t_j + 2 \leq n - \sigma_j \leq 2t(p)$ and $t_j = 0$ or $2t_j + 1 \leq n - \sigma_j \leq 2t(p)$ and $t_j \geq 1$. It follows from Lemmas 1.6, 1.7, 1.5 and 1.4 that

$$\begin{aligned} |S_{\mu_j,p^n}| &= p^{\sigma_j - 1}|S(p^{n-\sigma_j}, g_{\mu_j}(y))| \leq p^{\sigma_j - 1} m_j p^{n - \sigma_j - 1} \\ &= m_j p^{n-2} = m_j p^{(n/k) - 2} p^{n(1-1/k)} \leq m_j p^{(\sigma_j + 2t(p))/k - 2} p^{n(1-1/k)} \\ &\leq m_j p^{2t(p)/k - 1} p^{n(1-1/k)}. \end{aligned} \tag{1.42}$$

By (1.40) - (1.42) we obtain

$$\sum_{j\in A_3} |S_{\mu_j,p^n}| \leq \sum_{j\in A_3} m_j p^{2t(p)/k - 1} p^{n(1-1/k)}. \tag{1.43}$$

3). $j \in A_4$. By Lemmas 1.6 and 1.4, we have

$$\sum_{j\in A_4} |S_{\mu_j,p^n}| = \sum_{j\in A_4} p^{\sigma_j - 1}|S(p^{n-\sigma_j}, g_{\mu_j}(y))|.$$

We show that the usage of the induction hypothesis is permitted. By (1.9), $\deg g_{\mu_j}(y) \leq k$, and if $\deg g_{\mu_j}(y) \leq k - 1$, say $\deg g_{\mu_j}(y) = t$ and $g_{\mu_j}(y) = b_t y^t + \ldots + b_1 y + b_0$ with

$(b_1, \ldots, b_t, p) = 1$, then we define $G_{\mu_j}(y) = p^{n - \sigma_j} y^k + b_t y^t + \ldots + b_1 y + b_0$. Now $\deg G_{\mu_j}(y) = k$ and $(p^{n - \sigma_j}, b_1, \ldots, b_t, p) = 1$. That is, $G_{\mu_j}(y)$ satisfies all conditions of the induction hypothesis. Furthermore, by the induction hypothesis,

$$|S(p^{n - \sigma_j}, g_{\mu_j}(y))| = |S(p^{n - \sigma_j}, G_{\mu_j}(y))|$$
$$\leq m_j\, p^{2t(p)/k - 1}\, p^{(n - \sigma_j)(1 - 1/k)}.$$

Thus, in view of the induction hypothesis, Lemmas 1.6 and 1.4, we have

$$\begin{aligned}\sum_{j \in A_4} |S_{\mu_j, p^n}| &= \sum_{j \in A_4} p^{\sigma_j - 1} |S(p^{n - \sigma_j}, g_{\mu_j}(y))| \\ &= \sum_{j \in A_4} p^{\sigma_j - 1} |S(p^{n - \sigma_j}, G_{\mu_j}(y))| \\ &\leq \sum_{j \in A_4} p^{\sigma_j - 1}\, m_j\, p^{2t(p)/k - 1}\, p^{(n - \sigma_j)(1 - 1/k)} \\ &\leq \sum_{j \in A_4} m_j\, p^{2t(p)/k - 1}\, p^{n(1 - 1/k)}. \end{aligned} \tag{1.44}$$

Therefore, (1.29) follows from (1.36), (1.38), (1.43), (1.44), and (1.32). Thus the lemma holds for $p \leq k^{1/2}$.

Suppose now $k^{1/2} < p \leq (k - 1)^{k/(k + 1)}$. Here $t(p) = 1$ and $k \geq 8$ since $p \geq 5$.

For $n \leq 2t(p) + 1$,

$$|S(p^n, f(x))| \leq p^n \leq p\, p^{3/k - 1}\, p^{n(1 - 1/k)} = p^{1 + 1/k}\, p^{2/k - 1}\, p^{n(1 - 1/k)}$$
$$\leq (k - 1)\, p^{2/k - 1}\, p^{n(1 - 1/k)}.$$

For $n \geq 4$, we apply induction to show that

$$|S(p^n, f(x))| \leq m\, p^{2/k - 1}\, p^{n(1 - 1/k)}. \tag{1.45}$$

When $n = 4 \geq 2t + 2$ (since $t \leq t(p)$), Lemma 1.7 gives that

$$|S(p^n, f(x))| \leq \sum_{j=1}^{r} |S_{\mu_j, p^n}|. \tag{1.46}$$

Case 1. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 2$ and $t_j = 0$.

Case 1a. Suppose $t = 0$. Thus $\sigma_j = 2$, and $n - \sigma_j = 2 = 2t_j + 2$. By Lemmas 1.6 and 1.7 we have

$$|S_{\mu_j, p^n}| = p\, |S(p^2, g_{\mu_j}(y))| \leq m_j\, p^2 = p^{n - 2}$$
$$\leq p^{1/k - 1}\, p^{n(1 - 1/k)}.$$

Case 1b. Suppose now $t = 1$. By Lemma 1.2 again, $\sigma_j = 3$ and $n - \sigma_j = 1$. Hence

$$|S_{\mu_j, p^n}| = p^2 |S(p, g_{\mu_j}(y))|.$$

Now (1.11) gives that

$$g_{\mu_j}(y) \equiv p^{-3} \left(pyf'(\mu_j) + (py)^2 \frac{f''(\mu_j)}{2!} \right) \pmod p.$$

By this and Lemma 1.8, we obtain

$$|S_{\mu_j, p^n}| \le p^{5/2} \le p^{1/k - 1} p^{n(1 - 1/k)}.$$

Case 2. If $m_j \ge 2$, then Lemma 1.1 gives that

$$|S_{\mu_j, p^n}| \le p^{n - 1} = p^{4/k - 1} p^{n(1 - 1/k)} \le p^{(m_j + 2)/k - 1} p^{n(1 - 1/k)}$$
$$\le m_j p^{1/k - 1} p^{n(1 - 1/k)}.$$

Assume the induction hypothesis (1.45) holds for all integers in $[4, n - 1]$, where $n \ge 5$. We consider the following cases.

1). $n \le \sigma_j$.

If $m_j = 1$, then it follows from Lemma 1.2 that $\sigma_j = t + 2 \le 3$ which contradicts $n \le \sigma_j$. Hence $m_j \ge 2$ and it follows from Lemmas 1.6, 1.5 and 1.1 that

$$|S_{\mu_j, p^n}| \le p^{\sigma_j/k - 1} p^{n(1 - 1/k)} \le p^{(m_j + t + 1)/k - 1} p^{n(1 - 1/k)}$$
$$\le m_j p^{1/k - 1} p^{n(1 - 1/k)}.$$

2). $1 \le n - \sigma_j \le 2t_j$. Since $1 \le t_j \le t(p)$ and $t(p) = 1$, we have $t_j = 1$.

If $m_j = 1$, then by Lemma 1.2, $t_j = 0$ which contradicts $t_j = 1$. Hence $m_j \ge 2$. As in Case 1,

$$|S_{\mu_j, p^n}| \le p^{n/k - 1} p^{n(1 - 1/k)} \le p^{(\sigma_j + 2t_j)/k - 1} p^{n(1 - 1/k)}$$
$$\le p^{(m_j + t + 1 + t_j)/k - 1} p^{n(1 - 1/k)}$$
$$\le m_j p^{2/k - 1} p^{n(1 - 1/k)}.$$

3). $2t_j + 1 \le n - \sigma_j \le 2t(p)$. Here we must have $t_j = 0$.

If $m_j = 1$, then it follows from Lemma 1.2 that $\sigma_j = t + 2$ and $t_j = 0$ since $t(p) = 1$.

(i). $n - \sigma_j = 1$. Thus $n = \sigma_j + 1 \le 4$, a contradiction.

(ii). $n - \sigma_j = 2 = 2t_j + 2$. Lemmas 1.7, 1.6, and 1.5 give that

$$|S_{\mu_j, p^n}| = p^{\sigma_j - 1}\, |S(p^2, g_{\mu_j}(y))| \le m_j\, p^{n-2}$$

$$\le p^{(\sigma_j + 2)/k - 2}\, p^{n(1 - 1/k)}$$

$$\le p^{2/k - 1}\, p^{n(1 - 1/k)}.$$

Suppose that $m_j \ge 2$.

(i). $n - \sigma_j = 1$. It follows from Lemmas 1.5 and 1.1 that

$$|S_{\mu_j, p^n}| \le p^{n-1} = p^{(\sigma_j + 1)/k - 1}\, p^{n(1 - 1/k)}$$

$$\le p^{(m_j + t + 2)/k - 1}\, p^{n(1 - 1/k)}$$

$$\le m_j\, p^{2/k - 1}\, p^{n(1 - 1/k)}.$$

(ii). $n - \sigma_j = 2 = 2t_j + 2$. By Lemmas 1.7 and 1.4 we obtain

$$|S_{\mu_j, p^n}| \le m_j\, p^{n-2} = m_j\, p^{(\sigma_j + 2)/k - 2}\, p^{n(1 - 1/k)}$$

$$\le m_j\, p^{2/k - 1}\, p^{n(1 - 1/k)}.$$

4). $n - \sigma_j = 2t(p) + 1 = 3$.

If $m_j = 1$, then Lemma 1.2 gives that $\sigma_j = t + 2$ and $t_j = 0$. By Lemma 1.7 we have

$$|S_{\mu_j, p^n}| \le m_j\, p^{n-2} = p^{(t + 5)/k - 2}\, p^{n(1 - 1/k)}$$

$$\le p^{-1}\, p^{n(1 - 1/k)}.$$

Consider $m_j \ge 2$. When $t_j = 0$, we obain, by Lemmas 1.6, 1.10, and 1.4,

$$|S_{\mu_j, p^n}| = p^{\sigma_j - 1}\, |S(p^3, g_{\mu_j}(y))| \le p^{\sigma_j - 1}\, m_j\, p^{2/k - 1}\, p^{3(1 - 1/k)}$$

$$\le m_j\, p^{2/k - 1}\, p^{n(1 - 1/k)}.$$

When $t_j = 1$, for $m_j \le k - 2$, we deduce from Lemmas 1.7 and 1.5 that

$$|S_{\mu_j, p^n}| \le m_j\, p^{(\sigma_j + 3)/k - 2}\, p^{n(1 - 1/k)} \le m_j\, p^{(m_j + t + 3)/k - 2}\, p^{n(1 - 1/k)}$$

$$\le m_j\, p^{(k + 2)/k - 2}\, p^{n(1 - 1/k)} = m_j\, p^{2/k - 1}\, p^{n(1 - 1/k)},$$

where we have used $t \le t(p) = 1$.

For $m_j = k - 1$, it follows from Lemmas 1.6 and 1.4 that

$$|S_{\mu_j, p^n}| \le p^{n-1} = p^{(\sigma_j + 3)/k - 1}\, p^{n(1 - 1/k)}$$

$$\le m_j\, p^{3/k}\, (k - 1)^{-1}\, p^{n(1 - 1/k)}$$

$$\le m_j\, p^{2/k - 1}\, p^{n(1 - 1/k)}. \quad (\text{recall } p^{(k+1)/k} \le k - 1)$$

5). $n - \sigma_j \ge 2t(p) + 2$. In view of the induction hypothesis we obtain easily

$$|S_{\mu_j, p^n}| = p^{\sigma_j - 1} |S(p^{n - \sigma_j}, g_{\mu_j}(y))| \le p^{\sigma_j - 1} m_j p^{2/k - 1} p^{(n - \sigma_j)(1 - 1/k)}$$
$$\le m_j p^{2/k - 1} p^{n(1 - 1/k)}.$$

Hence the lemma holds for $p \le (k - 1)^{k/(k + 1)}$.

Lemma 1.15. Let $5 \le k \le 8$, $p = 3$, and $f(x)$ be defined as in (1.1) and satisfy $(a_1, \dots, ka_k, 3) = 1$. Then for $n \ge 1$ we have

$$|S(3^n, f(x))| \le (k - 1)\, 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

Proof. Here we note that $t(3) = [\frac{\log k}{\log 3}] = 1$ and $t = 0$.

For $n \le 2t(3) = 2$, we have trivially

$$|S(3^n, f(x))| \le 3^n \le 3^{2/k} 3^{n(1 - 1/k)}$$
$$\le (k - 1)\, 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

We now employ the induction method on n, $n \ge 2t(3) + 1 = 3$, to show that

$$|S(3^n, f(x))| \le m\, 3^{2/k - 1} 3^{n(1 - 1/k)}. \qquad (1.47)$$

When $n = 3$, (1.47) follows from Lemma 1.10 immediately.

Assume (1.47) holds for all integers in $[3, n - 1]$, where $n \ge 4$. We consider the following cases:

1). $n \le \sigma_j$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 2 = 2$, contradicting the condition $n \ge 4$. Thus $m_j \ge 2$. It follows from Lemmas 1.6, 1.5, and 1.1 that

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le 3^{\sigma_j/k - 1} 3^{n(1 - 1/k)}$$
$$\le m_j 3^{-1} 3^{n(1 - 1/k)}.$$

2). $1 \le n - \sigma_j \le 2t_j$. Then $1 \le t_j \le t(3) = 1$. Thus $t_j = 1$. If $m_j = 1$, then by Lemma 1.2, we must have $t_j = 0$, a contradiction. Hence $m_j \ge 2$. In view of Lemmas 1.5 and 1.1 we obtain

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le 3^{(\sigma_j + 2t_j)/k - 1} 3^{n(1 - 1/k)} \le 3^{(m_j + 2)/k - 1} 3^{n(1 - 1/k)}$$
$$\le m_j 3^{1/k - 1} 3^{n(1 - 1/k)}.$$

3). $2t_j + 1 \le n - \sigma_j \le 2t(3)$. Since $t(3) = 1$, we have $t_j = 0$. That is, $1 \le n - \sigma_j \le 2$.

If $m_j = 1$, then by lemma 1.2, $\sigma_j = t + 2 = 2$, since $t = 0$. This implies that $n - \sigma_j = 2 = 2t_j + 2$ as $m \ge 4$. It thus follows from Lemmas 1.6, 1.7, and 1.4 that

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1} |S(3^{n - \sigma_j}, g_{\mu_j}(y))| \le m_j 3^{n - 2}$$

$$= 3^{(\sigma_j + 2)/k - 2} 3^{n(1 - 1/k)}$$

$$\le 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

If $m_j \ge 2$, then we have, by Lemmas 1.6, 1.5, and 1.1,

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le 3^{(\sigma_j + 2)/k - 1} 3^{n(1 - 1/k)} \le 3^{(m_j + 3)/k - 1} 3^{n(1 - 1/k)}$$

$$\le m_j 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

4). $n - \sigma_j \ge 2t(3) + 1$. In view of the induction hypothesis and Lemma 1.4, we have

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1} |S(3^{n - \sigma_j}, g_{\mu_j}(y))| \le 3^{\sigma_j - 1} m_j 3^{2/k - 1} 3^{(n - \sigma_j)(1 - 1/k)}$$

$$\le m_j 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

Therefore (1.47) holds, and the lemma follows from Lemma 1.7 after summing over j.

Lemma 1.16. With the same conditions as Lemma 1.15 but replacing the condition $(a_1, \dots, ka_k, 3) = 1$ by $3 \| f'(x)$, we have, for $n \ge 1$,

$$|S(3^n, f(x))| \le (k - 1) 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

Proof. Here we have $t(3) = 1$ and $t = 1$.

For $n \le 2t(3) + 1 = 3$, it is easily seen that

$$|S(3^n, f(x))| \le 3^n \le 3^{3/k} 3^{n(1 - 1/k)} \le (k - 1) 3^{3/k - 1} \frac{3}{4} 3^{n(1 - 1/k)}$$

$$\le (k - 1) 3^{2/k - 1} 3^{n(1 - 1/k)}.$$

We now apply the induction method to show that, for $n \ge 2t(3) + 2 = 4$,

$$|S(3^n, f(x))| \le m\, 3^{2/k - 1} 3^{n(1 - 1/k)}. \quad (1.48)$$

When $n = 4 = 2t + 2$, the proof is similar to that of (1.45) in Lemma 1.14. Assume now (1.48) holds for all integers in $[4, n - 1]$, where $n \ge 5$.

1). $n \le \sigma_j$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 2 = 3$, but this is impossible. Thus $m_j \ge 2$. It therefore follows from Lemmas 1.6, 1.5, and 1.1 that

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le 3^{\sigma_j/k - 1} 3^{n(1 - 1/k)} \le 3^{(m_j + 2)/k - 1} 3^{n(1 - 1/k)}$$

$$\le m_j 3^{1/k - 1} 3^{n(1 - 1/k)}.$$

2). $1 \le n - \sigma_j \le 2t_j$. Here $t_j = 1$ since $t(3) = 1$. If $m_j = 1$, then by Lemma 1.2, $t_j = 0$ which is a contradiction. Thus $m_j \ge 2$. It follows from Lemmas 1.6, 1.5 and 1.1 that

$$|S_{\mu_j, 3^n}| \le 3^{n-1} \le 3^{(\sigma_j + 2)/k - 1}\, 3^{n(1 - 1/k)} \le 3^{(m_j + t + 3 - t_j)/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le m_j 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

3). $2t_j + 1 \le n - \sigma_j \le 2t(3)$. In this case we must have $t_j = 0$, that is, $1 \le n - \sigma_j \le 2$.

If $m_j = 1$, then Lemma 1.2 gives that $\sigma_j = t + 2 = 3$ and $t_j = 0$. Hence $n - \sigma_j = 2 = 2t_j + 2$. By Lemmas 1.6, 1.7, and 1.4, we obtain

$$|S_{\mu_j, 3^n}| \le m_j\, 3^{n-2} = 3^{(\sigma_j + 2)/k - 2}\, 3^{n(1 - 1/k)}$$
$$\le 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

Suppose now $m_j \ge 2$. When $n - \sigma_j = 1$, it follows from Lemmas 1.6, 1.5, and 1.1 that

$$|S_{\mu_j, 3^n}| \le 3^{n-1} = 3^{(\sigma_j + 1)/k - 1}\, 3^{n(1 - 1/k)} \le 3^{(m_j + t + 2)/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le m_j 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

When $n - \sigma_j = 2 = 2t_j + 2$, it follows from Lemmas 1.6, 1.7, and 1.4 that

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1}\, |S(3^2, g_{\mu_j}(y))| \le m_j 3^{n-2} = m_j\, 3^{(\sigma_j + 2)/k - 2}\, 3^{n(1 - 1/k)}$$
$$\le m_j 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

4). $n - \sigma_j = 2t(3) + 1 = 3$. If $m_j = 1$, then Lemma 1.2 gives that $\sigma_j = t + 2 = 3$ and $t_j = 0$. Thus by Lemma 1.7 we have

$$|S_{\mu_j, 3^n}| \le m_j\, 3^{n-2} = 3^{(\sigma_j + 2)/k - 2}\, 3^{n(1 - 1/k)}$$
$$\le 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

Suppose $m_j \ge 2$. When $t_j = 0$, it follows from Lemmas 1.6, 1.10, and 1.4 that

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1}\, |S(3^3, g_{\mu_j}(y))| \le 3^{\sigma_j - 1} m_j\, 3^{2/k - 1}\, 3^{3(1 - 1/k)}$$
$$\le m_j 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

When $t_j = 1$, we deduce from Lemmas 1.6, 1.7, and 1.5 that, for $m_j \le 3$,

$$|S_{\mu_j, 3^n}| \le m_j\, 3^{(\sigma_j + 3)/k - 2}\, 3^{n(1 - 1/k)} \le m_j\, 3^{(m_j + 4)/k - 2}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 3^{2/k - 1}\, 3^{n(1 - 1/k)}.$$

For $m_j \ge 4$, it follows from Lemmas 1.6 and 1.4 that

$$|S_{\mu_j, 3^n}| \le 3^{n-1} = 3^{(\sigma_j + 3)/k - 1} 3^{n(1-1/k)} \le m_j 3^{3/k} 4^{-1} 3^{n(1-1/k)}$$
$$\le m_j 3^{2/k - 1} 3^{n(1-1/k)}.$$

5). $n - \sigma_j \ge 2t(3) + 2$. It easily follows from the induction hypothesis that

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1} |S(3^{n-\sigma_j}, g_{\mu_j}(y))| \le 3^{\sigma_j - 1} m_j 3^{2/k - 1} 3^{(n-\sigma_j)(1-1/k)}$$
$$\le m_j 3^{2/k - 1} 3^{n(1-1/k)}.$$

Hence (1.48) holds. This completes the proof.

