SEQUENCES OF POSITIVE INTEGERS CONTAINING NO k-TERM ARITHMETIC PROGRESSIONS AND SMOOTH NUMBERS IN SHORT INTERVALS

GOUTAM PAL

INDIAN STATISTICAL INSTITUTE, KOLKATA
2009

SEQUENCES OF POSITIVE INTEGERS CONTAINING NO k-TERM ARITHMETIC PROGRESSIONS AND SMOOTH NUMBERS IN SHORT INTERVALS

GOUTAM PAL

Thesis submitted to the Indian Statistical Institute
in partial fulfilment of the requirements
for the award of the degree of
Doctor of Philosophy.
2009

Indian Statistical Institute
203, B.T. Road, Kolkata, India.

TO THE WORKING PEOPLE OF THE WORLD

Acknowledgements

My thesis is the outcome of my little knowledge of Mathematics which I have learnt from different teachers starting from my school days. I still remember them. At this pleasant moment I would like to recall my beloved teachers.

At first I offer my special thanks to my parents who were always with me and encouraged me to complete this works.

I would like to thank my primary school teacher late Satyajit Sir who taught me Arithmetic in school.

I am thankful to my beloved teacher Mr. Tapan Dutta who taught me Arithmetic and School Algebra.

I would like to thank my beloved teacher Mr. Utpal Nag who taught me School Geometry and School Algebra.

I would like to thank my beloved teachers Mr. Gopal Sandillo and Mr. Bijoy Patra who taught me Geometry and Trigonometry in school.

I am thankful to Prof. S. Mahato who taught me Dynamics, Statics, Differential Equations, Astronomy and Linear Programming during my college days.

I am deeply grateful to my beloved teacher Prof. Shamik Ghosh who taught me Higher Algebra and Real Analysis during my college days. He used to encourage us very much. I have got inspiration to do Mathematics from him.

I extend my sincere thanks to my beloved teachers Prof. Sreedhar Inamdar, Prof. N. S. N. Sastry, Prof. A. B. Raha, Prof. G. Misra, Prof. V. R. Padmawar, Prof. Mohan. Delampady, Prof. B. Rajeev, Prof. K. Ramamurty, Prof. Arup Bose, Prof. J. K. Ghosh, Prof. K. P. S. Bhakar Rao, Prof. Rajaram Bhat who taught me Mathematics and Statistics during my postgraduate studies.

I would like to express my sincere thanks to my beloved teacher Prof. C. R. Pradeep who taught me Algebra of Finite Fields.

I would like to thank Prof. Bhaskar Bagchi who taught me Linear Algebra, Finite Geometry and Complex Analysis. He has been and continues to be a great inspiration for me. I am grateful to him for suggesting one of my research problems "On sequence of positive integers containing no k terms in Arithmetic Progressions" and for several important and useful discussions with him.

I am grateful to Dr. Lianagapan Li for his valuable suggestions on the Graham's conjecture and for the interesting communications I had with him.

I would like to thank Prof. R. Balasubramanian for suggesting the other problem of my thesis on "Smooth Numbers in Short Intervals" and also for several interesting and useful discussions.

I offer special thanks to my beloved teacher Prof. V. R. Padmawar who has always helped me in my difficult times.

My deepest gratitude to my beloved teacher Prof. G. Misra for helping me in my difficult times and for agreeing to be the thesis supervisor. Without his help, this thesis could not have been completed.

I would like to thank Prof. S. C. Bagchi and Prof. Rudra Sarkar for their encouragements.

I am thankful to my senior Dr. Ashish Upaddhya for helping me in many ways.

I would like to thank my friends Dr. Satadal Ganguly, Dr. Arijit Dey, Mr. George Scaria, Mr. Subrata Shyam Roy, Mr. Narendra Nath Sarkar, Mr. Abhijit Mukherjee and Mr. Sanjoy Pusti for their encourangments and their technical help in preparing this thesis.

I offer special thanks to Prof. Anirban Mukhopadhyay and Dr. Satadal Ganguly for getting the opportunity to work with them. They are the co-authors of the paper "Smooth Numbers in Short Intervals" which grew out of one of the problems considered in this thesis.

I would like to thank Dr. Jaya Deb Roy, the principal of our college RCC Institute of Information Technology, Calcutta, for her encouragement and support.

I am thankful to my student Mr. Soumyadeep Chaudhuri for his support and encouragement.

I would like to thank Prof. Alok Goswami, the Convener, Ph.D. and D.Sc. Committee, I. S. I. , Calcutta, for his advice and encouragement.

Finally, I would like to thank all the faculties and members of the nonacademic staff in Indian Statistical Institute, Bangalore, Indian Institute of Sciences, Bangalore and Institute of Mathematical Sciences, Chennai, the institutions where much of the work presented here has been carried out, for creating excellent conditions for work.

Contents

Chapter 0

Introduction

In my thesis I have worked on two problems:

1. On sequences of positive integers containing no k terms in arithmetic progressions.

2. On smooth numbers in short intervals.

The first two chapters of my thesis deal with the first problem and in the rest of the thesis I have focused on the 2nd problem.