Lemma 1.17. Let $9 \le k \le 26$, $p = 3$, and $f(x)$ be defined as (1.1). Then for $n \ge 1$, we have

$$|S(3^n, f(x))| \le (k-1) 3^{1/k - 1} 3^{n(1-1/k)}.$$

Proof. Here we have $t(3) = [\frac{\log k}{\log 3}] = 2$.

For $n \le 2t(3)$,

$$|S(3^n, f(x))| \le 3^n \le (k-1) 3^{4/k - 1} \frac{3}{8} 3^{n(1-1/k)}$$
$$\le (k-1) 3^{-1} 3^{n(1-1/k)}.$$

For $n \ge 2t(3) + 1 = 5$, we use the inductive method as before to show that

$$|S(3^n, f(x))| \le m\, 3^{1/k - 1} 3^{n(1-1/k)}. \tag{1.49}$$

When $n = 5 \ge 2t + 1$, Lemma 1.7 gives

$$|S(3^n, f(x))| \le \sum_{j=1}^{r} |S_{\mu_j, 3^n}|. \tag{1.50}$$

If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 2$ and $t_j = 0$.

Suppose $t \le 1$, then $\sigma_j \le 3$, and $n - \sigma_j \ge 2 = 2t_j + 2$. We obtain, by Lemmas 1.6 and 1.7,

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1} |S(3^{n-\sigma_j}, g_{\mu_j}(y))| \le m_j 3^{n-2}$$
$$= m_j 3^{5/k - 2} 3^{n(1-1/k)}$$
$$\le m_j 3^{-1} 3^{n(1-1/k)}.$$

If $t = 2$, then $\sigma_j = 4$, and $n - \sigma_j = 1$. In view of Lemma 1.3,

$$g_{\mu_j}(y) \equiv 3^{-4} \left(3yf'(\mu_j) + (3y)^2 \frac{f''(\mu_j)}{2!} + + (3y)^3 \frac{f'''(\mu_j)}{3!} \right)$$

$$\equiv \left(\frac{f'(\mu_j)}{3^3} + \frac{1}{2}\frac{f''(\mu_j)}{3^2}\right)y + \frac{1}{2}\frac{f''(\mu_j)}{3^2}y^2 \qquad \text{(mod 3)},$$

since $y^3 \equiv y$ (mod3) by Fermat's theorem. By Lemmas 1.6 and 1.8 we have

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1}|S(3, g_{\mu_j}(y))| \le 3^{3.5}$$
$$\le 3^{1/k - 1}\, 3^{n(1 - 1/k)}.$$

If $m_j \ge 2$, it then follows from Lemma 1.6 that

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le m_j \frac{1}{2} 3^{5/9}\, 3^{-1}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 3^{-1}\, 3^{n(1 - 1/k)}.$$

Assume now that (1.49) holds for all integers in [5, n - 1], where $n \ge 6 \ge 2t + 2$. We consider the following cases.

1). $n \le \sigma_j$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 2 \le 4$, which contradicts $n \le \sigma_j$. Hence $m_j \ge 2$. When $m_j = 2$, it follows from Lemmas 1.6 and 1.5 that

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le 3^{(m_j + t + 1)/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 3^{-1}\, 3^{n(1 - 1/k)}.$$

When $m_j \ge 3$, we deduce from Lemmas 1.6 and 1.4 that

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le m_j\, 3^{\sigma_j/k - 2}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 3^{-1}\, 3^{n(1 - 1/k)}.$$

2). $1 \le n - \sigma_j \le 2t_j$. Here $1 \le t_j \le t(3) = 2$.

(i). $t_j = 1$. In this case $1 \le n - \sigma_j \le 2$. If $m_j = 1$, then by Lemma 1.2, we have $t_j = 0$, contradicting $t_j = 1$. If $m_j = 2$, it follows from Lemmas 1.6 and 1.5 that

$$|S_{\mu_j, 3^n}| \le 3^{n - 1} \le 3^{(\sigma_j + 2)/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le 3^{(m_j + t + 1 - t_j + 2)/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 2^{-1}\, 3^{6/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 3^{1/k - 1}\, 3^{n(1 - 1/k)}.$$

When $m_j = 3$, applying Lemmas 1.6 and 1.5 again we get

$$|S_{\mu_j, 3^n}| \le 3^{7/k - 1}\, 3^{n(1 - 1/k)}$$
$$\le m_j\, 3^{-1}\, 3^{n(1 - 1/k)}.$$

When $m_j \geq 4$, by Lemmas 1.6 and 1.4 we obtain

$$|S_{\mu_j, 3^n}| \leq 3^{n-1} \leq 3^{2/k} 3^{n(1-1/k)}$$

$$\leq m_j 3^{-1} 3^{n(1-1/k)}.$$

(ii). $t_j = 2$. Now $1 \leq n - \sigma_j \leq 4$. Similar to the proof of (i), we must have $m_j \geq 2$. For the cases $1 \leq n - \sigma_j \leq 3$, the proof is similar to that of (i). Hence we consider the case $n - \sigma_j = 4$. It follows from Lemmas 1.6 and 1.7 that

$$|S_{\mu_j, 3^n}| \leq m_j 3^{n-2} = m_j 3^{(\sigma_j+4)/k - 2} 3^{n(1-1/k)}. \tag{1.51}$$

If $m_j \leq 4$, then we have, by (1.51) and Lemma 1.5,

$$|S_{\mu_j, 3^n}| \leq 3^{(m_j + t + 1 - t_j + 4)/k - 1} 3^{n(1-1/k)}$$

$$\leq m_j 3^{-1} 3^{n(1-1/k)}.$$

If $m_j \geq 5$, it then follows from Lemmas 1.6 and 1.4 that

$$|S_{\mu_j, 3^n}| \leq 3^{(\sigma_j + 4)/k - 1} 3^{n(1-1/k)}$$

$$\leq 3^{4/k} 3^{n(1-1/k)} \leq m_j 5^{-1} 3^{4/k} 3^{n(1-1/k)}$$

$$\leq m_j 3^{-1} 3^{n(1-1/k)}.$$

3). $2t_j + 1 \leq n - \sigma_j \leq 2t(3)$. Here we have $t_j = 0$ or 1.

(i). $t_j = 0$. Thus we have $1 \leq n - \sigma_j \leq 4$.

Consider $n - \sigma_j = 1$.

When $t = 0$, for $m_j = 1$ Lemma 1.3 gives that

$$g_{\mu_j}(y) \equiv 3^{-\sigma_j} \left(3yf'(\mu_j) + (3y)^2 \frac{2f''(\mu_j)}{2!} \right) \pmod 3.$$

Thus, in view of Lemmas 1.6, 1.5, and 1.8, we have

$$|S_{\mu_j, 3^n}| \leq 3^{(\sigma_j + 4)/k - (3/2)} 3^{n(1-1/k)}$$

$$\leq 3^{6/k - (3/2)} 3^{n(1-1/k)}$$

$$\leq 3^{-1} 3^{n(1-1/k)}.$$

If $m_j \geq 2$, then by Lemma 1.6, 1.5, and 1.1 we get

$$|S_{\mu_j, 3^n}| \leq 3^{n-1} = 3^{n/k - 1} 3^{n(1-1/k)}$$

$$= 3^{(n - \sigma_j + \sigma_j)/k - 1} 3^{n(1-1/k)}$$

$$\leq 3^{(m_j + 2)/k - 1} 3^{n(1-1/k)}$$

$$\leq m_j 3^{1/k - 1}\, 3^{n(1 - 1/k)}.$$

Suppose $t \geq 1$. If $m_j = 1$, then Lemma 1.2 gives that $\sigma_j = t + 2$. By (1.12), we have

$$g_{\mu_j}(y) \equiv 3^{-t-2}\,((\,3f'(\mu_j) + \frac{3^2}{2}f'''(\mu_j))y + \frac{3^2}{2}f''(\mu_j)\,y^2)\ (\text{mod } 3).$$

It then follows from Lemmas 1.6, 1.5, and 1.8 that

$$|S_{\mu_j, 3^n}| \leq 3^{(m_j + t + 2)/k - 3/2}\, 3^{n(1 - 1/k)}$$

$$\leq 3^{5/k - 3/2}\, 3^{n(1 - 1/k)}$$

$$\leq 3^{1/k - 1}\, 3^{n(1 - 1/k)},$$

by noting that $t \leq t(3) = 2$ and $k \geq 9$.

When $m_j = 2$, then by Lemmas 1.6 and 1.5,

$$|S_{\mu_j, 3^n}| \leq 3^{n-1} = 3^{(\sigma_j + 1)/k - 1}\, 3^{n(1 - 1/k)}$$

$$\leq 3^{(m_j + t + 2)/k - 1}\, 3^{n(1 - 1/k)}$$

$$\leq 3^{6/k - 1}\, 3^{n(1 - 1/k)}$$

$$\leq m_j 3^{1/k - 1}\, 3^{n(1 - 1/k)}.$$

When $m_j \geq 3$, then by Lemmas 1.6, 1.5, and 1.4,

$$|S_{\mu_j, 3^n}| \leq 3^{n-1} = 3^{(\sigma_j + 1)/k - 1}\, 3^{n(1 - 1/k)}$$

$$\leq 3^{1/k}\, 3^{n(1 - 1/k)}$$

$$\leq m_j 3^{1/k - 1}\, 3^{n(1 - 1/k)}.$$

If $n - \sigma_j \geq 2$, then the argument is straightforward. By Lemmas 1.6 and 1.4 we have

$$|S_{\mu_j, 3^n}| \leq 3^{n-2} = 3^{(\sigma_j + 1)/k - 2}\, 3^{n(1 - 1/k)}$$

$$\leq 3^{1/k - 1}\, 3^{n(1 - 1/k)},$$

as required.

(ii). $t_j = 1$. Thus $3 \leq n - \sigma_j \leq 4$. If $m_j = 1$, then Lemma 1.2 gives that $t_j = 0$, leading to a contradiction. Hence $m_j \geq 2$. When $m_j \leq 4$, then by Lemmas 1.6, 1.7, and 1.5 we have

$$|S_{\mu_j, 3^n}| = 3^{\sigma_j - 1}\, |S(3^{n - \sigma_j}, g_{\mu_j}(y))|$$

$$\le m_j 3^{n-2}$$

$$\le m_j 3^{1/k - 1} 3^{n(1-1/k)}.$$

And when $m_j \ge 5$, we have, by Lemmas 1.6 and 1.4,

$$|S_{\mu_j, 3^n}| \le 3^{n/k - 1} 3^{n(1-1/k)}$$

$$\le 3^{(\sigma_j + 4)/k - 1} 3^{n(1-1/k)}$$

$$\le 3^{4/k} 3^{n(1-1/k)}$$

$$\le m_j 3^{4/k - 1} (\tfrac{5}{3})^{-1} 3^{n(1-1/k)}$$

$$\le m_j 3^{1/k - 1} 3^{n(1-1/k)}.$$

4). $n - \sigma_j \ge 2t(3) + 1$. It follows from the induction hypothesis, and Lemmas 1.6 and 1.4 that

$$|S_{\mu_j, 3^n}| \le 3^{\sigma_j - 1} m_j 3^{1/k - 1} 3^{(n-\sigma_j)(1-1/k)}$$

$$\le m_j 3^{1/k - 1} 3^{n(1-1/k)}.$$

This completes the proof.

Lemma 1.18. Let k be an integer ≥ 27, $p = 3$, and $f(x)$ satisfy (1.1). Then for $n \ge 1$,

$$|S(3^n, f(x))| \le (k-1) 3^{-1} 3^{n(1-1/k)}.$$

Proof. Here $t(3) = [\frac{\log k}{\log 3}] \ge 3$.

When $n \le 2t(3) - 1$,

$$|S(3^n, f(x))| \le 3^n \le 3^{n/k} 3^{n(1-1/k)}$$

$$\le 3^{(2t(3)-1)/k} 3^{n(1-1/k)}$$

$$\le k^{2/k} 3^{-1/k} 3^{n(1-1/k)}$$

$$\le (k-1) 3^{-1} 3^{n(1-1/k)}.$$

For $n \ge 2t(3) \ge 6$, we use the induction method to show that

$$|S(3^n, f(x))| \le m 3^{-1} 3^{n(1-1/k)}. \qquad (1.52)$$

When $n = 2t(3)$, Lemma 1.7 gives that

$$|S(3^n,f(x))| \leq \sum_{j=1}^{r} |S_{\mu_j}, 3^n| .$$

If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 2$ and $t_j = 0$.

(i). $n - \sigma_j \geq 2 = 2t_j + 2$. It follows from Lemmas 1.6 and 1.7 that

$$|S_{\mu_j}, 3^n| \leq m_j 3^{n-2} = 3^{2t(3)/k - 2} 3^{n(1 - 1/k)}$$
$$\leq 3^{-1} 3^{n(1-1/k)}.$$

(ii). $n - \sigma_j = 1$. Lemma 1.3 gives that

$$g_{\mu_j}(y) \equiv (\frac{f'(\mu_j)}{3^{t+1}} + \frac{1}{2}\frac{f'''(\mu_j)}{3^t})y + \frac{1}{2}\frac{f''(\mu_j)}{3^t} y^2 \quad (\text{mod } 3).$$

It thus follows from Lemmas 1.6 and 1.8 that

$$|S_{\mu_j}, 3^n| \leq 3^{2t(3)/k - 3/2} 3^{n(1-1/k)}$$
$$\leq 3^{-1} 3^{n(1-1/k)}.$$

(iii). $n \leq \sigma_j$. If $m_j = 1$, then Lemma 1.2 gives that $\sigma_j = t + 2 \leq 2t(3) - 1 = n - 1$, which contradicts the condition. Thus $m_j \geq 2$, and so

$$|S_{\mu_j}, 3^n| \leq 3^{2t(3)/k - 1} 3^{n(1-1/k)}$$
$$\leq m_j 3^{-1} 3^{n(1-1/k)}.$$

Assume (1.52) holds for all integers in $[2t(3), n - 1]$, where $n \geq 2t(3) + 1$.

1). $n \leq \sigma_j$. If $m_j = 1$, then in a manner similar to above we get a contradiction. So $m_j \geq 2$. When $m_j = 2$, it follows from Lemma 1.5 that

$$|S_{\mu_j}, 3^n| \leq 3^{\sigma_j/k - 1} 3^{n(1-1/k)}$$
$$\leq 3^{(m_j + t + 1)/k - 1} 3^{n(1-1/k)}$$
$$= 3^{(t+3)/k - 1} 3^{n(1-1/k)}$$
$$\leq k^{1/k} 3^{3/k - 1} 3^{n(1-1/k)}$$
$$\leq m_j 3^{-1} 3^{n(1-1/k)}.$$

And when $m_j \geq 3$, by Lemmas 1.6 and 1.4,

$$|S_{\mu_j}, 3^n| \leq 3^{n-1} \leq m_j 3^{\sigma_j/k - 2} 3^{n(1-1/k)}$$
$$\leq m_j 3^{-1} 3^{n(1-1/k)}.$$

2). $1 \le n - \sigma_j \le 2t_j$. Note that here $t_j \ge 1$. If $m_j = 1$, then by Lemma 1.2, $t_j = 0$, a contradiction. Thus $m_j \ge 2$. The proof is the same as that of 2) in Lemma 1.17.

3). $2t_j + 1 \le n - \sigma_j \le 2t(3) - 1$.

(i). $m_j = 1$. By Lemma 1.2, $\sigma_j = t + 2$ and $t_j = 0$. When $n - \sigma_j = 1$, Lemma 1.3 gives that

$$g_{\mu_j}(y) \equiv 3^{-\sigma_j}(3yf'(\mu_j) + (3y)^2\frac{f''(\mu_j)}{2!}) \pmod 3, \qquad \text{for } t = 0;$$

$$g_{\mu_j}(y) \equiv (\frac{f'(\mu_j)}{3^{t+1}} + \frac{1}{2}\frac{f'''(\mu_j)}{3^t})y + \frac{1}{2}\frac{f''(\mu_j)}{3^t}y^2 \pmod 3, \qquad \text{for } t \ge 1.$$

Hence, in view of Lemmas 1.6 and 1.8,

$$\begin{aligned} |S_{\mu_j, 3^n}| &\le 3^{(t+2)/k - 3/2}\, 3^{n(1-1/k)} \\ &\le k^{2/k}\, 3^{-1/2}\, 3^{-1}\, 3^{n(1-1/k)} \\ &\le 3^{-1}\, 3^{n(1-1/k)}. \end{aligned}$$

When $n - \sigma_j \ge 2 = 2t_j + 2$, we have, by Lemmas 1.6 and 1.7,

$$\begin{aligned} |S_{\mu_j, 3^n}| &\le 3^{n/k - 2}\, 3^{n(1-1/k)} \\ &\le 3^{(\sigma_j + 2t(3) - 1)/k - 2}\, 3^{n(1-1/k)} \\ &\le k^{3/k}\, 3^{1/k}\, 3^{-2}\, 3^{n(1-1/k)} \\ &\le 3^{-1}\, 3^{n(1-1/k)}. \end{aligned}$$

(ii). $m_j \ge 2$. The proof is similar to that of 2) in Lemma 1.17.

4). $n - \sigma_j \ge 2t(3)$. In view of the induction hypothesis and Lemma 1.4,

$$\begin{aligned} |S_{\mu_j, 3^n}| &\le 3^{\sigma_j - 1}\, m_j\, 3^{1/k - 1}\, 3^{(n-\sigma_j)(1-1/k)} \\ &\le m_j\, 3^{1/k - 1}\, 3^{n(1-1/k)}. \end{aligned}$$

This completes the proof.

Lemma 1.19. Let $5 \le k \le 7$, $p = 2$, and $f(x)$ be defined as (1.1). Then for $n \ge 1$,

$$|S(2^n, f(x))| \le (k-1)\, 2^{d(k)/k - 1}\, 2^{n(1-1/k)},$$

where

$$d(k) = \begin{cases} 2.5 & \text{if } k = 5; \\ 2 & \text{if } k = 6; \\ 1.5 & \text{if } k = 7. \end{cases}$$

Proof. Note here $t(2) = 2$. For $n \le 2t(2)$, we have trivially

$$|S(2^n, f(x))| \le 2^n \le 2^{4/k} 2^{n(1 - 1/k)}$$
$$\le (k - 1) 2^{-1} 2^{n(1 - 1/k)}.$$

When $n \ge 2t(2) + 1 = 5$, we employ the induction method to prove that

$$|S(2^n, f(x))| \le m\, 2^{d(k)/k - 1} 2^{n(1 - 1/k)}. \tag{1.53}$$

When $n = 5$, if $t = 2$, then $n = 2t + 1$, and if $t \le 1$, then $n \ge 2t + 2$. Therefore, by Lemma 1.7,

$$|S(2^n, f(x))| \le \sum_{j=1}^{r} |S_{\mu_j, 2^n}| . \tag{1.54}$$

(i). $m_j = 1$. It follows from Lemma 1.2 that $\sigma_j = t + 1$ and $t_j = 1$.

If $t \le 1$, then $n - \sigma_j = 5 - (t + 1) \ge 3 = 2t_j + 1$. We obtain, by Lemma 1.9,

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1} |S(2^{5 - \sigma_j}, g_{\mu_j}(y))| \le 2^{3.5}$$
$$\le 2^{d(k)/k - 1} 2^{n(1 - 1/k)}.$$

If $t = 2$, then $n - \sigma_j = 2$, and so

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1} |S(2^2, g_{\mu_j}(y))|.$$

Since

$$g_{\mu_j}(y) \equiv 2^{-3}(2yf'(\mu_j) + (2y)^2 \frac{f''(\mu_j)}{2!}) \pmod{2^2},$$

we deduce from Lemma 1.8 that

$$|S_{\mu_j, 2^n}| \le 2^{3.5} \le 2^{d(k)/k - 1} 2^{n(1 - 1/k)}.$$

(ii). $m_j \ge 2$. We have as usual

$$|S_{\mu_j, 2^n}| \le 2^4 \le m_j 2^{5/k - 2} 2^{n(1 - 1/k)}$$
$$\le m_j 2^{-1} 2^{n(1 - 1/k)}.$$

Suppose now that the hypothesis holds for all integers in $[2t(2) + 1, n - 1]$, where $n \ge 2t(2) + 2 = 6$. We consider the following cases.

1). $n \le \sigma_j$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 1 \le 3$, but it is impossible. Hence $m_j \ge 2$. It follows Lemmas 1.6 and 1.4 that

$$|S_{\mu_j, 2^n}| \le 2^{n-1} \le 2^{\sigma_j/k - 1} 2^{n(1-1/k)} \le 2^{n(1-1/k)}$$

$$\le m_j 2^{-1} 2^{n(1-1/k)}.$$

2). $1 \le n - \sigma_j \le 2t_j$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 1$ and $t_j = 1$. Thus $\sigma_j \le 3$ and $n - \sigma_j \ge 3$, which contradicts $n - \sigma_j \le 2t_j = 2$. Hence $m_j \ge 2$. When $m_j = 2$, Lemma 1.5 gives

$$|S_{\mu_j, 2^n}| \le 2^{(m_j + t + 1 + t_j)/k - 1} 2^{n(1-1/k)}$$

$$\le m_j 2^{d(k)/k - 1} 2^{n(1-1/k)}.$$

When $m_j = 3$, Lemma 1.5 gives as well

$$|S_{\mu_j, 2^n}| \le 2^{8/k - 1} 2^{n(1-1/k)} \le m_j 2^{3/k - 1} (\tfrac{2}{3}) 2^{n(1-1/k)}$$

$$\le m_j 2^{1/k - 1} 2^{n(1-1/k)}.$$

For $m_j \ge 4$, we obtain, by Lemma 1.4,

$$|S_{\mu_j, 2^n}| \le 2^{4/k} 2^{n(1-1/k)} \le m_j 2^{4/k - 2} 2^{n(1-1/k)}$$

$$\le m_j 2^{-1} 2^{n(1-1/k)}.$$

3). $2t_j + 1 \le n - \sigma_j \le 2t(2)$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 1$ and $t_j = 1$. Thus $3 \le n - \sigma_j \le 4$.

(i). $n - \sigma_j = 3$. We make the substitution $y = x + 2z$ in the sum $S(2^3, g_{\mu_j}(y))$, where x and z run independently through the values $x = 1, 2$; $z = 0, \dots, 3$. Then

$$|S(2^3, g_{\mu_j}(y))| = \left| \sum_{y=1}^{2} e_{2^3}(g_{\mu_j}(y)) \sum_{z=0}^{3} e_2\left(\frac{g'_{\mu_j}(y)}{2} z + \frac{1}{2} g''_{\mu_j}(y) z^2\right) \right|.$$

In view of the definition of $g_{\mu_j}(y)$ we have

$$\frac{g'_{\mu_j}(y)}{2} + \frac{g''_{\mu_j}(y)}{2} \equiv \frac{f'(\mu_j)}{2^{t+1}} + \frac{f''(\mu_j)}{2^t} y + \frac{f''(\mu_j)}{2^t} \pmod 2. \tag{1.55}$$

Since $2^{t+1} \nmid f''(\mu_j)$, the linear congruence

$$\frac{f''(\mu_j)}{2^t} y + \frac{f'(\mu_j)}{2^{t+1}} + \frac{f''(\mu_j)}{2^t} \equiv 0 \qquad \pmod 2$$

has only one solution. Hence

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1} |S(2^2, g_{\mu_j}(y))| \le 2^{n-2}$$

$\le 2^{1/k - 1}\, 2^{n(1 - 1/k)}.$

(ii). $n - \sigma_j = 4 = 2t_j + 2$. It easily follows from Lemmas 1.7 and 1.6 that

$$|S_{\mu_j, 2^n}| \le 2^{n-2} \le 2^{7/k - 2}\, 2^{n(1 - 1/k)}$$
$$\le 2^{d(k)/k - 1}\, 2^{n(1 - 1/k)}.$$

Suppose now $m_j \ge 2$.

(A). $t_j = 0$. Thus $1 \le n - \sigma_j \le 4$. When $m_j = 2$, we have $t_j = 1$ by Lemma 1.11. Thus $m_j \ge 3$. Lemma 1.4 gives that

$$|S_{\mu_j, 2^n}| \le 2^{n-1} \le 2^{(\sigma_j + 4)/k - 1}\, 2^{n(1 - 1/k)}$$
$$\le m_j\, 2^{4/k - 1} (\tfrac{2}{3})\, 2^{n(1 - 1/k)}$$
$$\le m_j\, 2^{d(k)/k - 1}\, 2^{n(1 - 1/k)}.$$

(B). $t_j = 0$. Here we have $3 \le n - \sigma_j \le 4$.

(i). $n - \sigma_j = 3$. It follows from Lemmas 1.9 and 1.4 that

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1}\, |S(2^{n - \sigma_j}, g_{\mu_j}(y))| \le 2^{n - 3/2}$$
$$= 2^{(\sigma_j + 3)/k - 3/2}\, 2^{n(1 - 1/k)}$$
$$\le 2^{3/k - 1/2}\, 2^{n(1 - 1/k)}$$
$$\le m_j\, 2^{1/k - 1}\, 2^{n(1 - 1/k)}.$$

(ii). $n - \sigma_j = 4$. When $m_j = 2$, Lemma 1.11 gives that $t_j = 1$. By substitution $y = x + 2^2 z$, where $x = 1, ..., 4$, $z = 0, ..., 3$, we have

$$|S(2^4, g_{\mu_j}(y))| = \left| \sum_{x=1}^{4} e_{2^4}(g_{\mu_j}(x)) \sum_{z=0}^{3} e_2\!\left(\frac{g'_{\mu_j}(x)}{2} z\right) \right|.$$

By

$$\frac{g'_{\mu_j}(x)}{2} \equiv 2^{-t-2}\,(f'(\mu_j) + 2f''(\mu_j)x + 2f'''(\mu_j)x^2) \qquad (\mathrm{mod}\ 2),$$

and $2^{t+2} \,\|\, f'(\mu_j)$, $2^{t+2} \mid 2f''(\mu_j)$, and $2^{t+2} \mid 2f'''(\mu_j)$, we know that the number of solutions of the congruence

$$\frac{g'_{\mu_j}(x)}{2} z \equiv 0 \pmod 2, \quad 1 \le z \le 2$$

does not exceed one. Therefore, by Lemma 1.4,

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1}\, |S(2^4, g_{\mu_j}(y))| \le 2^{n-2}$$

$$= 2^{(\sigma_j + 4)/k - 2}\, 2^{n(1 - 1/k)}$$
$$\le m_j\, 2^{-1}\, 2^{n(1 - 1/k)}.$$

Proof for the case $m_j \ge 3$ is similar to that of (A).

4). $n \ge 2t(2) + 1$. By the induction hypothesis and Lemma 1.4 we obtain

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1}\, |S(2^{n - \sigma_j}, g_{\mu_j}(y))|$$
$$\le 2^{\sigma_j - 1}\, m_j\, 2^{d(k)/k - 1}\, 2^{(n - \sigma_j)(1 - 1/k)}$$
$$\le m_j\, 2^{d(k)/k - 1}\, 2^{n(1 - 1/k)}.$$

The lemma now follows.

Lemma 1.20. Let $8 \le k \le 15$, $p = 2$, and $f(x)$ be defined as (1.1). Then for $n \ge 1$,

$$|S(2^n, f(x))| \le (k - 1)\, 2^{3/k - 1}\, 2^{n(1 - 1/k)}.$$

Proof. Note here $t(2) = 3$. For $n \le 2t(2)$,

$$|S(2^n, f(x))| \le 2^n \le 2^{6/k}\, 2^{n(1 - 1/k)}$$
$$\le (k - 1)\, 2^{-1}\, 2^{n(1 - 1/k)}.$$

For $n \ge 2t(2) + 1$, we will prove, again by the induction method,

$$|S(2^n, f(x))| \le m\, 2^{3/k - 1}\, 2^{n(1 - 1/k)}. \tag{1.56}$$

When $n = 2t(2) + 1 = 7$, if $t = 3$, then $n = 2t + 1$, and if $t \le 2$, then $n \ge 2t + 2$. Hence we have, by Lemma 1.7,

$$|S(2^n, f(x))| \le \sum_{j=1}^{r} |S_{\mu_j, 2^n}|. \tag{1.57}$$

(i). $m_j = 1$. By Lemma 1.2, we have $\sigma_j = t + 1$ and $t_j = 1$. Since $\sigma_j \le 4$, $n - \sigma_j \ge 3$. It therefore follows from Lemmas 1.7 and 1.9 that

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1}\, |S(2^{n - \sigma_j}, g_{\mu_j}(y))| \le 2^{n - 3/2}$$
$$\le 2^{3/k - 1}\, 2^{n(1 - 1/k)}.$$

(ii). $m_j \ge 2$. it is easily seen that

$$|S_{\mu_j, 2^n}| \le 2^{n - 1} \le m_j\, 2^{7/k - 2}\, 2^{n(1 - 1/k)}$$

$$\leq m_j 2^{-1} 2^{n(1-1/k)}.$$

Assume now (1.56) holds for all integers in $[2t(2)+1, n-1]$, where $n \geq 2t(2)+2 = 8$. We consider the following cases as before.

1). $n \leq \sigma_j$. If $m_j = 1$, then Lemma 1.2 gives that $\sigma_j = t+1 \leq 4$, contradicting $n \geq 8$. Thus $m_j \geq 2$. By Lemma 1.4,

$$|S_{\mu_j, 2^n}| \leq 2^{\sigma_j/k - 1} 2^{n(1-1/k)}$$
$$\leq m_j 2^{-1} 2^{n(1-1/k)}.$$

2). $1 \leq n - \sigma_j \leq 2t_j$. If $m_j = 1$, again Lemma 1.2 implies that $n \leq 6$, which contradicts $n \geq 8$. If $m_j \geq 2$, the proof is similar to that of 2) in Lemma 1.19.

3). $2t_j + 1 \leq n - \sigma_j \leq 2t(2)$. Here we must have $t_j \leq 2$.

If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t+1$ and $t_j = 1$. Thus $3 \leq n - \sigma_j \leq 6$. When $n - \sigma_j = 3$, it follows from Lemma 1.9 that

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1} |S(2^3, g_{\mu_j}(y))| \leq 2^{(t+4)/k - 3/2} 2^{n(1-1/k)}$$
$$\leq 2^{3/k - 1} 2^{n(1-1/k)}.$$

And when $2t_j + 2 = 4 \leq n - \sigma_j \leq 6$, we have, by Lemma 1.7,

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1} |S(2^3, g_{\mu_j}(y))| \leq 2^{n-2}$$
$$\leq 2^{2/k - 1} 2^{n(1-1/k)}.$$

When $m_j = 2$, by using a method similar to that of (B)(ii) in Lemma 1.19, we obtain

$$|S_{\mu_j, 2^n}| \leq 2^{n-2} = 2^{(\sigma_j + 4)/k - 2} 2^{n(1-1/k)}$$
$$\leq m_j 2^{-1} 2^{n(1-1/k)}.$$

If $m_j \geq 3$, then by Lemma 1.4,

$$|S_{\mu_j, 2^n}| \leq 2^{n-1} \leq m_j 2^{(\sigma_j + 6)/k - 2} \left(\frac{2}{3}\right) 2^{n(1-1/k)}$$
$$\leq m_j 2^{2/k - 1} 2^{n(1-1/k)}.$$

4). $n - \sigma_j \geq 2t(2) + 1$. By the induction hypothesis and Lemma 1.4 we have

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1} |S(2^{n-\sigma_j}, g_{\mu_j}(y))| \leq 2^{\sigma_j - 1} m_j 2^{3/k - 1} 2^{(n-\sigma_j)(1-1/k)}$$
$$\leq m_j 2^{3/k - 1} 2^{n(1-1/k)}.$$

This completes the proof.

Lemma 1.21. Let $k \geq 16$, $p = 2$, and $f(x)$ be defined as in (1.1). Then for $n \geq 1$,

$$|S(2^n, f(x))| \leq (k-1)\, 2^{-1}\, 2^{n(1-1/k)}.$$

Proof. Here we have $t(2) = [\frac{\log k}{\log 2}] \geq 4$. When $n \leq 2t(2)$,

$$|S(2^n, f(x))| \leq 2^n \leq 2^{2t(2)/k}\, 2^{n(1-1/k)}$$
$$\leq (k-1)\, 2^{-1}\, 2^{n(1-1/k)}.$$

For $n \geq 2t(2) + 1$, we apply the induction method to show that

$$|S(2^n, f(x))| \leq m\, 2^{-1}\, 2^{n(1-1/k)}. \qquad (1.58)$$

When $n = 2t(2) + 1$, if $t \leq 3$, then $n \geq 2t + 2$, and if $t \geq 4$, then $n \geq 2t + 1$. Thus we have, by Lemma 1.7,

$$|S(2^n, f(x))| \leq \sum_{j=1}^{r} |S_{\mu_j, 2^n}|. \qquad (1.59)$$

(A). $m_j = 1$. Lemma 1.2 gives that $\sigma_j = t + 1$ and $t_j = 1$. Since $t(2) \geq t$ and $t(2) \geq 4$, we have $n - \sigma_j = 2t(2) - t \geq t(2) \geq 4 = 2t + 2$. It then follows from Lemma 1.7 that

$$|S_{\mu_j, 2^n}| = 2^{\sigma_j - 1}\, |S(2^{n-\sigma_j}, g_{\mu_j}(y))| \leq 2^{n-2}$$
$$\leq 2^{-1}\, 2^{n(1-1/k)}.$$

(B). $m_j \geq 2$. We trivially have

$$|S_{\mu_j, 2^n}| \leq 2^{n-1} = 2^{(2t(2)+1)/k - 1}\, 2^{n(1-1/k)}$$
$$\leq m_j\, 2^{-1}\, 2^{n(1-1/k)}.$$

Assume now the induction hypothesis holds for all integers in $[2t(2) + 1, n - 1]$, where $n \geq 2t(2) + 2 \geq 10$. We consider the following cases as before.

1). $n \leq \sigma_j$. If $m_j = 1$, then by Lemma 1.2, $\sigma_j = t + 1$ and $t_j = 1$. But $n \geq 2t(2) + 2 > t + 1 = \sigma_j$, a contradiction.Thus $m_j \geq 2$. By Lemma 1.4,

$$|S_{\mu_j, 2^n}| \leq 2^{n-1} \leq m_j\, 2^{-1}\, 2^{n(1-1/k)}.$$

2). $1 \leq n - \sigma_j \leq 2t_j$. If $m_j = 1$, then by Lemma 1.2, $t_j = 1$ and $\sigma_j = t + 1$. Thus $1 \leq n - \sigma_j \leq 2$. But $n - \sigma_j \geq 2t(2) + 2 - t - 1 \geq t(2) + 1 \geq 5$, leading to a contradiction. Hence $m_j \geq 2$. When $2 \leq m_j \leq 3$, it follows from Lemma 1.5 that

$$
\begin{aligned}
|S_{\mu_j, 2^n}| &\le 2^{n-1} \le 2^{(m_j + t + 1 + t_j)/k - 1}\, 2^{n(1 - 1/k)} \\
&\le 2^{(2t(2) + 4)/k - 1}\, 2^{n(1 - 1/k)} \\
&\le 2^{n(1 - 1/k)} \\
&\le m_j\, 2^{-1}\, 2^{n(1 - 1/k)}.
\end{aligned}
$$

For $m_j \ge 4$, we have, by Lemma 1.4,

$$
\begin{aligned}
|S_{\mu_j, 2^n}| &\le 2^{(\sigma_j + 2t_j)/k - 1}\, 2^{n(1 - 1/k)} \\
&\le m_j\, 2^{2t_j/k - 2}\, 2^{n(1 - 1/k)} \\
&\le m_j\, 2^{-1}\, 2^{n(1 - 1/k)}.
\end{aligned}
$$

3). $2t_j + 1 \le n - \sigma_j \le 2t(2)$. If $m_j = 1$, then again by Lemma 1.2, $3 \le n - \sigma_j \le 2t(2)$. When $n - \sigma_j = 3$, Lemma 1.9 gives that

$$
\begin{aligned}
|S_{\mu_j, 2^n}| &= 2^{\sigma_j - 1}\, |S(2^3, g_{\mu_j}(y))| \le 2^{n - 3/2} \\
&\le 2^{-1}\, 2^{n(1 - 1/k)}.
\end{aligned}
$$

When $2t_j + 2 = 4 \le n - \sigma_j \le 2t(2)$, it follows easily from Lemma 1.7 that

$$
\begin{aligned}
|S_{\mu_j, 2^n}| &= 2^{\sigma_j - 1}\, |S(2^{n - \sigma_j}, g_{\mu_j}(y))| \le 2^{n - 2} \\
&\le 2^{-1}\, 2^{n(1 - 1/k)}.
\end{aligned}
$$

The proof for the case $m_j \ge 2$ is similar to that of 2).

4). $n - \sigma_j \ge 2t(2) + 1$. By the induction hypothesis and Lemma 1.4, we get immediately

$$
\begin{aligned}
|S_{\mu_j, 2^n}| &= 2^{\sigma_j - 1}\, |S(2^{n - \sigma_j}, g_{\mu_j}(y))| \\
&\le 2^{\sigma_j - 1}\, m_j\, 2^{-1}\, 2^{(n - \sigma_j)(1 - 1/k)} \\
&\le m_j\, 2^{-1}\, 2^{n(1 - 1/k)},
\end{aligned}
$$

as required.

4. PROOF OF THE THEOREM.

Nechaev and Topunov[36] proved that

$$
|S(q, f(x))| \le e^{c(k)}\, q^{1 - 1/k},
$$

where

$$c(3) \le 2.835 = 3 \times 0.945,$$

and

$$c(4) \le 3.34 \le 4 \times 0.84.$$

Hence we only consider $k \ge 5$. In view of Lemmas 1.12, 1.14 - 1.21, and [26], we have

$$|S(q, f(x))| \le \prod_{p \le (k-1)^{k/(k+1)}} (k-1) B_p(k) p^{-1} \prod_{(k-1)^{k/(k+1)} < p \le k} (k-1) p^{3/k-1} \cdot$$

$$\cdot \prod_{k < p \le (k-1)^{k/(k-2)}} (k-1) p^{3/k-1} \prod_{(k-1)^{k/(k-2)} < p \le (k-1)^2} p^{1/k} \cdot$$

$$\cdot \prod_{(k-1)^2 < p \le (k-1)^{2k/(k-2)}} (k-1) p^{-1/2+1/k} q^{1-1/k}$$

$$= e^{F(k)} q^{1-1/k} \qquad (1.60)$$

say, where

$$B_p(k) = \begin{cases} p^{2t(p)/k} & \text{if } 5 \le p \le (k-1)^{k/(k+1)} \\ 3^{2/k} & \text{if } p = 3 \text{ and } 5 \le k \le 8 \\ 3^{1/k} & \text{if } p = 3 \text{ and } 9 \le k \le 26 \\ 1 & \text{if } p = 3 \text{ and } k \ge 27 \\ 2^{d(k)/k} & \text{if } p = 2 \text{ and } 5 \le k \le 7 \\ 2^{3/k} & \text{if } p = 2 \text{ and } 8 \le k \le 15 \\ 1 & \text{if } p = 2 \text{ and } k \ge 16 \end{cases},$$

and in each product, $p|q$.

Let $x_k = (k-1)^{k/(k-2)}$ and $y_k = (k-1)^{k/(k+1)}$. Then

$$F(k) = \log(k-1)\,\pi(x_k) - \theta(x_k) + \sum_{p \le y_k} \log B_p(k) + \frac{3}{k}(\theta(x_k) - \theta(y_k))$$

$$+ \frac{1}{k}(\theta((k-1)^2) - \theta(x_k)) + \log(k-1)\,(\pi(x_k^2) - \pi((k-1)^2))$$

$$- (\frac{1}{2} - \frac{1}{k})(\theta(x_k^2) - \theta((k-1)^2)). \qquad (1.61)$$

When $5 \le k \le 30$, by direct computation for (1.61), we can obtain $F(k) \le 1.74k$.