In the first chapter of my thesis I have considered the function $r_k(N)$ for a fixed $k \geq 3$, where, by definition, $r_k(N)$ is the cardinality of a maximal subset of N consecutive natural numbers with the property that no k terms of it are in an Arithmetic Progression (A. P.). Obtaining 'good' estimates for $r_k(N)$ for sufficiently large N is one of the most challenging problems in this area. In section 2 of this chapter, I have listed some results on the lower and upper bounds of $r_k(N)$. Rankin's theorem is the best known result on the lower bound of $r_k(N)$ and Szemerédi's theorem is the best known result on the upper bound of $r_k(N)$. I have presented proofs of many known results on lower bounds of $r_k(N)$ in section 3. In particular I have presented a result which is a little weaker than Rankin's theorem for $k = 3$. I have used this result in chapter 2 to work on our problem. In section 4 of this chapter, I have presented the proofs of many known results on the upper bounds of $r_k(N)$. In particular, I have sketched the proof of Szemerédi's theorem for $k = 3$. I could not access the proof of theorem 1.4.4 of chapter 1. The proof that I have given is my own.

Szemerédi's theorem is a consequence of Erdös conjecture on sequences of positive integers containing no k terms in an A. P. I have shown this fact in Corollary 2.2.6 of chapter 2. In Chapter 2, I have assumed the conjecture of Erdös and obtained a very strong consequence from it.

This famous conjecture of Erdös asserts that if A is a subset of the set of all

positive integers having the property that $\sum_{a\in A}\frac{1}{a}=\infty$, then A must contain arithmetic progressions of arbitrary length. A special case of the conjecture, when A is the set of prime numbers, was proved by Green and Tao [GT08]. The conjecture implies that if a subset A of the set of positive integers contains no arithmetic progression of length k, where $k\geq 3$ is a fixed integer, then the sum $\sum_{a\in A}\frac{1}{a}$ must converge. One may ask whether the above sum can be arbitrarily large as the sets A vary. Our first theorem of this chapter answers the question in the negative.

Joseph L. Gerver [Ger77] considered the set S_p, given by the sequence $\{a_n\}$, where $a_1=1$ and for $n\geq 1$, a_{n+1} is the smallest positive integer bigger than a_n such that no p elements of $a_1, a_2, \cdots, a_{n+1}$ lie in arithmetic progression. He guessed in that paper that for any prime p, the set S_p may indeed maximize the sum of the reciprocals of the elements of a set of positive integers having no p terms in arithmetic progression. On the other hand Joseph L. Gerver and L.Thomas Ramsey [GR79] showed heuristically that the set S_p does not maximize the above sum for the composite p. A corollary to our second theorem in this chapter says that the Erdös conjecture implies the existence of a set of positive integers containing no p terms in arithmetic progression which maximizes the above sum. That is, not only the sum of reciprocals is bounded above, the supremum of the sums is actually achieved! This is the main result of section 2 in this chapter. The result is consequence of the fact that a continuous function on a compact space achieves its supremum.

In section 3 of this chapter, we have shown that, contrary to Gerver's speculation, the above greedy algorithm does not produce the sequence that maximizes the sum by showing the existence of a 'better' sequence. This is where Rankin's theorem has been used. In section 4 of this chapter, we have considered Graham's conjecture, a multidimensional version of the Erdös conjecture. In this section we have proved theorems analogous to those in section 2.

The last three chapters deal with the second problem. In chapter 3, I have presented some preliminary results on the topics on distribution of smooth numbers. A positive integer n is called y-smooth if all the prime factors p of n are smaller than or equal to y. An important problem is to count y-smooth numbers up to x. This number is denoted by $\Psi(x,y)$. Smooth numbers have applications to both theoretical and applicable parts of number theory. For example, Lenstra's celebrated method of factoring large integers using elliptic curves relies in a crucial way on the existence of smooth numbers in short intervals. In this context, a well-known conjecture (see, for example [Gra00] , [FG93]) predicts that there exist,

for any $\alpha > 0$, X^α-smooth numbers in intervals $(X, X + \sqrt{X}]$ for all sufficiently large X. This is the problem I have worked on. In Chapter 5, we present a proof of this conjecture under an assumption weaker than the Lindelöf hypothesis. In fact we can take the interval to be a little bit shorter than $\sqrt{X}$.

In section 2 of chapter 3, we have obtained bounds for $\Psi(x, y)$ with several known methods: Elementary Combinatorics Method, Geometric (Lattice Points) Method, Rankin's Upper Bound Method, Using Functional Equation: Buchstab Identity, Hildebrand Identity, The Saddle point Method etc. These methods give the following asymptotic result $\Psi(x, y) \sim \rho(u)x$, $u = \frac{\log X}{\log Y}$, (in a wider range of x, y) where $\rho(u)$ is a function of u. This function is called Dickman ρ-function. In section 3 of this chapter, we have studied the Dickman function ρ. In section 4, we have listed some known results on smooth numbers in short intervals.