Suppose now $k \ge 31$. Since (cf. T. M. Apostol: Introduction to Analytic Number Theory, Theorem 4.3)

$$\pi(x)\log x - \theta(x) = \log x \int_2^x \frac{\theta(t)}{t\log^2 t}\,dt\,, \tag{1.62}$$

we can write (1.61) as

$$\begin{aligned}\frac{F(k)}{k} &= \frac{\log(k-1)}{k}\int_2^{x_k}\frac{\theta(t)}{t\log^2 t}\,dt + \frac{\log(k-1)}{k}\int_{(k-1)^2}^{x_k^2}\frac{\theta(t)}{t\log^2 t}\,dt \\ &\quad + \frac{1}{k^2}(2\pi(y_k)\log k - 3\theta(y_k) - 4\log k) \\ &= I_1(k) + I_2(k) + I_3(k), \text{ say.}\end{aligned} \tag{1.62}$$

For $k \ge 1000$, it follows from (1.26) and (1.27) that $I_3(k) \le 0$. When $31 \le k \le 1000$, it is easily seen that $I_3(k) \le 0$, as $\pi(x)\log x - \theta(x)$ is increasing.

When $31 \le k \le 40$, by (1.25),

$$\begin{aligned} I_2(k) &\le (1.001102)\frac{\log(k-1)}{k}\int_{(k-1)^2}^{x_k^2}\frac{dt}{\log^2 t} \\ &\le (1.001102)\frac{\log(k-1)}{k}\sum_{i=0}^{3}\frac{(k-1)^{2+i/(k-2)}}{(2+i/(k-2))^2\log^2(k-1)}((k-1)^{i/(k-2)} - 1).\end{aligned}$$

Since $\dfrac{(k-1)^{2+i/(k-2)}}{k(k-2)(2+i/(k-2))^2}$ and $(k-1)^{i/(k-2)}$ are decreasing for $k \ge 9$ and $0 \le i \le 3$, we have, for $k \ge 31$,

$$I_2(k) \le 1.2109. \tag{1.63}$$

When $31 \le k \le 40$,

$$\begin{aligned} I_1(k) &= \frac{k-2}{k^2}(\pi(x_k)\log x_k - \theta(x_k)) \\ &\le \frac{29}{31^2}(\pi(48)\log 48 - \theta(48)) \\ &\le 0.5164.\end{aligned}$$

Therefore, when $31 \le k \le 40$, the theorem follows from (1.61) - (1.63) and $I_3(k) \le 0$.

For $k \geq 41$, in a same manner as the proof of (1.62), we obtain

$$I_2(k) \leq 1.1693. \tag{1.67}$$

When $41 \leq k \leq 60$,

$$I_1(k) \leq \frac{39}{41^2}(\pi(68)\log 68 - \theta(68)) \leq 0.5302, \tag{1.68}$$

when $61 \leq k \leq 100$,

$$I_1(k) \leq \frac{59}{61^2}(\pi(108.8)\log 108.8 - \theta(108.8)) \leq 0.5338, \tag{1.69}$$

and for $k \geq 101$,

$$I_1(k) \leq (1.001102)\frac{\log(k-1)}{k}\Big(\int_{(k-1)^{1+1/(k-2)}}^{(k-1)^{k/(k-2)}} + \int_{(k-1)}^{(k-1)^{1+1/(k-2)}} + \sum_{i=0}^{5}\int_{(k-1)^{0.5+i/12}}^{(k-1)^{0.5+(i+1)/12}} + \int_{(k-1)^{2/5}}^{(k-1)^{1/2}} + \int_{2}^{(k-1)^{2/5}}\Big)\frac{dt}{\log^2 t}$$

$$\leq 0.5680. \tag{1.70}$$

Hence, when $k \geq 41$, the theorem follows from (1.67) - (1.70) and $I_3(k) \leq 0$. This completes the proof.

§1.2. An improvement to Chalk's estimation of exponential sums.

1. INTRODUCTION.

Let q, p, k, f(x), and S(q, f(x)) be defined as in the previous section. Define t satisfying $p^t \| (ka_k, \ldots, 2a_2, a_1)$, where the symbol $\|$ means that t is the highest power of p such that $p^t \mid (ka_k, \ldots, 2a_2, a_1)$. Let $\mu_1, \ldots, \mu_r$ be the different zeros modulo p of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod p, \qquad 0 \le x < p, \tag{1.71}$$

and let $m_1, \ldots, m_r$ be their multiplicities. Set $\max_{1\le i\le r} m_i = M = M(f)$ and

$$\sum_{i=1}^{r} m_i = m = m(f). \tag{1.72}$$

Some results for S(q , f(x)) have been obtained. Interested readers may refer to Hua [26], Lonxton and Vaughan [29], or Ding and Qi [14].

Chalk [8] obtained an upper bound for $S(p^n, f(x))$ in terms of M.

Theorem A. (Chalk[8]) Suppose $n \ge 2$. If $r > 0$, then

$$| S(p^n, f(x)) | \le mkp^{t/(M+1)} p^{n[1 - 1/(M+1)]} \tag{1.73}$$

and if $r = 0$, then

$$S(p^n, f(x)) = 0 \qquad \text{for all } n \ge 2(t+1)$$

and otherwise $| S(p^n, f(x)) | \le p^{2t+1}$, where $p^t \le k$.

The case $r = 0$ is trivial, and so we assume $r > 0$ which implies $M \ge 1$. Ding [15] improved Chalk's result for the factor k.

Theorem B. (Ding [15]) For $r > 0$ we have

$$| S(p^n, f(x)) | \le mk^{1/2} p^{t/(M+1)} p^{n[1 - 1/(M+1)]} . \tag{1.74}$$

Let

$$\tau = [\frac{\log k}{\log p}]. \tag{1.75}$$

Clearly,

$$t \le \tau . \tag{1.76}$$

Our purpose here is to improve Theorem B further for the factor k.

Theorem 1.2. Suppose that $n \ge 2$ or $n = 1$ and $p \le k$. Then for $r > 0$ we have

$$| S(p^n, f(x)) | \le mp^{\tau/(M+1)}\, p^{t/(M+1)}\, p^{n[1 - 1/(M+1)]} . \tag{1.77}$$

By (1.75), $p^{\tau} \le k$, and note that $M \ge 1$. Thus, (1.77) is better than (1.74). Actually, this result is the best possible as shown by an example at the end of this section.

2. FUNDAMENTAL LEMMAS.

Let σ_j satisfy $p^{\sigma_j} \| f(\mu_j + px) - f(\mu_j)$ and let

$$g_j (y) = p^{-\sigma_j} (f(\mu_j + px) - f(\mu_j)).$$

Define t_j satisfying $p^{t_j} \| g_j'(y)$.

Lemma 1.22 ([26]). With the above terminology, we have

$$\sigma_j \le m_j + t + 1 - t_j .$$

Lemma 1.23 (A. Weil [46]).

$$|S(p , f(x))| \le (k - 1)p^{1/2}.$$

3. PROOF OF THEOREM 1.2.

Let $t' = \max_{1\le i\le r} t_j$ and $\delta = \max (t' , t)$. Then

$$\delta \le \tau. \tag{1.78}$$

We employ induction on n to show that

$$|S(p^n, f(x))| \le mp^{\tau/(M+1)} p^{t/(M+1)} p^{n[1 - 1/(M+1)]}. \tag{1.79}$$

1) $n \le 2t$. We have trivially

$$\begin{aligned} |S(p^n, f(x))| &\le p^n = p^{n/(M+1)} p^{n[1 - 1/(M+1)]} \\ &\le p^{2t/(M+1)} p^{n[1 - 1/(M+1)]} \\ &\le p^{\tau/(M+1)} p^{t/(M+1)} p^{n[1 - 1/(M+1)]}. \end{aligned}$$

2) $n = 2t + 1$. Let $x = y + p^{n-t-1}z$, where $y = 1, \dots, p^{n-t-1}$, $z = 0, \dots, p^{t+1} - 1$. If $n \ge 2$, then we have $t \ge 1$. This implies that for $m \ge 3$,

$$m(n - t - 1) = mt \ge 2t + 1 = n.$$

Thus

$$S(p^n, f(x)) = \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_p\left(\frac{f'(y)}{p^t} z + \frac{1}{2} f''(y) z^2\right).$$

By Lemma 1.23,

$$\begin{aligned} |S(p^n, f(x))| &\le p^t \sum_{y=1}^{p^{n-t-1}} \left| \sum_{z=0}^{p-1} e_p\left(\frac{f'(y)}{p^t} z + \frac{1}{2} f''(y) z^2\right)\right| \\ &\le p^{t+1/2} p^{n-t-1} \\ &= p^{n-1/2} \\ &= p^{n/(M+1) - 1/2} p^{n[1 - 1/(M+1)]} \\ &= p^{(2t+1)/(M+1) - 1/2} p^{n[1 - 1/(M+1)]} \\ &\le p^{\tau/(M+1)} p^{t/(M+1)} p^{n[1 - 1/(M+1)]}. \end{aligned}$$

Suppose now $n = 1$ and $p \le k$. Then $\tau \ge 1$. Therefore,

$$\begin{aligned} |S(p^n, f(x))| &\le p = p^{1/(M+1)} p^{1 - 1/(M+1)} \\ &\le p^{\tau/(M+1)} p^{1 - 1/(M+1)}, \end{aligned}$$

as required.

3) $n \ge 2t + 2$. By substituting $x = y + p^{n-t-1}z$, $y = 1, \dots, p^{n-t-1}$, $z = 0, \dots, p^{t+1} - 1$, we have

$$|S(p^n, f(x))| = \left| \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)) \right|$$

$$\leq \sum_{j=1}^{r} \Big| \sum_{\substack{y=1 \\ y \equiv \mu_j \pmod p}}^{p^n} e_{p^n}(f(y)) \Big|$$

$$= \sum_{j=1}^{r} | S_j |, \qquad \text{say.} \tag{1.80}$$

Define sets A_i (i = 1, 2, 3, 4, 5) by

$$A_1 = \{j:\ n \leq \sigma_j \},$$

$$A_2 = \{j:\ 1 \leq n - \sigma_j \leq 2t_j \},$$

$$A_3 = \{j:\ n - \sigma_j = 2t_j + 1 \},$$

$$A_4 = \{j:\ 2t_j + 2 \leq n - \sigma_j \leq t_j + \tau\},$$

and

$$A_5 = \{j:\ n - \sigma_j > t_j + \tau\}.$$

Clearly,

$$\sum_{i=1}^{5} \sum_{j \in A_i} m_j = m . \tag{1.81}$$

We consider the following cases.

(i) $j \in A_1$. We have , by Lemma 1.22,

$$\begin{aligned} | S_j | &\leq p^{n-1} = p^{n/(M+1) - 1}\, p^{n[1 - 1/(M+1)]} \\ &\leq p^{\sigma_j/(M+1) - 1}\, p^{n[1 - 1/(M+1)]} \\ &\leq p^{(m_j + t + 1)/(M+1) - 1}\, p^{n[1 - 1/(M+1)]} \\ &\leq p^{t/(M+1)}\, p^{n[1 - 1/(M+1)]} . \end{aligned}$$

(ii) $j \in A_2$. Again by Lemma 1.22 we obtain

$$\begin{aligned} | S_j | &\leq p^{n-1} = p^{n/(M+1) - 1}\, p^{n[1 - 1/(M+1)]} \\ &\leq p^{(\sigma_j + 2t_j)/(M+1) - 1}\, p^{n[1 - 1/(M+1)]} \\ &\leq p^{(m_j + t + 1 + t_j)/(M+1) - 1}\, p^{n[1 - 1/(M+1)]} \\ &\leq p^{(t + \tau)/(M+1)}\, p^{n[1 - 1/(M+1)]} . \end{aligned}$$

(iii) $j \in A_3$. It is easily seen that

$$| S_j | = p^{\sigma_j - 1} | S(p^{n - \sigma_j}, g_j(y)) | . \tag{1.82}$$

Let $y = u + p^{t_j} v$, where $1 \le u \le p^{t_j}$, $0 \le v \le p^{t_j+1} - 1$. Then

$$S(p^{n-\sigma_j}, g_j(y)) = S(p^{2t_j+1}, g_j(y))$$
$$= \sum_{u=1}^{p^{t_j}} e_{p^{2t_j+1}}(g_j(u)) \sum_{v=0}^{p^{t_j+1}-1} e_p\left(\frac{g_j'(u)}{p^{t_j}} v + \frac{1}{2} g_j''(u) v^2\right).$$

It then follows from this and Lemma 1.22 that

$$| S(p^{n-\sigma_j}, g_j(y)) | \le p^{t_j} \sum_{u=1}^{p^{t_j}} \left| \sum_{v=0}^{p-1} e_p\left(\frac{g_j'(u)}{p^{t_j}} v + \frac{1}{2} g_j''(u) v^2\right) \right|$$
$$\le p^{2t_j + 1/2}$$
$$= p^{n - \sigma_j - 1/2}$$
$$= p^{n/(M+1) - \sigma_j - 1/2} p^{n[1 - 1/(M+1)]}.$$

Thus, in view of (1.78) and Lemma 1.22, we obtain

$$| S_j | \le p^{n/(M+1) - 3/2} p^{n[1 - 1/(M+1)]}$$
$$= p^{(\sigma_j + 2t_j + 1)/(M+1) - 3/2} p^{n[1 - 1/(M+1)]}$$
$$\le p^{(m_j + t + 1 + t_j + 1)/(M+1) - 3/2} p^{n[1 - 1/(M+1)]}$$
$$\le p^{(t + \tau)/(M+1)} p^{n[1 - 1/(M+1)]}.$$

(iv) $j \in A_4$. If A_4 is nonempty then $\tau \ge t_j + 2$. It follows from Lemma 1.22 that

$$| S_j | \le p^{n-1} = p^{n/(M+1) - 1} p^{n[1 - 1/(M+1)]}$$
$$\le p^{(\sigma_j + t_j + \tau)/(M+1) - 1} p^{n[1 - 1/(M+1)]}$$
$$\le p^{(m_j + t + 1 + \tau)/(M+1) - 1} p^{n[1 - 1/(M+1)]}$$
$$\le p^{(t + \tau)/(M+1)} p^{n[1 - 1/(M+1)]}.$$

(v) $j \in A_5$. Let k_j be the degree of g_j and let $\tau_j' = [\frac{\log k_j}{\log p}]$. Since $k_j \le k$, we have $\tau_j' \le \tau$. By the induction hypothesis and (1.78), we have

$$| S_j | \le p^{\sigma_j - 1} m(g_j) p^{(t_j + \tau')/(M(g_j)+1)} p^{(n - \sigma_j)[1 - 1/(M(g_j)+1)]}$$
$$\le p^{\sigma_j - 1} m(g_j) p^{(t_j + \tau)/(M(g_j)+1)} p^{(n - \sigma_j)[1 - 1/(M+1)]}.$$

Since $n - \sigma_j > t_j + \tau$, $(t_j + \tau - (n - \sigma_j))/(M(g_j) + 1)$ is negative. Therefore, by Lemma 1.22 and the facts that $m(g_j) \le m_j$ and $M(g_j) \le M$,

$$| S_j | \le m_j p^{(\sigma_j + t_j + \tau)/(M+1) - 1} p^{n[1 - 1/(M+1)]}$$

$$\leq m_j\, p^{(m_j + t + 1 + \tau)/(M+1) - 1}\, p^{n[1 - 1/(M+1)]}$$

$$\leq m_j\, p^{(t + \tau)/(M+1)}\, p^{n[1 - 1/(M+1)]}.$$

By (i) - (v), (1.80) and (1.81), we see that (1.79) holds for Case 3). The theorem now follows.

4. Example. The following example shows that our theorem is essentially the best possible.

Let $p = 2$, $n = 1$, and $f(x) = x^3 + x$. By simple calculation,

$$S(2\, ,\, f(x)) = \sum_{x=0}^{1} e_2(x^3 + x) = 2. \tag{1.83}$$

It is easily seen that $f'(x) = 3x^2 + 1$ so that $t = 0$. Since $f'(0) \equiv 1 \not\equiv 0 \pmod 2$ and $f'(1) = 4 \equiv 0 \pmod 2$, we have $r = m = M = 1$. Now $\tau = [\frac{\log 3}{\log 2}] = 1$. Hence, our Theorem 1.2 gives that

$$2 = |\, S(2\, ,\, f(x))\, | \leq 2^{1/(M+1)}\, 2^{1 - 1/(M+1)} = 2.$$

CHAPTER 2. CONGRUENCES

§2.1. The condition of congruent solvability

Let k, s, and q be positive integers.

Let N(q) denote the number of solutions of the congruences

$$\begin{aligned} x_1 + \dots + x_s &\equiv b_1, \\ &\vdots \qquad\qquad (\text{mod } q) \qquad (2.1) \\ (x_1)^k + \dots + (x_s)^k &\equiv b_k, \end{aligned}$$

where $1 \le x_i \le q$, $(x_i, q) = 1$, $1 \le i \le s$.

For $q = p^n$, with p a prime and n a positive integer, Hua [26] proved that if

$$p > 2^s (2k^3)^{sk/(s - k^2)} = H, \quad \text{say,} \tag{2.2}$$

then congruence (2.1) is always solvable, where $s > k^2 + k$. By a simple observation, we have

$$H > 2^{k^2} k^{3k}. \tag{2.3}$$

Hence, H is quite large. The purpose here is to reduce H to k^2, approximately.

Theorem 2.1. Let $k \ge 3$,

$$b(k) = (k - 1)^{2k/(k - 2)}. \tag{2.4}$$

Then when $s \ge 2k^2$, congruence (2.1) is always solvable for $q = p^n$ if

$$p \ge b(k). \tag{2.5}$$

For the proof we will need some lemmas and the following notation.

Let $\sum_{x\,(m)}$ denote a sum in which the variable x runs through a complete set of residues modulo m and $\sum^*_{x\,(m)}$ denote a sum in which the variable x runs through a reduced set of residues modulo m.

Put

$$T\left(\frac{a_k}{m_k}, \dots, \frac{a_1}{m_1}\right) = \sum^*_{x\,(M)} e\left(\frac{a_k}{m_k}x^k + \dots + \frac{a_1}{m_1}x\right), \tag{2.6}$$

where M is the least common multiple of $m_1, \dots, m_k$, $e(m) = e^{2\pi i m}$. We also put

$$T(m, f(x)) = T\left(\frac{a_k}{m}, \dots, \frac{a_1}{m}\right) = \sum^*_{x\,(M)} e^{2\pi i f(x)/m}, \tag{2.7}$$

where

$$f(x) = a_k x^k + \dots + a_1 x + a_0 \quad \in \mathbf{Z}[x]$$

such that $(a_1, \dots, a_k, p) = 1$.

Define

$$A(M) = \sum_{\substack{c_k=1 \\ (c_k, \dots, c_1, M)=1}}^{M} \dots \sum_{c_1=1}^{M} \left(\frac{1}{\phi(M)} T\left(\frac{a_k}{M}, \dots, \frac{a_1}{M}\right)\right)^s e_M(-c_k b_k - \dots - c_1 b_1) \tag{2.8}$$

and

$$\partial_p = \sum_{n=0}^{\infty} A(p^n), \qquad A(1) = 1, \tag{2.9}$$

where $e_M(m) = e^{2\pi i m/M}$, and as usual, $\phi(m)$ is the number of positive integers not exceeding m and prime to m.

The symbols $S(q, f(x))$, r, m, μ_j, $g_{\mu_j}(y)$, t, t_j, and σ_j are defined as in Chapter 1. Furthermore, we define

$$T_v = \sum_{\substack{x=1 \\ x \equiv v \pmod p}}^{p^n} e_{p^n}(f(x)), \qquad T_0 = 0. \tag{2.10}$$

Lemma 2.1. Let $d \geq 2$ be an integer and let b_i, $i = 1, \ldots, d$, be real numbers such that $b_i \geq 4$ for all i. Then

$$\sum_{i=1}^{d} b_i \leq 2^{-(d-1)} \prod_{i=1}^{d} b_i .$$

Proof. We use induction on d to show the lemma. For $d = 2$, we want to show that

$$b_1 + b_2 \leq \frac{1}{2} b_1 b_2 . \tag{2.11}$$

Let

$$h(x, y) = xy - 2(x + y), \qquad x, y \geq 4.$$

Taking partial derivatives, we obtain

$$\frac{\partial h(x, y)}{\partial x} = y - 2 > 0,$$

and

$$\frac{\partial h(x, y)}{\partial y} = x - 2 > 0.$$

Hence, $h(x, y)$ is always increasing in each variable $x, y > 2$. This implies that

$$h(x, y) \geq h(4, 4) = 0, \text{ where } x, y \geq 4,$$

which shows that (2.11) holds.