To work further on smooth numbers in short intervals we have applied the ζ function technique initiated by Balog [Balo87] and continued, among others, by Xuan [Xuan99]. Outcome of this method depends on bounds of the particular Dirichlet series we are using (in our case, the Riemann zeta function). Thus, in chapter 4, we have been led to study the Riemann ζ function in the critical strip. I have been unable to improve upon the best known result unconditionally but various improvements have been obtained under several widely believed hypotheses. While studying the ζ function, I found some results on the distribution of the non-trivial zeros of ζ function and the bounds of ζ and $\frac{\zeta'}{\zeta}$ near the critical line under different hypotheses that I could not locate in the literature. We have calculated number of zeros of the ζ function on the critical line in the intervals $(T, T + f(T)]$, where $f(T) = \frac{1}{\log\log T}$ or $\frac{1}{\log T}$, under the Riemann Hypothesis and the Montgomery conjecture. Using these results we have got bounds of $\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}$ uniformly for $1/2 + \frac{1}{\log\log t} \leq \sigma \leq \sigma_1 < 1$ and $1/2 + \frac{1}{\log t} \leq \sigma \leq \sigma_1 < 1$ respectively. We have also proved some results on the bounds of the ζ function on the line $\sigma = 1/2$ in section 2 of chapter 5. In chapter 5, we have also given a brief description of Lenstra's elliptic curve method of factoring large integers which is an important application of the conjecture mentioned above.

Finally we have proved our main theorem under an assumption weaker than the Lindelöf Hypothesis : If $\zeta(1/2 + it) \ll t^{\alpha/2+o(1)}$ then there is a X^α-smooth number in the interval $(X, X + (\log X)^{-1/2+o(1)}\sqrt{X}]$ for all sufficiently large X.

Chapter 1

Sequences of positive integers containing no k terms in an A. P. I

1.1 Introduction.

In 1926, B.L. van der Waerden [Wae28] proved the following wonderful theorem: *If the set of all integers is partitioned into two classes then at least one class contains arbitrarily long arithmetic progressions.* It is obvious that neither class must contain an infinite arithmetic progression. In fact, It is easy to see that for any sequence $\{a_n\}$ there is another sequence $\{b_n\}$, with $b_n \geq a_n$, which contains no arithmetic progression of three terms, but which intersects every infinite arithmetic progression. The finite form of van der Waerden's theorem goes as follows : *Let l be a positive integer. Then for each positive integer n, there exists a least positive integer $f(n,l)$ with the property that if the integers from* 1 *to $f(n,l)$ are partitioned into l classes, then at least one class contains an arithmetic progression of n terms.* For a short proof, see the note of Graham and Rothschild [GR74]. However, the best upper bound on $f(n,l)$ known at present is extremely poor. The best lower bound known, due to Berklemp [Ber68], asserts that $f(n) \doteq f(n,3) > n2^n$, which improves previous results of Erdös, Rado and W. Schmidt.

In 1936, Erdös and Turán [ET36] considered the quantity $r_k(N)$, defined to be the maximum number of positive integers not exceeding N containing no k terms in arithmetic progression. They were led to the investigation of $r_k(N)$ by several problems. First of all the problem of estimating $r_k(N)$ is by itself interesting. Secondly, a good upper bound on $r_k(N)$ will improve the poor upper bound on

$f(n,l)$. Finally, the estimate $r_k(N) < \pi(N)$ will imply a famous conjecture (now a theorem due to B. Green and T. Tao [GT08]) in number theory that says *there are arbitrarily long arithmetic progressions of prime numbers.* This conjecture is a particular case of a conjecture of Erdös [UL75]: *If the sum of the reciprocals of a set of positive integers is infinite then it contains arbitrarily long arithmetic progressions.*

The problem of finding the bounds of $r_k(N)$ for all $k \geq 3$ or for some specific values of k have been studied by several authors. Clearly the case $k = 2$ is quite trivial. In this chapter we shall study some of those bounds on $r_k(N)$. Let us denote $r_3(N)$ by $r(N)$. We define the size(k) of the set of positive integers not exceeding N by $r_k(N)$. Notice that the size(k) of an arithmetic progression with N terms is also $r_k(N)$.

1.2 Results on bounds of size functions.

In this section we shall discuss the known results on the bounds of the size functions. We shall prove some of these results in the next two sections.

G. Szekeres conjectured that $r\{(3^n+1)/2\} = 2^n$ and this was proved [ET36] for $n < 5$. This will imply

$$r(N) < cN^{\frac{\log 2}{\log 3}}$$

for some fixed $c > 0$.

More generally, he conjectured that for any n and for any prime p,

$$r_p\left(\frac{(p-2)p^n+1}{p-1}\right) = (p-1)^n.$$

An immediate consequence of this conjecture will be that for every n, there is an infinity of n combinations of primes forming an arithmetic progression. That is there are infinitely many arithmetic progressions of primes of arbitrary length.

Moreover, it will give a new proof of van der Waerden's theorem with the better upper bound for $f(n,l)$ in any of the previous proofs, viz,

$$f(n,l) < n^{cn\log l}.$$

But this conjecture was proved to be false by Salem and Spencer [SS42] who

showed that for every $\varepsilon > 0$ and sufficiently large N,

$$r(N) > N^{1-\frac{(\log 2+\varepsilon)}{\log\log N}}. \tag{1.2.1}$$

This upper bound of $r(N)$ was improved by Behrend [Beh46] who proved that for every $\varepsilon > 0$ and sufficiently large N,

$$r(N) > N^{1-\frac{(2\sqrt{2\log 2}+\varepsilon)}{\sqrt{\log N}}}. \tag{1.2.2}$$

We shall prove both these results in the next section.

For $k \geq 3$ let A_k be a set of positive integers no k terms of which are in an arithmetical progression. In the foregoing discussion, let us denote A_3 by A.