Let $d \geq 2$ and assume that the lemma holds for d. Then by the induction hypothesis,

$$\sum_{i=1}^{d+1} b_i = \sum_{i=1}^{d} b_i + b_{d+1} \leq 2^{-(d-1)} \prod_{i=1}^{d} b_i + b_{d+1} . \tag{2.12}$$

Since

$$2^{-(d-1)} \prod_{i=1}^{d} b_i \geq \sum_{i=1}^{d} b_i \geq 4,$$

the right side of (2.12) does not exceed

$$2^{-1} \left(\left(2^{-(d-1)} \prod_{i=1}^{d} b_i \right) b_{d+1} \right) = 2^{-d} \prod_{i=1}^{d+1} b_i ,$$

as required.

Lemma 2.2. If integers $d \geq 1$, $b_i \geq 1, i = 1, \ldots, d$, then

$$\sum_{i=1}^{d} 2^{b_i} \leq 2^{b_i + \ldots + b_d}.$$

Proof. The lemma follows from the simple observation that if a, b ≥ 1, then $2^a + 2^b \leq 2^{a+b}$, and the use of mathematical inductioin.

Lemma 2.3. If $n \geq 2$, then

$$|T_{\mu_j}| \begin{cases} \leq p^{n-1} & \text{if } n \leq \sigma_j \\ = p^{\sigma_j - 1} |S(p^{n-\sigma_j}, g_{\mu_j}(y))| & \text{if } n > \sigma_j \end{cases}$$

Proof. If $n \geq 2$, then each integer x, $1 \leq x \leq p^n$, $(x, p) = 1$, can be uniquely expressed as

$$x = y + p^{n-1} z, \qquad 1 \leq y \leq p^{n-1}, (y, p) = 1, 0 \leq z < p.$$

If $v \neq \mu_j, j = 1, \ldots, r$, then

$$T_v = \sum_{\substack{x=1 \\ x \equiv v \ (\mathrm{mod}\ p)}}^{p^n} e_{p^n}(f(x)) = \sum_{\substack{y=1 \\ y \equiv v \ (\mathrm{mod}\ p)}}^{p^{n-1}} e_{p^n}(f(y)) \sum_{z=0}^{p-1} e_{p^n}(p^{n-1} z f'(y))$$

$$= \sum_{\substack{y=1 \\ y \equiv v \ (\mathrm{mod}\ p)}}^{p^{n-1}} e_{p^n}(f(y)) \sum_{z=0}^{p-1} e_p(z f'(y))$$

$$= 0.$$

Hence,

$$T_{\mu_j} = \sum_{\substack{x=1 \\ x \equiv \mu_j \ (\mathrm{mod}\ p)}}^{p^n} e_{p^n}(f(x))$$

$$= \sum_{y=1}^{p^{n-1}} e_{p^n}(f(\mu_j + py)). \tag{2.13}$$

If $n \leq \sigma_j$, then it is easily seen that

$$|T_{\mu_j}| \leq p^{n-1},$$

and when $n > \sigma_j$, by (2.13) we have

$$|T_{\mu_j}| = \left| e_{p^n}(f(\mu_j)) \sum_{y=1}^{p^{n-1}} e_{p^{n-\sigma_j}}(p^{-\sigma_j}(f(\mu_j + py) - f(\mu_j)))\right|$$

$$= \left|p^{\sigma_j - 1} \sum_{y=1}^{p^{n-\sigma_j}} e_{p^{n-\sigma_j}}(g_{\mu_j}(y))\right|$$

$$= p^{\sigma_j - 1} |S(p^{n-\sigma_j}, g_{\mu_j}(y)| .$$

This completes the proof.

Lemma 2.4.

$$|T(p^n, f(x))| \leq \sum_{j=1}^{r} |T_{\mu_j}| .$$

Proof. This follows directly from the definitions (2.7) and (2.10) as well as the first proof of Lemma 2.3.

Lemma 2.5. [11] If $n \geq 1$ and $p > (k-1)^{2k/(k-2)}$, then

$$|S(p^n, f(x))| \leq p^{n(1-1/k)} .$$

Lemma 2.6. If $p \geq (k-1)^{2k/(k-2)}$, then

$$|T(p^n, f(x))| \leq \begin{cases} p^{1-1/k}(1 + p^{-1/2}(k-1)^{-1}) & \text{for } n = 1 \\ p^{n(1-1/k)} & \text{for } n \geq 2. \end{cases}$$

Proof. For $n = 1$, by A. Weil's inequality (see Lemma 1.23), we have immediately

$$\begin{aligned} |T(p, f(x))| &\leq |S(p, f(x))| + 1 \\ &\leq (k-1)\, p^{1/2} + 1 \\ &= (k-1)\, p^{1/2}(1 + p^{-1/2}(k-1)^{-1}) \\ &= (k-1)\, p^{-1/2+1/k} p^{1-1/k}(1 + p^{-1/2}(k-1)^{-1}) \\ &\leq p^{1-1/k}(1 + p^{-1/2}(k-1)^{-1}), \end{aligned}$$

as $p \geq (k-1)^{2k/(k-2)}$.

Suppose now $n \geq 2$. If $n > \sigma_j$, then by Lemmas 2.3 and 2.5, we have

$$
\begin{aligned}
|T_{\mu_j}| &= p^{\sigma_j - 1} |S(p^{n - \sigma_j}, g_{\mu_j}(y)| \\
&\leq p^{\sigma_j - 1} p^{(n - \sigma_j)(1 - 1/k)} \\
&= p^{n(1 - 1/k)} p^{\sigma_j/k - 1}.
\end{aligned}
$$

(2.14)

If $n \leq \sigma_j$, then by Lemma 2.3 we obtain

$$
\begin{aligned}
|T_{\mu_j}| &\leq p^{n-1} \\
&= p^{n(1 - 1/k)} p^{n/k - 1} \\
&\leq p^{n(1 - 1/k)} p^{\sigma_j/k - 1}.
\end{aligned} \tag{2.15}
$$

It follows from Lemma 2.4, (2.14) and (2.15) that for any $n \geq 2$, we have

$$|T(p^n, f(x))| \leq p^{n(1 - 1/k)} \sum_{j=1}^{r} p^{\sigma_j/k - 1}. \tag{2.16}$$

Lemma 1.5 gives that

$$\sigma_j \leq m_j + t + 1,$$

where t is the highest power of p dividing $f'(x)$. Since $p > k$ and $(a_1, \ldots, a_k, p) = 1$, we have $t = 0$. Therefore,

$$\sigma_j \leq m_j + 1, \tag{2.17}$$

and so, by (2.16),

$$|T(p^n, f(x))| \leq p^{n(1 - 1/k)} \sum_{j=1}^{r} p^{(m_j + 1)/k - 1} = p^{n(1 - 1/k)} \Sigma, \text{ say.} \tag{2.18}$$

Suppose $p \geq 2^k$. Since $m_j + 1 - k \leq 0$, we have

$$\Sigma = \sum_{j=1}^{r} p^{(m_j + 1 - k)/k} \leq \sum_{j=1}^{r} 2^{m_j + 1 - k} = 2^{1-k} \sum_{j=1}^{r} 2^{m_j}.$$

By Lemma 2.2, the sum at the right-most side does not exceed

$$2^{m_1 + \ldots + m_r} = 2^m.$$

Thus,

$$\Sigma \leq 2^{1 - k + m} \leq 1, \tag{2.19}$$

as $m + 1 \leq k$.

Suppose now $p < 2^k$. If $r = 1$, then

$$\Sigma = p^{(m_1 + 1 - k)/k} \leq 1.$$

Next assume $r > 1$. If $p^{(m_j + 1)/k} \leq 4$ for all $j = 1, \ldots, r$, then

$$\Sigma \leq 4 r p^{-1} \leq 4 (k - 1) p^{-1}. \qquad (2.20)$$

Recall $p \geq (k - 1)^{2k/(k - 2)}$, and so

$$\Sigma \leq 4(k - 1)^{-(k + 2)/(k - 2)} \leq 1, \qquad (2.21)$$

for all $k \geq 2$. Suppose some of the $p^{(m_j + 1)/k} \leq 4$ but some are not. Then, we may assume $p^{(m_j + 1)/k} \leq 4$, $j = 1, \ldots, v$, and $p^{(m_j + 1)/k} > 4$, $j = v + 1, \ldots, r$. Using Lemma 2.1,

$$\begin{aligned}
\Sigma &\leq (4v + \sum_{j=v+1}^{r} p^{(m_j + 1)/k})\, p^{-1} \\
&\leq (4v + p^{(m_{v+1} + \ldots + m_r + 1)/k})\, p^{-1} \\
&\leq (4(k - 1) + p^{m/k})\, p^{-1} \\
&\leq (4(k - 1) + p^{(k - 1)/k})\, p^{-1} \\
&= (4(k - 1)\, p^{-1 + 1/k} + 1)\, p^{-1/k} \\
&\leq (4(k - 1)^{1 - (1 - 1/k)(2k)/(k - 2)} + 1)\, p^{-1/k} \\
&= (4(k - 1)^{-k/(k - 2)} + 1)\, p^{-1/k} \\
&\leq 1, \qquad (2.22)
\end{aligned}$$

since $p \geq (k - 1)^{2k/(k - 2)}$.

If $p^{(m_j + 1)/k} > 4$, for all $j = 1, \ldots, r$, then again by Lemma 2.1,

$$\begin{aligned}
\Sigma &\leq p^{(m_1 + \ldots + m_r + 1)/k - 1} \\
&= p^{(m + 1 - k)/k} \\
&\leq 1. \qquad (2.23)
\end{aligned}$$

The lemma follows from (2.18) - (2.23).

Lemma 2.7. [26]

$$\sum_{i=0}^{n} A(p^i) = p^{nk} \phi^{-s}(p^n)\, N(p^n).$$

Lemma 2.8. For $s \geq 2k^2$ and $p \geq (k-1)^{2k/(k-2)}$, we have

$$|\partial_p - 1| \leq \frac{p^{k-s/k}}{(1-p^{-1})^s}(1+p^{-1/2}(k-1)^{-1})^s.$$

Proof. By Lemma 2.6, if $p \geq (k-1)^{2k/(k-2)}$, then

$$|T(\frac{a_k}{p^n}, \dots, \frac{a_1}{p^n})| \leq \begin{cases} p^{1-1/k}(1+p^{-1/2}(k-1)^{-1}) & \text{for } n = 1 \\ p^{n(1-1/k)} & \text{for } n \geq 2. \end{cases}$$

Thus, by (2.8), for $p \geq (k-1)^{2k/(k-2)}$, when $n \geq 2$,

$$\begin{aligned} |A(p^n)| &\leq p^{ns(1-1/k)} \left(\frac{1}{\phi(p^n)}\right)^s \sum_{\substack{a_k=1}}^{p^n} \cdots \sum_{\substack{a_1=1 \\ (a_k, \dots, a_1, p^n)=1}}^{p^n} 1 \\ &= \left(\frac{p^{n(1-1/k)}}{p^n(1-1/p)}\right)^s (p^{nk} - p^{(n-1)k}) \\ &= p^{n(k-s/k)}(1-p^{-k})(1-p^{-1})^{-s}, \end{aligned}$$

and

$$\begin{aligned} |A(p)| &\leq (1+p^{-1/2}(k-1)^{-1})^s \left(\frac{1}{\phi(p)}\right)^s \sum_{\substack{a_k=1}}^{p} \cdots \sum_{\substack{a_1=1 \\ (a_k, \dots, a_1, p)=1}}^{p} 1 \\ &= \left(\frac{p^{1-1/k}}{p(1-1/p)}\right)^s (p^k - 1)(1+p^{-1/2}(k-1)^{-1})^s \\ &= p^{k-s/k}(1-p^{-k})(1-p^{-1})^{-s}(1+p^{-1/2}(k-1)^{-1})^s. \end{aligned}$$

Hence, recalling (2.9) and the fact $s \geq 2k^2$,

$$\begin{aligned} |\partial_p - 1| &\leq (1-p^{-k})(1-p^{-1})^{-s}\left(p^{k-s/k}(1+p^{-1/2}(k-1)^{-1})^s + \sum_{n=2}^{\infty} p^{n(k-s/k)}\right) \\ &= (1-p^{-k})(1-p^{-1})^{-s}\left(p^{k-s/k}(1+p^{-1/2}(k-1)^{-1})^s + \frac{p^{2(k-s/k)}}{1-p^{k-s/k}}\right) \\ &= (1-p^{-k})(1-p^{-1})^{-s}\frac{p^{k-s/k}}{1-p^{k-s/k}} \\ &\quad \left((1+p^{-1/2}(k-1)^{-1})^s(1-p^{k-s/k}) + p^{k-s/k}\right) \end{aligned}$$

$$\leq \frac{p^{k - s/k}}{(1 - p^{-1})^s}(1 + p^{-1/2}(k-1)^{-1})^s(1 - p^{k - s/k} + p^{k - s/k})$$
$$= \frac{p^{k - s/k}}{(1 - p^{-1})^s}(1 + p^{-1/2}(k-1)^{-1})^s,$$

as required.

Proof of the theorem. Suppose $p > b(k)$ and $s \geq 2k^2$. Define

$$w(k, p, s) = \frac{p^{k - s/k}(1 + p^{-1/2}(k-1)^{-1})^s}{(1 - p^{-1})^s} \tag{2.24}$$

and

$$W(k, p, s) = \log w(k, p, s). \tag{2.25}$$

Then

$$W(k, p, s) = (k - s/k)\log p - s\log(1 - p^{-1}) + s\log(1 + p^{-1/2}(k-1)^{-1}). \tag{2.26}$$

Now

$$\frac{\partial W(k, p, s)}{\partial s} = -\frac{1}{k}\log p - \log(1 - p^{-1}) + \log(1 + p^{-1/2}(k-1)^{-1})$$
$$= \log\frac{p^{1 - 1/k}(1 + p^{-1/2}(k-1)^{-1})}{p - 1}. \tag{2.27}$$

We will show that $p(1 - p^{-1/k}(1 + p^{-1/2}(k-1)^{-1})) > 1$ which implies

$$\frac{p^{1 - 1/k}(1 + p^{-1/2}(k-1)^{-1})}{p - 1} < 1. \tag{2.28}$$

Clearly, $p(1 - p^{-1/k}(1 + p^{-1/2}(k-1)^{-1}))$ is increasing with p. Thus, if $p \geq b(k)$, then

$$p(1 - p^{-1/k}(1 + p^{-1/2}(k-1)^{-1}))$$
$$\geq (k-1)^{2k/(k-2)}(1 - (k-1)^{-2/(k-2)}(1 + (k-1)^{-k/(k-2)}(k-1)^{-1}))$$
$$= (k-1)^{2(k-1)/(k-2)}((k-1)^{2/(k-2)} - 1 - (k-1)^{-(2k-2)/(k-2)})$$
$$> (k-1)^{2(k-1)/(k-2)}((k-1)^{2/(k-1)} - 1 - (k-1)^{-(2k-2)/(k-2)})$$
$$= R, \quad \text{say.} \tag{2.29}$$

Since for $x \geq 3$,

$$x^{2/x} = e^{(2/x)\log x} = 1 + \frac{2}{x}\log x + \frac{1}{2!}\left(\frac{2}{x}\right)^2 \log^2 x + \dots,$$

we have

$$x^{2/x} - 1 \geq \frac{2}{x}.$$

Thus,

$$\begin{aligned} R &\geq (k-1)^{2(k-1)/(k-2)}\left(\frac{2}{(k-1)} - (k-1)^{-(2k-2)/(k-2)}\right) \\ &\geq (k-1)^2\left(\frac{2}{(k-1)} - \frac{1}{(k-1)^2}\right) \\ &= (k-1)\left(2 - \frac{1}{k-1}\right) \\ &> 1, \qquad \text{for } k \geq 4. \end{aligned}$$

If $k = 3$, it is easily seen that

$$R = 2^4 (3 - 2^{-4}) > 1.$$

Thus, by (2.29),

$$p(1 - p^{-1/k}(1 + p^{-1/2}(k-1)^{-1})) > 1.$$

Consequently, (2.28) holds. Therefore, by (2.27) and (2.28),

$$\frac{\partial W(k, p, s)}{\partial s} < 0, \qquad \text{for } p > b(k),\ s \geq 2k^2 \text{ and } k \geq 3.$$

Hence, $W(k, p, s)$ is decreasing for $s \geq 2k^2$. By (2.26),

$$\begin{aligned} W(k, p, s) &\leq -k\log p - 2k^2 \log(1 - p^{-1}) + 2k^2 \log(1 + p^{-1/2}(k-1)^{-1})) \\ &= W_1(k, p), \qquad \text{say.} \end{aligned} \tag{2.30}$$

Since

$$\frac{\partial W_1(k, p)}{\partial p} = -\frac{k}{p} - \frac{2k^2}{p^2 - p} - \frac{k^2}{(1 + p^{-1/2}(k-1)^{-1})\, p^{3/2}(k-1)} < 0,$$

it follows that $W_1(k, p)$ is decreasing with p for $p \geq b(k)$. Thus,

$$W_1(k, p) \leq -\frac{2k^2}{k-2}\log(k-1) - 2k^2 \log(1 - b(k)^{-1}) +$$

$$2k^2 \log (1 + b(k)^{-1/2} (k-1)^{-1}). \tag{2.31}$$

If $0 < x < 1$, then

$$\log (1 - x) = -x - x^2/2 - x^3/3 - \dots .$$

This implies that

$$\log (1 - x) \geq -x - x^2/2 - x^3(1 + x + x^2 + \dots)$$
$$= -x - x^2/2 - x^3/(1 - x). \tag{2.32}$$

By (2.31) and (2.32),

$$W_1(k, p) \leq -\frac{2k^2}{k-2} \log (k-1) + 2k^2 \left(\frac{1}{b(k)} + \frac{1}{2b(k)^2} + \frac{1}{b(k)^2(b(k)-1)}\right) + \frac{2k^2}{b(k)^{1/2}(k-1)}$$
$$= W_2(k), \quad \text{say.} \tag{2.33}$$

Here we have used the well-known fact that $\log (1 + x) \leq x$, for $x > 0$. Since $b(k) > (k-1)^2$, it is easily seen that $W_2(k) < 0$ for all $k \geq 3$. Therefore, by (2.30) and (2.33), we have

$$W(k, p, s) < 0.$$

On recalling (2.24) and (2.25), we have

$$\frac{p^{k - s/k}(1 + p^{-1/2}(k-1)^{-1})^s}{(1 - p^{-1})^s} < 1.$$

By this and Lemma 2.8, we obtain

$$\partial_p > 0, \qquad \text{for } p \geq b(k) \text{ and } s \geq 2k^2. \tag{2.34}$$

By (2.9) and Lemma 2.7, we have

$$\partial_p = \lim_{n \to \infty} p^{nk} \phi^{-s}(p^n) N(p^n). \tag{2.35}$$

It follows from the definition of $N(m)$ that if there exists an n_0 such that $N(p^{n_0}) = 0$, then $N(p^n) = 0$ for all $n > n_0$. Hence, by (2.35), $\partial_p = 0$, contradicting (2.34). This implies that $N(p^n) > 0$ for all n and $p \geq b(k)$.

§2.2. On polynomial congruences modulo p^n

As usual, let p be a prime ,

$$f(x) = a_k x^k + \ldots\ldots + a_1 x + a_0 \tag{2.36}$$

be a polynomial with integral coefficients such that $(a_k , \ldots\ldots , a_1 , p) = 1$ and write

$$S(p^n, f(x)) = \sum_{x \bmod p^n} e_{p^n}(f(x)) , \tag{2.37}$$

where the sum is taken over a complete set of residues modulo p^n and $e_{p^n}(t) = \exp(2\pi i t/p^n)$.

We denote by $V_a(f, p^n)$ the a set of f modulo p^n, that is,

$$V_a(f, p^n) = \{x \bmod p^n: \ f(x) \equiv a \pmod{p^n}\} \tag{2.38}$$

and put

$$N = N(f, p^n) = \text{Card } V_a(f, p^n). \tag{2.39}$$

L. K. Hua [26] proved that

$$|S(p^n, f(x))| \le k^3 p^{n[1 - (1/k)]} , \tag{2.40}$$

and so one can deduce that

$$N(f, \ p^n) < (2 + \sqrt{2}\,) k^3 p^{n[1 - (1/k)]}.$$

Define t satisfying $p^t \| (ka_k , \ldots , 2a_2 , a_1)$, where the symbol $\|$ means that t is the highest order v such that $p^v \mid (ka_k , \ldots , 2a_2 , a_1)$. Let $\mu_1 , \ldots , \mu_r$ be the different zeros modulo p of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod{p}, \qquad 0 \le x \le p ,$$

and let $m_1 , \ldots , m_r$ be their multiplicities. Put $\max\limits_{1 \le i \le r} m_i = M = M(f)$ and $\sum\limits_{i=1}^{r} m_i = m = m(f)$.