In Behrend's method, the set A depends upon N, i.e., the set used for $N = 10000$ might be quite different from that for $N = 10001, 10002$ etc.. Moreover the argument in Behrend's method makes use of the pigeonhole principle and hence is not constructive. Moser [Mos53] constructed an infinite sequence with no three terms in an arithmetic progression, and which yields, for N sufficiently large,

$$r(N) > N^{1-\frac{c}{\sqrt{\log N}}} \tag{1.2.3}$$

where $c > 0$ is a fixed constant. Rankin [Ran60] constructed sets of positive integers no k terms of which are in an arithmetic progression, and which gives, for every $\varepsilon > 0$, and for N sufficiently large,

$$r_k(N) > N \exp\{-c(1+\varepsilon)(\log N)^{\frac{1}{1+\log k}}\} \tag{1.2.4}$$

for some $c > 0$. This improves Behrend's corresponding inequalities for $k > 4$.

In the other direction, in 1936, P. Erdös and P. Turán [ET36] proved, if $N \geq 8$,

$$r(2N) \leq N. \tag{1.2.5}$$

They also noted that the result is true for $N = 4$, 5, 6, but not for $N = 7$ as no three terms of 1, 2, 4, 5, 10, 11, 13, 14 are in arithmetic progression and hence $r(14) = 8 > 7$. In the same paper they improved it by proving that for each $\varepsilon > 0$ there exists a positive integer $N_0(\varepsilon)$ such that

$$r(N) < (\frac{4}{9} + \varepsilon)N, \tag{1.2.6}$$

for all $N \geq N_0(\varepsilon)$. In the same paper they again improved this result to

$$r(N) < (\frac{3}{8} + \varepsilon)N, \tag{1.2.7}$$

for all $\varepsilon > 0$ and $N > N_0(\varepsilon)$ and made the following conjecture:

$$r(N) = o(N), \tag{1.2.8}$$

as $N \to \infty$.

The notation $f(x) = o(g(x))$ as $x \to a$, for finite a (resp. as $x \to \infty$ or $-\infty$) means $\frac{f(x)}{g(x)} \to 0$ as $x \to a$ (resp. as $x \to \infty$ or $-\infty$).

In 1953, Leo Moser [Mos53] proved that, for all $N \geq 1$,

$$r(N) < \frac{2}{5}N + 3. \tag{1.2.9}$$

In the same paper he also proved with little complicated combinatorial arguments that, for all $N \geq 1$,

$$r(N) < \frac{4}{11}N + 5. \tag{1.2.10}$$

We shall sketch the proofs of some of these results in section 4.

P. Erdös and P.Turán [ET36] observed, for $k \geq 3$

$$r_k(M + N) \leq r_k(M) + r_k(N) \tag{1.2.11}$$

from which it follows by a simple argument that

$$\lim_{N \to \infty} \frac{r_k(N)}{N} = c_k \tag{1.2.12}$$

exists. Erdös and Turán conjectured [ET36] that $c_k = 0$ for all $k \geq 3$. In 1938 Behrend [Beh38] proved that either $c_k = 0$ for all k, or $\lim_{k \to \infty} c_k = 1$.

The first satisfactory upper bound for $r(N)$ was due to K. F. Roth [Rot53] who proved the conjecture (1.2.8) by proving that

$$r(N) = O(\frac{N}{\log \log N}). \tag{1.2.13}$$

The notation $f(x) = O(g(x))$ or $f(x) \ll g(x)$ as $x \to a$ (resp. $x \to \infty$) means that there is a constant $c > 0$ such that $|f(x)| \leq c|g(x)|$ for all x in an open interval containing a (resp. for all sufficiently large positive x).

In 1967, E. Szemerédi [Sze68] proved that $c_4 = 0$ i.e. $r_4(N) = o(N)$. The

proof used the general theorem of van der Waerden. K. F. Roth [Rot70, Rot72] later gave an analytic proof for the result $r_4(N) = o(N)$ in which he did not use van der Waerden's theorem.

Finally in 1975, E. Szemerédi [Sze75] proved that $r_k(N) = o(N)$ for which he used deep combinatorial results such as Szemerédi's uniformity lemma. In 1998, Gowers [Gow98, Gow01] extended the Fourier-analytic style of Roth's argument to $k = 4$, and then finally in 2001, to all k.

We shall sketch only the proof of the result $r(N) = o(N)$ due to Roth in section 4 and we refer to the original papers for the details of the proofs.

1.3 Results on lower bounds of size functions.

In this section we shall prove some known results on the lower bounds of the size functions discussed in the previous section.

First we prove the lower bound on $r(N)$ due to Salem and Spencer [SS42].

Theorem 1.3.1. *For every $\varepsilon > 0$, there is a positive integer $N_0(\varepsilon)$ such that*

$$r(N) > N^{1-\frac{\log 2+\varepsilon}{\log\log N}}$$

for all $N > N_0$.