Recently Chalk [9] obtained that

$$N(p^n, f(x)) < (2 + \sqrt{2}\,) \, m \, k \, p^{t/(M+1)} p^{n[1 - (1/(M+1))]} , \tag{2.41}$$

by using his result on exponential sums (cf. Chalk [8]).

Let $\tau = \left[\frac{\log k}{\log p}\right]$. Note that

$$p^{\tau} \le p^{\log k / \log p} = k. \tag{2.42}$$

We proceed to prove

Theorem 2.2.

$$N(p^n, f(x)) < (2 + \sqrt{2}\,)\, m\, p^{\tau/(M+1)}\, p^{t/(M+1)}\, p^{n[1 - (1/(M+1))]}. \tag{2.43}$$

By (2.42),

$$p^{\tau/(M+1)} \le k^{1/(M+1)},$$

which is clearly better than (2.41) as $M \ge 1$.

Proof. We have

$$\begin{aligned} N(p^n, f(x)) &= p^{-\alpha} \sum_{y=1}^{p^\alpha} \sum_{z=0}^{p^\alpha - 1} e_{p^\alpha}(z(f(y) - a)) \\ &= p^{-\alpha} \sum_{z=0}^{p^\alpha - 1} e_{p^\alpha}(-za) \sum_{y=1}^{p^\alpha} e_{p^\alpha}(zf(y)). \end{aligned}$$

Thus

$$\begin{aligned} N(p^n, f(x)) &\le p^{-\alpha} \sum_{z=1}^{p^\alpha - 1} \Big| \sum_{y=1}^{p^\alpha} e_{p^\alpha}(zf(y)) \Big| + 1 \\ &= p^{-\alpha} \sum_{z=1}^{p^\alpha - 1} |S(p^\alpha, zf(y))| + 1. \end{aligned}$$

Note that there are at most $p^{\alpha - v}$ values for z such that $z = p^v u$ with $p \nmid u$. This implies that

$$\sum_{z=1}^{p^\alpha - 1} |S(p^\alpha, zf(y))| \le \sum_{v=0}^{\alpha - 1} p^v p^{\alpha - v} |S(p^{\alpha - v}, f(x))|.$$

By Theorem 1.2, we obtain

$$\begin{aligned} N(p^n, f(x)) &\le m\, p^{\tau}\, p^{t/(M+1)} \sum_{v=0}^{\alpha} p^{(\alpha - v)(1 - 1/(M+1))} \\ &\le m\, p^{\tau}\, p^{t/(M+1)} \Big(\sum_{v=0}^{\alpha} p^{-v(1 - 1/(M+1))} \Big)\, p^{\alpha(1 - 1/(M+1))} \\ &< (2 + \sqrt{2}\,)\, m\, p^{\tau/(M+1)}\, p^{t/(M+1)}\, p^{n(1 - (1/(M+1)))}, \end{aligned}$$

since

$$\sum_{v=0}^{\alpha} p^{-v(1 - 1/(M+1))} < \sum_{v=0}^{\infty} p^{-v/2}$$

$$= \frac{1}{1 - p^{-1/2}}$$

$$\leq 2 + \sqrt{2} ,$$

as $M \geq 1$ and $p \geq 2$. This completes the proof.

CHAPTER 3. SMALL SETS OF *k*-TH POWERS

§3.1. Small sets of k-th powers

1. INTRODUCTION.

The famous Waring problem states that for every $k \geq 2$ there exists a number $r \geq 1$ such that every natural number is the sum of at most r kth powers. Let $g(k)$ be the smallest possible value for r. Analogous to $g(k)$, let $G(k)$ denote the minimal value of r such that every sufficiently large integer is the sum of r kth powers. Clearly $G(k) \leq g(k)$. In 1770, Lagrange proved that $g(2) = 4$. Since every positive integer of the form $8t + 7$ cannot be written as the sum of three squares, $G(2)$ cannot be 3, and so $G(2) = g(2) = 4$. In 1909, Wieferich [47] proved $g(3) = 9$. Landau [27] and Linnik [28] obtained $G(3) \leq 8$ and $G(3) \leq 7$ in 1909 and 1943 respectively. Though forty-nine years have passed without an improvement to $G(3)$, it is never-the-less conjectured that $G(3) = 4$ (cf. [37], p. 240).

Choi, Erdös and Nathanson [12] showed that for every $N > 1$, there is a set A of squares such that $|A| < (4/\log 2)\, N^{1/3} \log N$ and every $n \leq N$ is a sum of four squares in A, here and below we denote by $|A|$ the cardinality of set A. Nathanson [33] proved the following more general result.

Theorem A. Let $k \geq 2$ and $s = g(k) + 1$. For any $\varepsilon > 0$ and given $N \geq N(\varepsilon)$ there exists a finite set A of k-th powers such that

$$|A| \leq (2 + \varepsilon)N^{1/(k+1)}$$

and each nonnegative integer $n \leq N$ is the sum of s elements belonging to A.

Our Theorem 3.1 is a generalization of Theorem A (Theorem A is the special case $r = 1$).

Theorem 3.1. Let $k \geq 2$ and for any positive integer r let $u_r = g(k) + r$. Then for every $\varepsilon > 0$ and given $N \geq N(r, \varepsilon)$, there exists a finite set A of k-th powers such that

$$|A| \leq C(r,\varepsilon)N^{1/(k+r)}$$

and every nonnegative integer $n \leq N$ is the sum of u_r k-th powers in A, where $C(r,\varepsilon) = r(1 + \varepsilon)^r + 1$.

Since in most cases $G(k) < g(k)$, one could naturally think of sharpening Theorem 3.1 in terms of G(k). Our Theorem 3.2 achieves this goal.

Theorem 3.2. Let $k \geq 2$ and $q = g(k) - G(k)$. For each positive integer $r \geq q$ let $u_r' = g(k) + r - q$. Then for every $\varepsilon > 0$ and given $N \geq N(r, \varepsilon)$, there exists a finite set A of k-th powers such that

$$|A| \leq C'(r, \varepsilon) N^{1/(k + r)}$$

and every nonnegative integer $n \leq N$ is the sum of u_r' elements of A, where $C'(r, \varepsilon) = r (2 + \varepsilon)^r + 1$.

We list known values and estimations for some g(k) and G(k) in order to facilitate the comparison of Theorems 3.1 and 3.2 (cf. [37], Chapter 4, [44], [45], and [48]):

$g(4) = 19$, $G(4) = 16$; $g(5) = 37$, $6 \leq G(5) \leq 18$; $g(6) = 73$, $9 \leq G(6) \leq 27$;
$143 \leq g(7) \leq 3806$, $8 \leq G(7) \leq 36$; $279 \leq g(8) \leq 36119$, $32 \leq G(8) \leq 47$;
$g(9) \geq 548$, $13 \leq G(9) \leq 55$; $g(10) \geq 1079$, $12 \leq G(10) \leq 63$.

To compare Theorems 3.1 and 3.2 let the r of Theorem 3.1 equal the r-q of Theorem 3.2. For example, if k=6 let $r=q+1\geq 47$. Theorem 3.2 gives $|A| \leq (6(2+\varepsilon)^6+1)N^{1/53}$ and Theorem 3.1 gives $|A| \leq (6(1+\varepsilon)^6+1)N^{1/7}$ and in both cases all $n \leq N$ (for sufficiently large N) are the sums of 74 elements of A. It appears that q is large for all $k \geq 3$ (even small k).

We give a corollary which is an application of Theorem 3.2 to cubes.

COROLLARY. For every $\varepsilon > 0$ and given $N \geq N(\varepsilon)$, there exists a finite set A of cubes such that

$$|A| \leq N^{1/5+\varepsilon}$$

and every nonnegative integer $n \leq N$ is the sum of nine cubes in A.

Next, Theorem 3.3 is for squares.

Theorem 3.3. For every $N > 2$, there is a set A of squares such that

$$|A| < 7\, N^{1/4}$$

and every nonnegative integer $n \leq N$ is the sum of at most five squares in A.

Since $g(2) = 4$, $g(2) + 1 = 5$. Taking $k = 2$ in Theorem A, the conclusion is that there exists a finite set of squares such that $|A| \leq (2+\varepsilon)\, N^{1/3}$ and every nonnegative integer $n \leq N$ is the sum of 5 squares. Hence our Theorem 3.3 is better, for large N, than the case $k = 2$ in Theorem A. For example, if $N = 10^{12}$, then Theorem A gives $|A| < (2 + \varepsilon)N^{1/3} \approx$ 20,000 while Theorem 3.3 gives $|A| < 7N^{1/4} = 7000$.

Unfortunately our methods do not readily lead to infinite basic sets A of kth powers with $|A \cap \{1,2, ...,N\}| \le cN^{\alpha}$ for all N where $\alpha < 1/k$.

2. PROOF OF THEOREM 3.1.

Let $\varepsilon > 0$ and r and N be positive integers. Define

$$A_0 = \{ a^k : \ 0 \le a \le (1+\varepsilon)^r N^{1/(k+r)} \},$$

$$A_1 = \{ [s_1^{1/k} N^{k/(k(k+r))}]^k : \ 1 \le s_1 \le (1+\varepsilon)^{r-1} N^{1/(k+r)} \},$$

$$A_2 = \{ [s_2^{1/k} N^{(k+1)/(k(k+r))}]^k : \ 1 \le s_2 \le (1+\varepsilon)^{r-2} N^{1/(k+r)} \},$$

.
.
.

$$A_r = \{ [s_r^{1/k} N^{(k+r-1)/(k(k+r))}]^k : \ 1 \le s_r \le N^{1/(k+r)} \}.$$

Let $A = A_0 \cup A_1 \cup A_2 \cup \ ... \ \cup A_r$. Then

$$|A| \le (1 + (1+\varepsilon) + (1+\varepsilon)^2 + ... + (1+\varepsilon)^r) N^{1/(k+r)} \le C(r, \varepsilon) N^{1/(k+r)}.$$

It follows from the definition of g(k) that each integer $n \in [0, (1+\varepsilon)^{rk} N^{k/(k+r)}]$ is a sum of g(k), hence of $u_r = g(k) + r$, elements of $A_0 \subseteq A$.

We need two lemmas.

Lemma 3.1. If $N^{k/(k+r)} < n \le (1+\varepsilon)^{r-1} N^{(k+1)/(k+r)}$, then there is an integer $t_1^k \in A_1$ such that $n - t_1^k$ is a sum of g(k) elements of A_0.

Proof. Suppose $N^{k/(k+r)} < n \le (1+\varepsilon)^{r-1} N^{(k+1)/(k+r)}$. Define $s_1 = [\frac{n}{N^{k/(k+r)}}]$ and $t_1 = [s_1^{1/k} \ N^{1/(k+r)}]$. Then $s_1 \le (1+\varepsilon)^{r-1} N^{1/(k+r)}$,

$$n - t_1^k \ge s_1 N^{k/(k+r)} - s_1 N^{k/(k+r)} = 0,$$

and

$$n - t_1^k < (s_1 + 1) N^{k/(k+r)} - (s_1^{1/k} N^{1/(k+r)} - 1)^k$$

$$= (s_1 + 1) N^{k/(k+r)} - s_1 N^{k/(k+r)} - \sum_{j=1}^{k-1} \binom{k}{j} (-1)^{k-j} s_1^{j/k} N^{j/(k+r)}$$

$$\leq N^{k/(k+r)} + 2^k (s_1)^{(k-1)/k} N^{(k-1)/(k+r)}$$

$$\leq (1 + 2^k (1+\varepsilon)^{r(k-1)/k} N^{-1/(k(k+1))}) N^{k/(k+r)}$$

$$\leq (1+\varepsilon) N^{k/(k+r)},$$

provided N is sufficiently large. So $n - t_1^k$ is a sum of g(k) elements of $A_0 \subseteq A$ and consequently n is a sum of g(k) + 1 elements of A. This completes the proof of Lemma 3.1.

Lemma 3.2. Let $N^{(k+i)/(k+r)} < n \leq (1+\varepsilon)^{r-i-1} N^{(k+i+1)/(k+r)}$, where $1 \leq i \leq r-1$.Then there exists an integer $t_{i+1}^k \in A_{i+1}$ such that $n - t_{i+1}^k \in [0, (1+\varepsilon)N^{(k+i)/(k+r)}] \subseteq [0, (1+\varepsilon)^{r-i} N^{(k+i)/(k+r)}]$.

Proof. Suppose $N^{(k+i)/(k+r)} < n \leq (1+\varepsilon)^{r-i-1} N^{(k+i+1)/(k+r)}$, where $1 \leq i \leq r-1$. Define $s_{i+1} = [\frac{n}{N^{(k+i)/(k+r)}}]$ and $t_{i+1} = [s_{i+1}^{1/k} N^{(k+i)/(k(k+r))}]$. Then $t_{i+1}^k \in A_{i+1}$, $s_{i+1} N^{(k+i)/(k+r)} \leq n < (s_{i+1}+1) N^{(k+i)/(k+r)}$, and $s_{i+1}^{1/k} N^{(k+i)/(k(k+r))} - 1 < t_{i+1} \leq s_{i+1}^{1/k} N^{(k+i)/(k(k+r))}$. So

$$n - t_{i+1}^k \geq s_{i+1} N^{(k+i)/(k+r)} - s_{i+1} N^{(k+i)/(k+r)} = 0$$

and

$$n - t_{i+1}^k < (s_{i+1} + 1) N^{(k+i)/(k+r)} - (s_{i+1}^{1/k} N^{(k+i)/(k(k+r))} - 1)^k$$

$$= (s_{i+1} + 1) N^{(k+i)/(k+r)} - s_{i+1} N^{(k+i)/(k+r)}$$

$$- \sum_{j=1}^{k-1} \binom{k}{j} (-1)^{k-j} s_{i+1}^{j/k} N^{j(k+i)/(k(k+r))}$$

$$\leq N^{(k+i)/(k+r)} + 2^k (s_{i+1})^{(k-1)/k} N^{(k-1)/(k+r)}$$

$$\leq N^{(k+i)/(k+r)} + 2^k (1+\varepsilon)^{(r-i)(k-1)/k} N^{(k-1)/(k(k+r)) + (k-1)/(k+r)}$$

$$= (1 + 2^k (1+\varepsilon)^{(r-i)(k-1)/k} N^{-(i+1/k)/(k+r)}) N^{(k+i)/(k+r)}$$

$$\leq (1+\varepsilon) N^{(k+i)/(k+r)},$$

for sufficiently large N. This completes the proof of Lemma 3.2.

We now prove Theorem 3.1. If $N^{k/(k+r)} < n \leq (1+\varepsilon)^{r-1} N^{(k+1)/(k+r)}$, then it follows from Lemma 3.1 that there exists an integer $t_1^k \in A_1$ such that $n - t_1^k$ is a sum of $g(k)$, hence of $g(k) + r$, elements of $A_0 \subseteq A$.

Suppose $N^{(k+i)/(k+r)} < n \leq (1+\varepsilon)^{r-i-1} N^{(k+i+1)/(k+r)}$, $1 \leq i \leq r-1$. By Lemma 3.2, there exists an integer $t_{i+1}^k \in A_{i+1}$ such that $n - t_{i+1}^k \in [0, (1+\varepsilon)^{r-i} N^{(k+i)/(k+r)}]$. Write $m = n - t_{i+1}^k$. If $m \in [0, (1+\varepsilon)^r N^{k/(k+r)}]$, then m is sum of $g(k)$ elements of A_0, and so n is a sum of $g(k) + 1$ elements of A. If $m \in (N^{k/(k+r)}, (1+\varepsilon)^{r-1} N^{(k+1)/(k+r)}]$, then Lemma 3.1 yields that there is an integer $t_1^k \in A_1$ such that $m - t_1^k$ is a sum of $g(k)$ elements of A_0, and so n is a sum of $g(k) + 2$ elements of A (Note that in this case r=2). If

$$m \in (N^{(k+j)/(k+r)}, (1+\varepsilon)^{r-j-1} N^{(k+j+1)/(k+r)}]$$

for some j, $1 \leq j < i$, then again by Lemma 3.1, there exists an integer $t_{j+1}^k \in A_{j+1}$ such that $m - t_{j+1}^k \in [0, (1+\varepsilon)^{r-j} N^{(k+j)/(k+r)}]$. Repeatedly using this method, finally we get a sequence $\{\alpha_1, \alpha_2, \ldots, \alpha_v\}$ of positive integers, where $\alpha_1 > \alpha_2 > \ldots > \alpha_v$, $1 \leq v \leq i$, such that $t_{\alpha_w}^k \in A_{\alpha_w}$ for all $1 \leq w \leq v$ and

$$n - t_{\alpha_1}^k - t_{\alpha_2}^k - \ldots\ldots - t_{\alpha_v}^k \in [0, (1+\varepsilon)^r N^{k/(k+r)}].$$

Therefore $n - t_{\alpha_1}^k - t_{\alpha_2}^k - \ldots\ldots - t_{\alpha_v}^k$ is a sum of $g(k)$ elements of A_0, and so n is a sum of $g(k) + v$, hence of $g(k) + r$ for $v \leq r$, elements of A, as required.

3. PROOF OF THEOREM 3.2. Let $\varepsilon > 0$. Define

$$A_0 = \{ a^k : \ 0 \le a \le (2+\varepsilon)^r N^{1/(k+r)} \},$$

$$A_i = \{ [s_i^{1/k} N^{(k+i-1)/(k(k+r))}]^k : \ 1 \le s_i \le (2+\varepsilon)^{r-i} N^{1/(k+r)} \}, \ i = 1, \dots, r.$$

Let $A = A_0 \cup A_1 \cup \dots \cup A_r$. Then

$$|A| \le (1 + (2+\varepsilon) + (2+\varepsilon)^2 + \dots + (2+\varepsilon)^r) N^{1/(k+r)}$$

$$\le (r(2+\varepsilon)^r + 1) N^{1/(k+r)}$$

$$= C'(r, \varepsilon) N^{1/(k+r)},$$

for sufficiently large N. Now each integer $n \in [0, (2+\varepsilon)^{rk} N^{k/(k+r)}]$ is a sum of g(k) (of course of u_r' ($\ge g(k)$)) elements of A_0. Again we need two lemmas. We omit the proofs which are analogous to those of Lemmas 3.1 and 3.2. (Just let s_{i+1} here be one less than the s_{i+1} in Lemmas 3.1 and 3.2 ($0 \le i \le r-1$).)

Lemma 3.3. If $N^{k/(k+r)} < n \le (2+\varepsilon)^{r-1} N^{(k+1)/(k+r)}$, then there is an integer $t_1^k \in A_1$ such that $n - t_1^k$ is a sum of G(k) elements of A_0.

Lemma 3.4. Let $N^{(k+i)/(k+r)} < n \le (2+\varepsilon)^{r-i-1} N^{(k+i+1)/(k+r)}$, where $1 \le i \le r-1$. Then there exists an integer $t_{i+1} \in A_{i+1}$ such that $n - t_{i+1}^k \in [N^{(k+i)/(k+r)}, (2+\varepsilon) N^{(k+i)/(k+r)}] \subseteq [N^{(k+i)/(k+r)}, (2+\varepsilon)^{r-i} N^{(k+i)/(k+r)}]$.

We proceed to prove Theorem 3.2. If $N^{k/(k+r)} < n \le (2+\varepsilon)^{r-1} N^{(k+1)/(k+r)}$, then it follows from Lemma 3.3 that there exists an integer $t_1^k \in A_1$ such that $n - t_1^k$ is a sum of G(k) elements of A_0 and so n is a sum of G(k) + 1 elements of A.