Proof. Let $d \geq 3$ be an integer and n be another integer divisible by d. Let $S(d, n)$ be the set of all integers of the form

$$A = a_0 + a_1(2d-1) + a_2(2d-1)^2 + \cdots + a_{n-1}(2d-1)^{n-1}$$

where the "coefficients" a_i are integers with the condition that exactly n/d coefficients are equal to 0, exactly n/d coefficients are equal to 1, exactly n/d coefficients are equal to 2, etc. ..., and exactly n/d coefficients are equal to $d-1$. Thus all the integers in $S(d, n)$ are distinct and

$$\#\left(S(d,n)\right) = \frac{n!}{(n/d)!}. \tag{1.3.1}$$

Here $\#(S)$ denotes the number of elements of the set S. Also, for all $A \in S(d, n)$ we have

$$A < (2d-1)^n. \tag{1.3.2}$$

First we shall prove that no three elements of $S(d,n)$ are in an arithmetic progression. Suppose that $A, B, C \in S(d,n)$ and that $A + C = 2B$. Let a_i, b_i, c_i be the coefficients of $(2d-1)^i$ in the $(2d-1)$-ary expansions of A, B, C respectively. We shall prove that $a_i = c_i = b_i$ for all i. Since $a_i + c_i \leq 2d-2$ and $2b_i \leq 2d-2$, the equality $A+C = 2B$ implies $a_i + c_i = 2b_i$ for all $i = 0, 1, \ldots, n-1$. We shall prove by induction on m, $0 \leq m \leq d-1$, that the n/d coefficients equal to m occupy the same places in A, B and C. This will prove that $A = B = C$. Now there are in B exactly n/d coefficients equal to 0, and if $b_k = 0$ then $a_k = c_k = 0$; i.e., the n/d coefficients equal to 0 occupy the same places in A, C and B. Next there are, in B, exactly n/d coefficients equal to 1, and if $b_l = 1$, then as $a_l \neq 0$ and $c_l \neq 0$, the equality $a_l + c_l = 2b_l$ implies $a_l = c_l = 1 = b_l$; i.e., n/d coefficients equal to 1 occupy the same places in A, C, B. Therefore, the result is true for $m = 0, 1$. This is the base case of the induction. Let us assume the result for some $m-1$, $1 \leq m \leq d-1$. Now if $b_h = m$ and a_h, c_h are different from $0, 1, \cdots, m-1$, then $a_h = c_h = m = b_h$ as $a_h + c_h = 2b_h$. Hence the n/d coefficients equal to m occupy the same places in A, B and C. This completes the induction and we have proved that A=B=C. This proves that no three distinct elements of $S(d,n)$ in arithmetic progression.

Now if n and n/d are large enough, then by (1.3.1) and using the Stirling's formula, we have,

$$\#\left(S(d,n)\right) > \frac{n^n\sqrt{2\pi n}e^{-n}}{[(n/d)^{n/d}\sqrt{2\pi(n/d)}e^{-n/d}]^d}\frac{1}{K^d},$$

K being a constant (as close to 1 as we want). Therefore,

$$\#\left(S(d,n)\right) > (d/\theta n)^{d/2}d^n, \tag{1.3.3}$$

θ being a constant (as close to 2π as we want).

Let us now fix an N and let us choose d such that

$$(2d-1)^{d\omega(d)} \leq N < (2d+1)^{(d+1)\omega(d+1)}, \tag{1.3.4}$$

where $\omega(d)$ is an integer increasing to infinity with d such that $\frac{\omega(d)}{\log d} \to \infty$ but $\frac{\log \omega(d)}{\log d} \to 0$ as $d \to \infty$. For example, we may take $\omega(d) = [(\log d)(\log\log d)]$. (Here and in what follows, by $[x]$ we mean the largest integer $\leq x$). Now we

construct the set $S(d,n)$ with $n = d\omega(d)$. We have by (1.3.2), (1.3.3) and (1.3.4)

$$r(N) \geq r[(2d-1)^{d\omega(d)}] \geq \#\left(S(d,n)\right) > \left(\frac{1}{\theta\omega(d)}\right)^{d/2} d^{d\omega(d)}.$$

Therefore,

$$\frac{r(N)}{N} > \left(\frac{1}{\theta\omega(d)}\right)^{d/2} \frac{d^{d\omega(d)}}{(2d+1)^{(d+1)\omega(d+1)}}.$$

Now, as $N \to \infty$, $d \to \infty$, and

$$\log\left(\frac{N}{r(N)}\right) < (d+1)\omega(d+1)\log(2d+1) - d\omega(d)\log(d) + \frac{d}{2}\log\omega(d) + \frac{d}{2}\log\theta = d\omega(d)[\log 2 + o(1)], \tag{1.3.5}$$

if we assume, as in our example, $\omega(d)$ increases regularly enough to have $\omega(d+1) - \omega(d) = o(1)$. By (1.3.4)

$$\begin{aligned} \log N &\geq d\omega(d)\log(2d-1) \\ \log\log N &< \log(d+1) + \log\omega(d+1) + \log\log(2d+1) \end{aligned}$$

and so

$$\frac{\log N}{\log\log N} > d\omega(d)[1 + o(1)]. \tag{1.3.6}$$

Now, by (1.3.5) and (1.3.6), it follows that, as $N \to \infty$

$$r(N) > N^{1-\frac{\log 2+\varepsilon}{\log\log N}}$$

for every $\varepsilon > 0$ which proves the theorem. □

Now we shall prove a theorem which gives a better lower bound for $r(N)$. This is due to F. A. Behrend [Beh46].

Theorem 1.3.2. *For each $\varepsilon > 0$ there is a positive integer $N_0(\varepsilon)$ such that*

$$r(N) > N^{1-\frac{2\sqrt{2\log 2}+\varepsilon}{\sqrt{\log N}}}$$

for all $N \geq N_0(\varepsilon)$.

Proof. The main idea behind Behrend's proof is that in any Euclidean space $\mathbb{R}^d$, a sphere $\{x \in \mathbb{R}^d : \|x\| = r\}$ cannot contain a proper arithmetic progression of

length 3. For $d \geq 2$, $n \geq 2$ and $k \leq n(d-1)^2$ consider the set $S_k(d,n)$ of all numbers of the form

$$A = a_0 + a_1(2d-1) + a_2(2d-1)^2 + \cdots + a_{n-1}(2d-1)^{n-1}$$

where the coefficients a_i are integers subject to the following conditions

$$0 \leq a_i < d. \tag{1.3.7}$$

$$(normA)^2 = k \tag{1.3.8}$$

where

$$normA = \sqrt{a_0^2 + a_1^2 + \cdots + a_{n-1}^2}.$$

Therefore, this is a subset of an n dimensional sphere. Let us prove that no three members of this set are in arithmetical progression. Suppose A, B, C are in this set and $A + C = 2B$. Therefore $normA = normB = normC$. Also,

$$norm(A+C) = norm(2B) = 2\sqrt{k}$$

and

$$normA + normC = 2\sqrt{k}.$$

Thus, the triangle inequality

$$norm(A+C) \leq normA + normC$$

is actually an equality. This is only possible if $(a_0, a_1, \ldots, a_{n-1})$ and $(c_0, c_1, \ldots, c_{n-1})$ are proportional and in fact, since their norms are equal, identical, i.e., if $A = C = B$. There are d^n different systems $(a_0, a_1, \ldots, a_{n-1})$ satisfying (1.3.7) and $n(d-1)^2 + 1$ possible values of k; hence for some k, $S_k(d,n)$ must contain at least

$$\frac{d^n}{n(d-1)^2+1} > \frac{d^{n-2}}{n}$$

terms; since all these terms are $< (2d-1)^n$ we have

$$r((2d-1)^n) > \frac{d^{n-2}}{n}.$$

Now let N be given; choose $n = \left[\sqrt{\frac{2\log N}{\log 2}}\right]$, and d such that

$$(2d-1)^n \leq N < (2d+1)^n.$$

Here for x, a real number, $[x]$ is the greatest integer $\leq x$. Thus,

$$r(N) \geq r((2d-1)^n) > \frac{d^{n-2}}{n} > \frac{(N^{1/n}-1)^{n-2}}{n2^{n-2}} = \frac{N^{1-2/n}}{n2^{n-2}}(1-N^{-1/n})^{n-2},$$

and for all sufficiently large N,

$$r(N) > \frac{N^{1-2/n}}{n2^{n-2}} = N^{1-\frac{2}{n}-\frac{\log n}{\log N}-\frac{(n-1)\log 2}{\log N}} > N^{1-\frac{2\sqrt{2\log 2}+\varepsilon}{\sqrt{\log N}}}$$

for any $\varepsilon > 0$. This proves the theorem. □

Now let us describe the Leo Moser construction [Mos53].

Theorem 1.3.3. *We can construct an infinite sequence R, no three of which are in an arithmetical progression, and if $r^*(N)$ denotes number of elements in R not exceeding N, then*

$$r^*(N) > N^{1-\frac{c}{\sqrt{\log N}}}$$

for some $c > 0$.

Proof. Given a positive integer x, written in denary (i.e., expanded in base 10) form, we enclose x in a set of parentheses, putting the first digit (counting from the right to the left) in the first parenthesis, the next two digits in the next one, the next three digits in the one after that, and so on. If the last non-empty parenthesis (the one farthest to the left which does not consist entirely of zeros) does not have a maximal number of digits, we fill it with zeros. For example, we write the number $A = 125270890123400$ as $A = (12527)(0890)(123)(40)(0)$.

Now suppose that the rth parenthesis in x contains non-zero digits, but all further parentheses to the left contain zeros. Let x_i be the number represented by the digits in the ith parenthesis, for $i = 1, 2, \ldots, r-2$. Further, let $\overline{x}$ be the number represented by the digits in the last two parentheses of x taken together, but excluding the last digit. In our example, $A_1 = 0, A_2 = 40, A_3 = 123, A_4 = 0890, A_5 = 12527$ and $\overline{A} = 25270890$. Now our R consists a number x if it satisfies the following conditions:

1. The last digit of x must be 1.

2. x_i must begin with 0 for $i = 1, 2, \ldots, r-2$.

3. We must have

$$\sum_{i=1}^{r-2} x_i^2 = \overline{x}.$$

Let us first prove that no three terms of R are in arithmetical progression. Note that if two elements of R have different number of non-empty parentheses then their arithmetic mean cannot satisfy condition 1 and hence cannot be in R. Thus we need to consider two elements x, y in R having the same number of parentheses. We shall prove that $z = \frac{x+y}{2}$ is not in R by showing that z does not satisfy condition 3. Since x, y are in R,

$$\overline{z} = \frac{\overline{x} + \overline{y}}{2} = \sum_{i=1}^{r-2} \frac{x_i^2 + y_i^2}{2}.$$

On the other hand z is in R implies

$$\overline{z} = \sum_{i=1}^{r-2} z_i^2 = \sum_{i=1}^{r-2} (\frac{x_i + y_i}{2})^2.$$

Hence if z is in R then

$$\sum_{i=1}^{r-2} \frac{x_i^2 + y_i^2}{2} = \sum_{i=1}^{r-2} (\frac{x_i + y_i}{2})^2.$$

Thus

$$\sum_{i=1}^{r-2} (\frac{x_i - y_i}{2})^2 = 0,$$

which implies $x_i = y_i$ for $i = 1, 2, \ldots, r-2$. This together with condition 1 implies that x and y are not distinct.