Suppose $N^{(k+i)/(k+r)} < n \le (2+\varepsilon)^{r-i-1} N^{(k+i+1)/(k+r)}$, $1 \le i \le r-1$. By Lemma 3.4, there exists an integer $t_{i+1}^k \in A_{i+1}$ such that $n - t_{i+1}^k \in$

$[\, N^{(k+i)/(k+r)}, \quad (2+\varepsilon)^{r-i} N^{(k+i)/(k+r)} \,]$. Write $m = n - t_{i+1}^{k}$. If $m \in [\, N^{k/(k+r)}, (2+\varepsilon)^{r} N^{k/(k+r)} \,]$, then m is sum of G(k) elements of A_0, and so n is a sum of G(k) + 1 elements of A. If $m \in (N^{k/(k+r)}, (2+\varepsilon)^{r-1} N^{(k+1)/(k+r)} \,]$, then Lemma 3.3 yields that there is an integer $t_1^k \in A_1$ such that $m - t_1^k$ is a sum of G(k) elements of A_0, and so n is a sum of G(k) + 2 elements of A (Note that in this case r = 2). If $m \in (\, N^{(k+j)/(k+r)}, (2+\varepsilon)^{r-j-1} N^{(k+j+1)/(k+r)} \,]$ for some j, $1 \le j < i$, then again by Lemma 3.4, there exists an integer $t_{j+1}^{k} \in A_{j+1}$ such that $m - t_{j+1}^{k} \in [\, N^{(k+j)/(k+r)}, (2+\varepsilon)^{r-j} N^{(k+j)/(k+r)} \,]$. Repeatedly using this method, finally we get a sequence $\{ \alpha_1, \alpha_2, \ldots\ldots, \alpha_v \}$ of positive integers, where $\alpha_1 > \alpha_2 > \ldots\ldots > \alpha_v$, $1 \le v \le i$, such that $t_{\alpha_w}^{k} \in A_{\alpha_w}$ for all $1 \le w \le v$ and

$$n - t_{\alpha_1}^{k} - t_{\alpha_2}^{k} - \ldots\ldots - t_{\alpha_v}^{k} \in [\, N^{k/(k+r)}, (2+\varepsilon)^{r} N^{k/(k+r)} \,].$$

Therefore $n - t_{\alpha_1}^{k} - t_{\alpha_2}^{k} - \ldots\ldots - t_{\alpha_v}^{k}$ is a sum of G(k) elements of A_0, and so n is a sum of G(k) + v, hence of G(k) + r as $v \le r$, elements of A. Since G(k) = g(k) - q, this completes the proof of Theorem 3.2.

4. PROOF OF COROLLARY. Since g(3) = 9 and $G(3) \le 7$ by Linnik's theorem,we can take $r = q \ge 2$ in Theorem 3.2. Then $u_r' = 9$ and the result follows for sufficiently large N. If G(3) = 4, then this corollary is immediately improved to

$$|A| < N^{1/8+\varepsilon}.$$

5. PROOF OF THEOREM 3.3. We start with a lemma the simple proof of which may be found in [12].

Lemma 3.5. Let $a \geq 1$. Let $m \geq a^2$ and $m \not\equiv 0 \pmod 4$. Then either $m - a^2$ or $m - (a-1)^2$ is a sum of three squares.

Now define $A_1 = \{ b^2 : 0 \leq b \leq 3N^{1/4} \text{ and } b^2 \leq N \}$. Let A_2 consist of the squares of all numbers of the form $[k_1^{1/2} N^{1/4}] - i$, where $9 \leq k_1 \leq N^{1/4}$ and $i \in \{0,1\}$, and let A_3 consist of the squares of all numbers of the form $[k_2^{1/2} N^{3/8}] - j$, where $2 \leq k_2 \leq N^{1/4}$ and $j \in \{0,1\}$. Then $|A_1| \leq 3N^{1/4} + 1$, $|A_2| \leq 2N^{1/4} - 16$, and $|A_3| \leq 2N^{1/4} - 2$. Let $A = A_1 \cup A_2 \cup A_3$, then $|A| < 7N^{1/4}$.

The set A_1 contains all squares not exceeding $\min(N, 9N^{1/2})$. This implies that if $0 \leq n \leq \min(N, 9N^{1/2})$ then n is a sum of four squares in $A_1 \subseteq A$.

Now suppose $9N^{1/2} < n \leq N^{3/4}$. Put $k_1 = [\frac{n}{N^{1/2}}]$, $b = [k_1^{1/2} N^{1/4}]$. Clearly $9 \leq k_1 \leq N^{1/4}$ and $b^2 \leq n$. If either $c = b$ or $c = b - 1$ then Lagrange's theorem yields that $n - c^2$ is the sum of four squares. Note also $c^2 \in A_2$. Since $k_1 N^{1/2} \leq n < (k_1+1)N^{1/2}$ and $b \leq k_1^{1/2} N^{1/4} < b + 1$, it follows that

$$
\begin{aligned}
0 &\leq n - c^2 < (k_1 + 1) N^{1/2} - (b - 1)^2 \\
&\leq (k_1 + 1) N^{1/2} - (k_1^{1/2} N^{1/4} - 2)^2 \\
&< N^{1/2} + 4 k_1^{1/2} N^{1/4} \\
&< 9 N^{1/2}.
\end{aligned}
$$

Thus $n - c^2$ is the sum of four squares in A_1. Hence if $0 \leq n \leq N^{3/4}$ and $n \not\equiv 0 \pmod 4$, then n is a sum of five squares in A.

We now consider the case $N^{3/4} < n \leq N$. Put $k_2 = [\frac{n}{N^{3/4}}]$, $a = [k_2^{1/2} N^{3/8}]$. If c is either a or a-1, then

$$0 \leq n - c^2 < (k_2 + 1)\, N^{3/4} - (a - 1)^2 < N^{3/4} + 4\, N^{1/2} .$$

If $0 \leq n - c^2 \leq 9\, N^{1/2}$, then $n - c^2$ is a sum of four squares in A_1. Suppose now $9\, N^{1/2} < n - c^2 \leq N^{3/4} + 4\, N^{1/2}$. Write $m = n - c^2$ where we may choose c so that $m \not\equiv 0 \pmod 4$. Put $k_3 = [\frac{m}{N^{1/2}}]$ and $b = [k_3^{1/2} N^{1/4}]$. Thus $9 \leq k_3 \leq N^{1/4} + 4$, $b^2 \leq k_3 N^{1/2} \leq m$. If d is either b or b - 1, then d is in A_2 and

$$0 \leq m - d^2 < (k_3 + 1)\, N^{1/2} - (b - 1)^2 < 9\, N^{1/2} .$$

Thus, by Lemma 3.5, we may choose d such that $m - d^2$ is a sum of three squares in A_1. Hence n is the sum of five squares from A. This completes the proof.

§3.2. Small sets for squares

1. INTRODUCTION.

Lagrange proved his famous theorem in 1770 that every positive integer is a sum of four squares. Consequently, for $k \geq 4$, every integer is a sum of k squares because one can always write $n = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 0^2 + \ldots + 0^2$. The more interesting problem is then to consider the representation of positive integers n by k nonvanishing squares. For $k \geq 4$, the problem has been solved by Dubouis [16] in 1911. The result is, for $k \geq 6$, all positive integers are sums of k nonvanishing squares except for 1, 2, ... , k - 1 and all k + b, where $b \in B = \{1, 2, 4, 5, 7, 10, 13\}$,and for k = 5, the same statement holds with $b \in B \cup \{28\}$. For k = 4, all positive integers are sums of four nonvanishing squares except for the finite set consisting of 1, 2, 3 and n = 4 + b, where $b \in B \cup \{25, 37\}$, and the three infinite sets $4^a m$ with m = 2, 6, 14. For k = 3, Gogisvili [17] proved in 1970 that there exists a finite set T of positive integers with t elements, $T \supset \{1, 2, 5, 10, 13, 25, 37, 58, 85, 130\}$, and such that every positive integer n which is neither of the form $4^a(8m + 7)$ nor of theform $n = 4^a m$ with $m \in T$ is a sum of three nonvanishing squares.

Let A be an increasing sequence of positive integers and define

$$A(x) = \sum_{\substack{a \leq x \\ a \in A}} 1 \quad .$$

Choi, Erdös, and Nathanson [12] proved that Lagrange's theorem holds for a sequence of squares satisfying $|A| < (4/\log 2)\, N^{1/3} \log N$ and they conjectured that for every $\varepsilon > 0$ and $N \geq N(\varepsilon)$ there exists a set A of squares such that $|A| < N^{(1/4)+\varepsilon}$ and every $n \leq N$ is the sum of four squares in A.

We first consider nonvanishing squares. For every $\varepsilon > 0$, we construct a set A of squares with $|A| < N^{1/k+\varepsilon}$ for sufficiently large N and every integer n, $\omega \leq n \leq N$, is a sum of (k + 1) nonvanishing squares in A for some positive integer ω and for all $k \geq 4$.

P. T. Bateman and G. B. Purdy [1] proved that every integer greater than 245 is the sum of five distinct squares. Naturally, we would think of small sets for distinct squares. In the third section, for each $k \geq 3$ we construct a set A of squares such that $|A| < k(2+\varepsilon)^k N^{1/k}$ and every integer n, $N^{\varepsilon} < n \leq N$, is a sum of (k+3) distinct elements of A, where ε is a small positive number less than 0.0064.

2. NONVANISHING SQUARES.

Lemma 3.6. (cf. [18]) Every positive integer $n \geq 42$ is a sum of four nonvanishing squares except three infinite sets $4^a m$ with m = 2, 6, 14.

For convenience, write $\mathcal{L} = \{4^a m: m = 2, 6, 14\}$.

Lemma 3.7. (cf. [16]) There is a positive integer ω such that if n is a positive integer $>\omega$ and n is not of the form $4^a(8m + 7)$ and $n \not\equiv 0 \pmod 4$, then n is a sum of three nonvanishing squares.

Lemma 3.8. (cf. [18]) For $k \geq 6$, all positive integers are sums of k nonvanishing squares except for 1, 2, ... , k-1 and all k+b, where $b \in B = \{1, 2, 4, 5, 7, 10, 13\}$, and for k = 5, the same statement holds with $b \in B \cup \{28\}$.

Lemma 3.9. Let $b \geq 1$, $n - b^2 \geq 42$, $n \not\equiv 0 \pmod 4$. Then either $n - b^2$ or $n - (b - 1)^2$ is a sum of four nonvanishing squares.

Proof. By Lemma 3.6, if $q \geq 42$ is not a sum of four nonvanishing squares then q must be of the form $4^a m$ with $m = 2, 6, 14$ and $a \geq 1$. Define

$$c = \begin{cases} b & \text{if b is even} \\ b-1 & \text{if b is odd} \end{cases},$$

then c is even and $c^2 \equiv 0 \pmod 4$. Hence $n - c^2 \not\equiv 0 \pmod 4$ as $n \not\equiv 0 \pmod 4$. It then follows from Lemma 3.6 that $n - c^2$ is a sum of four nonvanishing squares.

Lemma 3.10. Let $b \geq 1$, $n - b^2 \geq \omega$, $n \not\equiv 0 \pmod 4$, where ω is as chosen in Lemma 3.7. Then there is a positive integer c , where c is either b or b - 1, such that $n - c^2$ is a sum of three nonvanishing squares.

Proof. If an integer $q > \omega$ is not a sum of three nonvanishing squares, then either $q \equiv 0 \pmod 4$ or $q \equiv 3 \pmod 4$. Suppose b is even. If $n \equiv 1$ or $2 \pmod 4$, then $n - b^2 \equiv n \pmod 4$, and so $n - b^2$ is a sum of three nonvanishing squares. If $n \equiv 3 \pmod 4$, then $n - (b-1)^2 \equiv n - 1 \equiv 2 \pmod 4$. Thus $n - (b-1)^2$ is a sum of three nonvanishing squares. If b is odd, then b-1 is even, and so we can obtain the same results.

Theorem 3.4. There is a set A of squares with $|A| < (4/\log 4)N^{1/3}\log N$ for sufficiently large N and every integer $n \notin \mathcal{L}$, $42 \leq n \leq N$, is a sum of four nonvanishing squares in A .

Proof. Let N be a large integer. Define

$$A_0 = \{a^2 : \ 1 \leq a \leq 2N^{1/3}\}$$

and

$$A_1 = \{[s^{1/2}N^{1/3}]^2 - j: \ 1 \leq s \leq N^{1/3}, j \in \{0, 1\}\}.$$

Let $A_2 = A_0 \cup A_1$. Then $|A_2| \leq 4N^{1/3}$. Note that A_0 contains all positive squares in $[1, 4N^{2/3}]$. If $42 \leq n \leq 4N^{2/3}$ and $n \not\equiv 0 \pmod 4$, then it follows from Lemma 3.6 that n is a sum of four squares in A_0.

Suppose $4N^{2/3} < n \leq N$ and $n \not\equiv 0 \pmod 4$. Put $s = [\frac{n-42}{N^{2/3}}]$ and $t = [s^{1/2}N^{1/3}]$. Then $1 < s \leq N^{1/3}$, $sN^{2/3} + 42 \leq n < (s+1)N^{2/3} + 42$, and $s^{1/2}N^{1/3} - 1 < t \leq s^{1/2}N^{1/3}$. We obtain

$$n - t^2 \geq sN^{2/3} + 42 - sN^{2/3} = 42,$$

and

$$\begin{aligned} n - (t-1)^2 &< (s+1)N^{2/3} + 42 - (s^{1/2}N^{1/3} - 2)^2 \\ &= sN^{2/3} + N^{2/3} + 42 - sN^{2/3} + 4s^{1/2}N^{1/k} - 4 \\ &< N^{2/3} + 42 + 4N^{1/2} \\ &< 2N^{2/3}, \end{aligned}$$

for sufficiently large N. Then, by Lemma 3.10, $n - c^2$ is a sum of three squares in A_0, where c is either t or (t - 1). Clearly, c^2 is nonzero and in A_1. Hence, n is a sum of four squares in A_2.

Let $A = \{4^b a^2 : a^2 \in A_2, b \geq 0\}$. If $42 \leq n \leq N$ and $n \notin \mathcal{L}$, then $n = 4^b m$ with $m \not\equiv 0 \pmod 4$ and $m \neq 2, 6, 14$. By the above argument, m is the sum of four squares in A_2. Consequently, n is the sum of four squares in A. Note that the number of b is less than or equal to logN/log4. This implies that $|A| \leq (4/\log 4)N^{1/3}\log N$ as required.

Theorem 3.5. Let $\varepsilon > 0$ and k be an integer ≥ 4. There is a set A of squares with $|A| \leq \frac{2k}{\log 4}(1+\varepsilon)^k N^{1/k}\log N$ for sufficiently large N and every integer n, $\omega_k \leq n \leq N$, $n \notin \mathcal{L}$, is a sum of (k + 1) nonzero squares in A, where $\omega_k = \max(k + 29, 42)$.

Proof. Let N be a large integer. Define

$A_0 = \{a^2 : \ 1 \leq a \leq (1+\varepsilon)^k N^{1/k}\}$,

$A_i = \{[s_i^{1/2}N^{(i+1)/2k}]^2 - j : \ 1 \leq s_i \leq (1+\varepsilon)^{k-i}N^{1/k}, j \in \{0, 1\}\}$, $i = 1, \dots, k-1$.

Let $A' = A_0 \cup A_1 \ \ldots \cup A_{k-1}$. Then $|A'| \leq 2k(1 + \varepsilon)^k N^{1/k}$. Note that A_0 contains all positive squares in $[1, (1 + \varepsilon)^{2k} N^{2/k}]$.

Suppose $(1 + \varepsilon)^{2k} N^{2/k} < n \leq (1 + \varepsilon)^{k-1} N^{3/k}$ and $n \not\equiv 0 \pmod 4$. Put $s_1 = \left[\frac{n-\omega_k}{N^{2/k}}\right]$ and $t_1 = [s_1^{1/2} N^{1/k}]$. Then $1 < s_1 \leq (1 + \varepsilon)^{k-1} N^{1/k}$, $s_1 N^{2/k} + \omega_k \leq n < (s_1 + 1)N^{2/k} + \omega_k$, and $s_1^{1/2} N^{1/k} - 1 < t_1 \leq s_1^{1/2} N^{1/k}$. We obtain

$$n - t_1^2 \geq s_1 N^{2/k} + \omega_k - s_1 N^{2/k} = \omega_k,$$

and

$$\begin{aligned} n - (t_1 - 1)^2 &< (s_1 + 1)N^{2/k} + \omega_k - (s_1^{1/2} N^{1/k} - 2)^2 \\ &= s_1 N^{2/k} + N^{2/k} + \omega_k - s_1 N^{2/k} + 4 s_1^{1/2} N^{1/k} - 4 \\ &< N^{2/k} + \omega_k + 4N^{3/(2k)} \\ &< (1 + \varepsilon) N^{2/k}, \end{aligned}$$

for sufficiently large N. Then, by Lemma 3.10, $n - c_1^2$ is a sum of three squares in A_0 , where c_1 is either t_1 or $(t_1 - 1)$. Clearly, c_1 is positive and in A_1. Hence, n is a sum of four squares in A'.

Assume now $(1 + \varepsilon)^{k-i} N^{i/k} < n \leq (1 + \varepsilon)^{k-i+1} N^{(i+1)/k}$ and $n \not\equiv 0 \pmod 4$, where $2 < i \leq k-1$. Put $s_{i-1} = \left[\frac{n-\omega_k}{N^{i/k}}\right]$ and $t_{i-1} = [s_{i-1}^{1/2} N^{1/k}]$. It follows that $1 \leq s_{i-1} \leq (1 + \varepsilon)^{k-i+1} N^{1/k}$, $s_{i-1} N^{i/k} + \omega_k \leq n < (s_{i-1}+1) N^{i/k} + \omega_k$, and $s_{i-1}^{1/2} N^{1/k} - 1 < t_{i-1} \leq s_{i-1}^{1/2} N^{1/k}$. Thus

$$n - t_{i-1}^2 \geq s_{i-1} N^{i/k} + \omega_k - s_{i-1} N^{i/k} = \omega_k$$

and

$$\begin{aligned} n - (t_{i-1} - 1)^2 &< (s_{i-1}+1) N^{i/k} + \omega_k - (s_{i-1}^{1/2} N^{1/k} - 2)^2 \\ &= s_{i-1} N^{i/k} + N^{i/k} + \omega_k - s_{i-1} N^{i/k} + 4 s_{i-1}^{1/2} N^{1/k} - 4 \\ &\leq (1 + \varepsilon) N^{i/k}, \end{aligned}$$

for sufficiently large N.

Consider first $k \geq 5$. If $n - t_{i-1}^2 \in [\omega_k, (1 + \varepsilon)^{2k} N^{2/k}]$, then by Lemma 3.3, $n - t_{i-1}^2$ is a sum of k elements in A_0. If $n - t_{i-1}^2 \in ((1 + \varepsilon)^{2k} N^{2/k}, (1 + \varepsilon)^{k-1} N^{3/k}]$, then by the above argument and Lemma 3.8, $n - t_{i-1}^2 - c_1^2$ is a sum of (k - 1) elements of A_0, and so n is the sum of (k + 1) elements of A'. If $n - t_{i-1}^2 \in ((1 + \varepsilon)^{k-\alpha}N^{\alpha/k}, (1 + \varepsilon)^{k-\alpha+1}N^{(\alpha+1)/k}]$, where $2 \le \alpha < i$, then we repeatedly use this method, finally there exist $\alpha_1, \dots, \alpha_h$ such that $t_{\alpha_1}^2, \dots, t_{\alpha_h}^2 \in A'$ and $n - t_{\alpha_1}^2 - \dots - t_{\alpha_h}^2 \in [\omega_k, (1 + \varepsilon)^{2k}N^{2/k}]$. It follows from Lemma 3.8 that $n - t_{\alpha_1}^2 - \dots - t_{\alpha_h}^2$ is a sum of (k - h + 1) elements os A_0. Therefore, n is the sum of (k + 1) elements of A'.

Let $A = \{4^b a: 4^b a \le N, a \in A'\}$. It is easily seen that $b \le \log N/\log 4$ which implies that $|A| \le \frac{2k}{\log 4}(1 + \varepsilon)^k N^{1/k}\log N$. If $\omega_k \le n \le N$, then we can write $n = 4^b m$ with $m \not\equiv 0 \pmod 4$. By the above argument, m is a sum of (k + 1) elements of A'. Consequently, n is the sum of (k + 1) elements of A.

For the case of k = 4, we can employ similar argument but using Lemma 3.9 for Lemma 3.8. This completes the proof.

3. DISTINCT SQUARES.

Lemma 3.11. ([1]) Every positive integer greater than 245 is the sum of five *distinct* squares of positive integers.

Lemma 3.12. Let $k \ge 6$. Every sufficiently large integer is the sum of k *distinct* squares of positive integers.

Proof. Suppose we know that every $n > N_s$ is the sum of s distinct positive squares. Let $a = [\sqrt{n/2}] + 1$, where $n > 2((N_s + 2)^{1/2} + 1)^2$. Then

$$\sqrt{n/2} < a < \sqrt{n/2} + 1,$$

and therefore

$$\frac{n}{2} < a^2,$$

that is,

$$\frac{n}{2} > n - a^2 > n - (\sqrt{n/2} + 1)^2 = (\sqrt{n/2} - 1)^2 - 2 > N_s,$$

so that $n - a^2$ is expressible as the sum of s distinct, positive squares each less than $\frac{n}{2} < a^2$.