We now estimate how many integers in R contain exactly r parentheses. Among the r parentheses, we can make the first digit in each of first $(r-2)$ parentheses 0. We then fill up the first $(r-2)$ parentheses arbitrarily. This can be done in

$$10^{0+1+2+\cdots+(r-3)} = 10^{\frac{1}{2}(r-2)(r-3)}$$

ways. The last two parentheses can then be filled up in such way as to satisfy conditions (1) and (3). In this case we only need to check that the last two parentheses should not be overfilled, and that the last digit, which we set equal to 1, is not interfered with. This follows from the fact that we have $2r-2$ choices in the last two parentheses other than the last digit and the sum of squares of the numbers in the first $(r-2)$ parentheses satisfies

$$\leq (10^1)^2 + (10^2)^2 + \cdots + (10^{r-2})^2 < 10^{2r-2}.$$

Now for a given N let r be the positive integer such that

$$10^{\frac{1}{2}r(r+1)} \leq N < 10^{\frac{1}{2}(r+1)(r+2)}. \tag{1.3.9}$$

Since all the integers with at most r parentheses will not exceed N, and since r parentheses can be filled up at least $10^{\frac{1}{2}(r-2)(r-3)}$ ways, we have, by the right-hand inequality in (1.3.9),

$$r^*(N) \geq 10^{\frac{1}{2}(r-2)(r-3)} > 10^{\log N - 9\sqrt{2\log N}} > N^{1-c/\sqrt{logN}}.$$

This proves the theorem. □

In 1961, R. A. Rankin [Ran60] found a lower bound for $r_k(N)$ for sufficiently large N. We get Behrend's result as a particular case of this result for $k = 3$. We note that if no three terms of a set A of positive integers are in arithmetical progression then no $k \geq 3$ terms of the set A are in arithmetical progression. Hence, for every $\varepsilon > 0$ and for some positive integer $N_0(\varepsilon)$, we have

$$\begin{aligned} r_k(N) \geq r(N) &> N^{1-\frac{2\sqrt{2\log 2}+\varepsilon}{\sqrt{\log N}}} \\ &> N\exp\{-2(2\log 2)^{\frac{1}{2}}(1+\varepsilon)(\log N)^{\frac{1}{2}}\} \end{aligned}$$

for all $N > N_0(\varepsilon)$.

Rankin found a better lower bound for $r_k(N)$ and in greater generality. Let us state the result for the lower bound of $r_k(N)$ and we refer to his paper [Ran60] for the proof.

Theorem 1.3.4. *(R. A. Rankin). Let $k > 2^m$, where m is a positive integer. Let $c = (m+1)2^{m/2}(\log 2)^{\frac{m}{m+1}}$ and let ε be positive. Then there exists a positive real number $N_0(\varepsilon)$ depending on ε and m such that for each $N > N_0(\varepsilon)$, we can construct a set $A \subseteq \{1, 2, \ldots, [N]\}$, no k terms of which are in an arithmetical*

progression, with

$$\#(A) > N \exp\{-c(1+\varepsilon)(\log N)^{\frac{1}{1+m}}\}.$$

Therefore,

$$r_k(N) > N \exp\{-c(1+\varepsilon)(\log N)^{\frac{1}{1+m}}\}.$$

In particular, if $k = 3$ then $m = 1$ and we get Behrend's result. For $k = 4$ the same lower bound for $r_4(N)$ holds as $m = 1$ in this case. But for $k = 5$ we get a larger lower bound, since we can take $m = 2$. Thus it improves upon and generalizes Behrend's result.

1.4 Results on upper bounds of size functions.

In this section we shall sketch proofs of some known results on the upper bounds on size functions.

Let us start with the results of P. Erdös and P. Turán [ET36].

Theorem 1.4.1. *$r(2N) \leq N$ if $N \geq 8$.*

Theorem 1.4.2. *For $\varepsilon > 0$, there exists a positive integer $N_0(\varepsilon)$ such that for all $N > N_0(\varepsilon)$ we have,*

$$r(N) < (\frac{4}{9} + \varepsilon)N.$$

Theorem 1.4.3. *For $\varepsilon > o$, there exists a positive integer $N_0(\varepsilon)$ such that for all $N > N_0(\varepsilon)$ we have,*

$$r(N) < (\frac{3}{8} + \varepsilon)N.$$

Proof. The basic observation by P. Erdös and P. Turán [ET36] is that

$$r(M+N) \leq r(M) + r(N), \tag{1.4.1}$$

for all positive integers M and N. Hence for all $N \geq 1$ we have,

$$r(2N) \leq 2r(N). \tag{1.4.2}$$

Next the proofs proceed by induction on N. They prove theorem 1.4.1 by showing that $r(2N) \leq N$ for $N = 8, 9, 10, 11$ with elementary arguments and theorem 1.4.2

by showing $r(2^k+2^{k-3}-1) \leq 2^{k-1}$ for all $k \geq 4$ with elementary arguments. With the similar short of arguments one can prove the theorem 1.4.3. □

More generally it is easy to observe that, for all $M, N \geq 1$ we have,

$$r_k(M+N) \leq r_k(M) + r_k(N). \tag{1.4.3}$$

We shall prove the following theorem for each $k \geq 3$. I could not access the proof of the theorem in the literature. So I have given my own proof below.