Theorem 3.6. Let ε be a small positive number less than 0.0064, k be an integer ≥ 3, and N be a large integer. Then there is a set of squares such that $|A| \leq k(2+\varepsilon)^k N^{1/k}$ and every integer n, $N^\varepsilon < n \leq N$, is a sum of (k+3) *distinct* elements of A.

Proof. Define

$$A_0 = \{ a^2 : 0 \leq a \leq (2+\varepsilon)^k N^{1/k} \},$$

and

$$A_i = \{ [s_i^{1/2} N^{(i+1)/(2k)}]^2 : 1 \leq s_i \leq (2+\varepsilon)^{k-i+1} N^{1/k} \}, i = 1, \dots, k-1.$$

Let $A = A_0 \cup A_1 \cup \dots \cup A_{k-1}$, then

$$|A| \leq ((2+\varepsilon) + (2+\varepsilon)^2 + \dots + (2+\varepsilon)^k) N^{1/k}$$
$$\leq k(2+\varepsilon)^k N^{1/k}.$$

It follows directly from Lemma 3.12 that each integer n, $N^\varepsilon < n \leq (2+\varepsilon)^{2k} N^{2/k}$, is a sum of (k+3) distict elements of A_0.

Suppose $(2+\varepsilon)^{k-i} N^{i/k} < n \leq (2+\varepsilon)^{k-i-1} N^{(i+1)/k}$. Put $s_i = [\frac{n}{N^{i/k}}] - 1$ and $t_i = [s_i^{1/2} N^{i/(2k)}]$. Then

$$(2+\varepsilon)^{k-i} - 2 < s_i \leq (2+\varepsilon)^{k-i-1} N^{1/k} - 1, \tag{3.1}$$

$$(s_i + 1) N^{i/k} \leq n < (s_i + 2) N^{i/k},$$

and

$$s_i^{1/2} N^{i/(2k)} - 1 < t_i \leq s_i^{1/2} N^{i/(2k)}. \tag{3.2}$$

Thus, we have

$$n - t_i^2 \geq (s_i + 1) N^{i/k} - s_i N^{i/k} = N^{i/k}$$

and

$$n - t_i^2 < (s_i + 2) N^{i/k} - (s_i^{1/2} N^{i/(2k)} - 1)^2$$
$$= s_i N^{i/k} + 2N^{i/k} - s_i N^{i/k} + 2 s_i^{1/2} N^{i/(2k)} - 1$$
$$< (2+\varepsilon) N^{i/k}.$$

Since N is sufficiently large,

$$[N^{i/k}, (2+\varepsilon)N^{i/k}) \subset ((2+\varepsilon)^{k-i+2}N^{(i-1)/k}, (2+\varepsilon)^{k-i+1}N^{i/k}].$$

Let $n_{i-1} = n - t_i^2$. Then $n_{i-1} \in [N^{i/k}, (2+\varepsilon)N^{i/k})$. Put $s_{i-1} = [\frac{n_{i-1}}{N^{(i-1)/k}}] - 1$ and $t_{i-1} = [s_{i-1}^{1/2}N^{(i-1)/(2k)}]$.

Clearly,

$$N^{1/k} - 2 < s_{i-1} \le (2+\varepsilon)N^{1/k} - 1, \tag{3.3}$$

$$(s_{i-1}+1)N^{(i-1)/k} \le n_{i-1} < (s_{i-1}+2)N^{(i-1)/k},$$

and

$$s_{i-1}^{1/2}N^{(i-1)/(2k)} - 1 < t_{i-1} \le s_{i-1}^{1/2}N^{(i-1)/(2k)}. \tag{3.4}$$

Thus

$$n_{i-1} - t_{i-1}^2 \ge (s_{i-1}+1)N^{(i-1)/k} - s_{i-1}N^{(i-1)/k} = N^{(i-1)/k}$$

and

$$\begin{aligned} n_{i-1} - t_{i-1}^2 &< (s_{i-1}+2)N^{(i-1)/k} - (s_{i-1}^{1/2}N^{(i-1)/(2k)} - 1)^2 \\ &= s_{i-1}N^{(i-1)/k} + 2N^{(i-1)/k} - s_{i-1}N^{(i-1)/k} + 2s_{i-1}^{1/2}N^{(i-1)/(2k)} - 1 \\ &< (2+\varepsilon)N^{(i-1)/k}. \end{aligned}$$

Let $n_{i-2} = n_{i-1} - t_{i-1}^2$. Then

$$n_{i-2} \in [N^{(i-1)/k}, (2+\varepsilon)N^{(i-1)/k}) \subset ((2+\varepsilon)^{k-i+3}N^{(i-2)/k}, (2+\varepsilon)^{k-i+2}N^{(i-1)/k}].$$

Put $s_{i-2} = [\frac{n_{i-2}}{N^{(i-2)/k}}] - 1$ and $t_{i-2} = [s_{i-2}^{1/2}N^{(i-2)/(2k)}]$. By the same way as above, we get

$$N^{1/k} - 2 < s_{i-2} \le (2+\varepsilon)N^{1/k} - 1, \tag{3.5}$$

$$s_{i-2}^{1/2}N^{(i-2)/(2k)} - 1 < t_{i-2} \le s_{i-2}^{1/2}N^{(i-2)/(2k)}, \tag{3.6}$$

and

$$N^{(i-2)/k} \le n_{i-2} - t_{i-2}^2 < (2+\varepsilon)N^{(i-2)/k}.$$

It follows from (3.10) - (3.13) that

$$t_{i-1} > s_{i-1}^{1/2}N^{(i-1)/(2k)} - 1 > (N^{1/k} - 2)^{1/2}N^{(i-1)/(2k)} - 1$$

and

$$t_{i-2} \le s_{i-2}^{1/2}N^{(i-2)/(2k)} \le ((2+\varepsilon)N^{1/k} - 1)^{1/2}N^{(i-2)/(2k)} < (2+\varepsilon)^{1/2}N^{(i-1)/(2k)}.$$

But

$$(N^{1/k} - 2)^{1/2}N^{(i-1)/(2k)} - 1 > (1 - \varepsilon)^{1/2}N^{i/(2k)} > (2 + \varepsilon)^{1/2}N^{(i-1)/(2k)},$$

and so $t_{i-1} > t_{i-2}$.

Continuing in this way, we obtain a sequence of positive integers $t_{i-1}, t_{i-2}, \ldots, t_1$ such that $t_1 < t_2 < \ldots < t_{i-1}$ and

$$n - t_i^2 - t_{i-1}^2 - \ldots - t_1^2 \in [N^{1/k}, (2 + \varepsilon)^{1/2}N^{2/k}].$$

Since $k - i \geq 2$, $k - i + 3 \geq 5$. It then follows from Lemmas 3.11 and 3.12 that $n - t_i^2 - t_{i-1}^2 - \ldots - t_1^2$ is a sum of $(k - i + 3)$ distinct elements of A_0. Therefore, if $t_i > t_{i-1}$, then n is the sum of (k+3) distinct elements of A, as $t_1 > (2 + \varepsilon)^{1/2}N^{2/k}$ and $t_j \in A$ for all $j = 1, \ldots, i$.

We now prove that $t_i > t_{i-1}$. By (3.8) - (3.11) we have

$$t_i > s_i^{1/2}N^{i/(2k)} - 1 > ((2 + \varepsilon)^{k-i} - 2)^{1/2}N^{i/(2k)} - 1 \geq$$
$$(((2 + \varepsilon)^{k-i} - 2)^{1/2} - \varepsilon)N^{i/(2k)}, \tag{3.7}$$

and

$$t_{i-1} \leq s_{i-1}^{1/2}N^{(i-1)/(2k)} \leq ((2 + \varepsilon)N^{1/k} - 1)^{1/2}N^{(i-1)/(2k)} < (2 + \varepsilon)^{1/2}N^{i/(2k)}. \tag{3.8}$$

If $k - i \geq 2$, then it is easily seen that $(2 + \varepsilon)^{k-i} - 2)^{1/2} - \varepsilon > (2 + \varepsilon)^{1/2}$ for $\varepsilon < (0.086)^2$, and the assertion follows from (3.14) and (3.15).

We now consider $k - i = 1$. This means $(2 + \varepsilon)N^{(k-1)/k} < n \leq N$. We consider the following two cases.

Case 1. $5N^{(k-1)/k} < n \leq N$. Put $s_{k-1} = [\frac{n}{N^{(k-1)/k}}] - 1$ and $t_{k-1} = [s_{k-1}^{1/2}N^{(k-1)/(2k)}]$. Then

$$4 \leq s_{k-1} \leq N^{1/k} - 1, \tag{3.9}$$
$$s_{k-1}^{1/2}N^{(k-1)/(2k)} - 1 < t_{k-1} \leq s_{k-1}^{1/2}N^{(k-1)/(2k)}, \tag{3.10}$$

and

$$(s_{k-1} + 1)N^{(k-1)/k} \leq n < (s_{k-1} + 2)N^{(k-1)/k}.$$

Thus we obtain as before that

$$N^{(k-1)/k} \leq n - t_{k-1}^2 < (2 + \varepsilon)N^{(k-1)/k}.$$

Letting $n_{k-1} = n - t_{k-1}^2$, then $n_{k-1} \in [N^{(k-1)/k},(2+\varepsilon)N^{(k-1)/k})$. Put $s_{k-2} = [\frac{n_{k-1}}{N^{(k-2)/k}}] - 1$ and $t_{k-2} = [s_{k-2}^{1/2}N^{(k-2)/(2k)}]$. We then have

$$N^{1/k} - 2 \le s_{k-2} \le (2+\varepsilon)N^{1/k} - 1, \tag{3.11}$$

$$s_{k-2}^{1/2}N^{(k-2)/(2k)} - 1 < t_{k-2} \le s_{k-2}^{1/2}N^{(k-2)/(2k)}, \tag{3.12}$$

and

$$(s_{k-2}+1)N^{(k-2)/k} \le n_{k-1} < (s_{k-2}+2)N^{(k-2)/k}.$$

Thus

$$N^{(k-2)/k} \le n_{k-1} - t_{k-2}^2 < (2+\varepsilon)N^{(k-2)/k}.$$

It follows from (3.16) - (3.19) that

$$t_{k-1} > s_{k-1}^{1/2}N^{(k-1)/(2k)} - 1 \ge 2N^{(k-1)/(2k)} - 1 \ge (2-\varepsilon)N^{(k-1)/(2k)},$$

and

$$t_{k-2} \le s_{k-2}^{1/2}N^{(k-2)/(2k)} \le ((2+\varepsilon)N^{1/k} - 1)^{1/2}N^{(k-2)/(2k)} < (2+\varepsilon)^{1/2}N^{(k-1)/(2k)}.$$

Clearly, $t_{k-1} > t_{k-2}$ as required.

Case 2. $(2+\varepsilon)N^{(k-1)/k} < n \le 5N^{(k-1)/k}$. We put here $s_{k-2} = [\frac{n}{N^{(k-2)/k}}] - 1$ and $t_{k-2} = [s_{k-2}^{1/2}N^{(k-2)/(2k)}]$. Then

$$(2+\varepsilon)N^{1/k} - 2 < s_{k-2} \le 5N^{1/k} - 1, \tag{3.13}$$

$$s_{k-2}^{1/2}N^{(k-2)/(2k)} - 1 < t_{k-2} \le s_{k-2}^{1/2}N^{(k-2)/(2k)}, \tag{3.14}$$

and

$$(s_{k-2}+1)N^{(k-2)/k} \le n < (s_{k-2}+2)N^{(k-2)/k}.$$

This implies that

$$N^{(k-2)/k} \le n - t_{k-2}^2 < (2+\varepsilon)N^{(k-2)/k}.$$

Let $n_{k-2} = n - t_{k-2}^2$. Then $n_{k-2} \in [N^{(k-2)/k},(2+\varepsilon)N^{(k-2)/k})$. Putting $s_{k-3} = [\frac{n_{k-2}}{N^{(k-3)/k}}] - 1$ and $t_{k-3} = [s_{k-3}^{1/2}N^{(k-3)/(2k)}]$, we then have

$$N^{1/k} - 2 \le s_{k-3} \le (2+\varepsilon)N^{1/k} - 1, \tag{3.15}$$

$$s_{k-3}^{1/2}N^{(k-3)/(2k)} - 1 < t_{k-3} \le s_{k-3}^{1/2}N^{(k-3)/(2k)}, \tag{3.16}$$

and

$$(s_{k-3} + 1)N^{(k-3)/k} \leq n_{k-2} < (s_{k-3} + 2)N^{(k-3)/k}.$$

Thus

$$N^{(k-3)/k} \leq n_{k-2} - t_{k-3}^2 < (2 + \varepsilon)N^{(k-3)/k}.$$

By (3.20) - (3.23) we obtain

$$t_{k-2} > s_{k-2}^{1/2}N^{(k-2)/(2k)} - 1 \geq ((2 + \varepsilon)N^{1/k} - 2)^{1/2}N^{(k-2)/(2k)} - 1$$
$$> 2^{1/2}N^{(k-1)/(2k)},$$

and

$$t_{k-3} \leq s_{k-3}^{1/2}N^{(k-3)/(2k)} \leq ((2 + \varepsilon)N^{1/k} - 1)^{1/2}N^{(k-3)/(2k)} < (2 + \varepsilon)^{1/2}N^{(k-2)/(2k)}.$$

Hence $t_{k-2} > t_{k-3}$. This completes the proof.

References

[1] Bateman P. T. and Purdy G. B., Every integer greater than 245 is the sum of five distinct squares of positive integers, Personal communication.

[2] Brown T. C., Erdös P., and Freedman A. R., Quasi-progressions and descending waves, J. Comb. Theory (Ser. A), 53 (1) (1990), 81-95.

[3] Brown T. C. and Freedman A. R., Arithmetic progressions in lacunary sets, Rocky Mountain J. Math., 17 (3) (1987), 587-596.

[4] Brown T. C. and Freedman A. R., Small sets which meet all the k(n)-term arithmetic progressions in the interval [1, n], J. Comb. Theory, 51 (2) (1989), 244-249.

[5] Brüdern J., Sums of squares and higher powers, J. London Math. Soc. (2) 35 (1987), 233-243.

[6] Brüdern J., Sums of squares and higher powers (II), J. London Math. Soc. 103 (1988), 27-33.

[7] Brüdern J., On Waring's problem for cubes and biquadrates, J. London Math. Soc., (2) 37 (1988), 25-42.

[8] Chalk J. H. H., On Hua's estimate for exponential sums, Mathematika 34 (2) (1987), 115 - 123.

[9] Chalk J. H. H., Some remarkes on polynomial congruences modulo p^{α}, C. R. Acad. Sci. Paris, 307 (1988), Série I, 513 - 515.

[10] Chen J. R., On the representation of a natural numbers as sum of terms of the form $x(x + 1) \ldots (x + k - 1)/k!$, Acta Math. Sinica, 9(1959), 264-270.

[11] Chen J. R., On Professor Hua's estimate of exponential sums, Sci. Sinica, 20 (6) (1977), 711-719.

[12] Choi S. L. G., Erdös P. and Nathanson M. B., Lagrange's theorem with $N^{1/3}$ squares, Proc. Amer. Math. Soc., 79 (1980) (2), 203 - 205.

[13] Ding P. & Qi M. G., On estimate of complete trigonometric sums, Chin. Ann. of Math., 6B (1) (1985), 109-120.

[14] Ding P. and Qi M. G., Further estimate of complete trigonometric sums, J. Tsinghua Univ. (29) (6) (1989), 74 - 85.

[15] Ding P., An improvement to Chalk's estimation of exponential sums, Acta Arith. LIX. 2 (1991), 149-155.

[16] Dubouis E., Solution of a problem of J. Tannery, Intermediaire Math., 18(1911), 55-56.

[17] Gogisvili G. P., The summation of a singular series that is connected with diagonal quadratic forms in 4 variables (in Russian; Georgian summary), Sakharth. SSR Mecn. Akad. Mat. Inst. Srom., 38(1970), 5-30.

[18] Grosswald E., Representations of integers as sums of squares, Springer-Verlag New York Inc., 1985.

[19] Halberstam H. and Richert H. E., *Sieve Methods*, Academic Press, New York, 1974.

[20] Halberstam H., Representation of integers as sums of a square, a positive cube, and a fourth power of a prime, J. London Math. Soc., 25 (1950), 158-168.

[21] Halberstam H., Representation of integers as sums of a square of a prime, a cube of a prime, and a cube, Proc. London Math. Soc., 52 (2) (1951), 455-466.

[22] Halberstam H., On the representation of large numbers as sums of squares, higher powers, and primes, Proc. London Math. Soc., 53 (2) (1951), 363-380.

[23] Hooley C., On a new approach to various problems of Waring's type, in Recent Progress in Analytic Number Theory, Vol. 1, Academic Press, London 1981, 127-191.

[24] Hooley C., On Waring's problem, Acta Math., 157 (1986), 49-97.

[25] Hua L. K., On an exponential sums, J. Chinese Math. Soc., 2 (1940), 301-312.

[26] Hua L. K., *Additive theory of prime numbers*, AMS Providence, R.I., 1965.

[27] Landau E., Handbuch der Lehre von der Verteilung der Primzahlen, Teubner, Leipzig, 1909.

[28] Linnik Yu.V., An elementary solution of a problem of Waring by Schnirelmann's method, Mat. Sbornik, 12 (54) (1943), 225 - 230.

[29] Loxton J. H. and Vaughan R. C., The estimation of complete exponential sums, Canad. Math. Bull. 28 (1985), 440 - 454.

[30] Lu M. G., On a note of complete trigonometric sums, Acta Math. Sinica, 27 (1984), 817-823. (Chinese)

[31] Lu M. G., Estimate of a complete trigonometric sum, Sci. Sinica (Ser. A), 28(6)(1985), 561-578.

[32] Lu M. G., On a problem of sums of mixed powers, Acta Arith. LVIII.1 (1991), 89-102.

[33] Nathanson M. B., Waring's problem for sets of density zero, Analytic Number Theory, Lecture Notes in Math. 899, 301 - 310.

[34] Necheav V. I., On the representation of natural numbers as a sum of terms of the form $(x(x + 1) \dots (x + n - 1))/n!$, Izv. Akad. Nauk SSSR, Ser. Mat. 17 (1953), 485-498. (Russian)

[35] Necheav V. I., An estimate of a complete rational trigonometric sum, Mat. Zametki, 17 (1975), 839-849; English transl. in Math. Notes, 17(1975).

[36] Necheav V. I. and Topunov V. L. An estimate of the modulus of complete rational trigonometric sums of degree three and four, Proc. Steklov Inst. of Math., (1983) (Issue 4), 135-140.

[37] Ribenboim P., *The book of prime number records*, Second edition, Springer-Verlag, New York, 1989.

[38] Rosser J. B. and Schoenfeld L., Approximate formulas for some functions of prime numbers, Illinois J. Math., 6 (1962), 64-94.

[39] Rosser J. B. and Schoenfeld L., Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, Math. Comp., 29 (1975), 243-269.

[40] Schmidt W. M., On cubic polynomials I. Hua's estimate of exponential sums, Mh. Math., 93 (1982), 63-74.

[41] Stechin S. B., Estimate of a complete rational trigonometric sum, Proc. Steklov Inst. of Math., (1980) (Issue 1), 201-220; 143 (1977), 188-207 (Russian).

[42] Vaughan R. C., *The Hardy-Littlewood method* (University Press, Cambridge, 1981).

[43] Vaughan R. C., Sums of three cubes, J. Reine Ange. Math., 365 (1986), 122-170.

[44] Vaughan R. C., A new iterative method in Waring's problem, Acta Math. 162 (1989), 1 - 71.

[45] Vaughan, R. C., and Wooley T. D., On Waring's problem: some refinements, Proc. London Math. Soc., (3) 63 (1991), 35 - 68.

[46] Weil A., On some exponential sums, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204 -207.

[47] Wieferich, A., Beweis des Satzes, dass sich eine jede ganze Zahl als Summe von hochsten neun positiven Kuben darstellen lasst, Math. Ann., 66 (1909), 95 - 101.

[48] Wooley T. D., Large improvements in Waring's problem, Ann. of Math., 135 (1992), 131-164.