Theorem 1.4.4. *There is non-negative number $c_k \leq 1$ such that*

$$\lim_{N\to\infty} \frac{r_k(N)}{N} = c_k.$$

Proof. Let $k \geq 3$ be a fixed integer. Define $a_k(N)$, for $N \geq 1$, by

$$a_k(N) = \frac{r_k(N)}{N}. \tag{1.4.4}$$

$$\text{and let} \quad A_k(N) = A_k \bigcap [1, N], \tag{1.4.5}$$

for any set A_k of positive integers containing no k terms in arithmetic progression. For any two positive integers M and N, we have

$$\#\left(A_k(M+N)\right) \leq \#\left(A_k(M)\right) + \#\left(A_k(N)\right).$$

Thus

$$\#\left(A_k(MN)\right) \leq M\#\left(A_k(N)\right) \tag{1.4.6}$$

and

$$\#\left(A_k(M)\right) \leq \#\left(A_k\left\{\left(\left[\frac{M}{N}\right]+1\right)N\right\}\right) \leq \frac{M+N}{N}\#\left(A_k(N)\right). \tag{1.4.7}$$

Hence,

$$a_k(MN) \leq a_k(N), \tag{1.4.8}$$

$$a_k(M) \leq \left(1+\frac{N}{M}\right) a_k(N). \tag{1.4.9}$$

Finally we have trivial inequality

$$\frac{1}{M} \leq a_k(M) \leq 1. \tag{1.4.10}$$

Let $l \geq 2$ be a positive integer. Then by (1.4.8), $\{a_k(l^t)\}_{t\geq 0}$ is a decreasing sequence which is bounded bellow and hence converges to $c_k \geq 0$ (say). Now for every subsequence $\{x_n\}_{n\geq 0}$ of the sequence of all natural numbers we can find a further subsequence $\{x_{n_m}\}_{m\geq 0}$ such tha $l^{2t} < x_{n_m} \leq l^{3t}$ for some $t \geq 1$. Now by (1.4.9) we have

$$a_k\left(x_{n_m}\right) \leq \left(1 + \frac{l^t}{x_{n_m}}\right) a_k(l^t) < \left(1 + \frac{1}{l^t}\right) a_k(l^t).$$

and hence

$$a_k(l^{4t}) \leq \left(1 + \frac{x_{n_m}}{l^{4t}}\right) a_k\left(x_{n_m}\right) \leq \left(1 + \frac{1}{l^t}\right)^2 a_k(l^t). \tag{1.4.11}$$

Now taking limit as $m \to \infty$ in (1.4.11) we have

$$\lim_{m\to\infty} a_k\left(x_{n_m}\right) = c_k.$$

Thus every subsequence of the sequence $\{a_k(N)\}$ has a further subsequence which converges to c_k. Hence the sequence $\{a_k(N)\}$ converges to c_k, proving the theorem. □

P. Erdös and P. Turán [ET36] made the conjecture that $c_k = 0$ for all $k \geq 3$. A few years later, in 1938, Behrend [Beh38] proved that.

Theorem 1.4.5. *Either* $c_k = 0$ *for every* $k \geq 3$ *or* $\lim_{k\to\infty} c_k = 0$.

For the proof of this theorem we refer to his paper [Beh38].

In 1953, Leo Moser [Mos53] proved the following theorems on upper bound of $r(N)$.

Theorem 1.4.6. *For all* $N \geq 1$ *we have*

$$r(N) < \frac{2}{5}N + 3.$$

Theorem 1.4.7. *For all* $N \geq 1$ *we have*

$$r(N) < \frac{4}{11}N + 3.$$

The proofs are not quite difficult and we refer to his original paper [Mos53] for the proof. One should note here that these two theorems hold for all $N \geq 1$.

In 1952, K. F. Roth [Rot53] proved the following theorem.

Theorem 1.4.8. $r(N) = O(\frac{N}{\log\log N})$. *i.e.,* $a(N) = \frac{1}{\log\log N}$.

Below we shall sketch the proof of the theorem. For the details of the proof we refer to the original paper of K. F. Roth [Rot53].

Let x and y be any two positive integers. Then we have the following obvious facts.

$\#(A(x))$ is also the greatest number of integers that can be selected from x consecutive terms of an arithmetic progression containing no 3 terms in arithmetical progression.

$$\#(A(x+y)) \leq \#(A(x)) + \#(A(y)), \quad \#(A(xy)) \leq x\#(A(y))$$
$$\#(A(x)) \leq \#\left(A\left(\left\{\left[\frac{x}{y}\right]+1\right\}y\right)\right) \leq \frac{x+y}{y}\#(A(y)).$$

$$a(xy) \leq a(y), \tag{1.4.12}$$
$$a(x) \leq (1+yx^{-1})a(y), \tag{1.4.13}$$
$$x^{-1} \leq a(x) \leq 1. \tag{1.4.14}$$

These follow from (1.4.8),(1.4.9), and (1.4.10) by setting $r = 3$.

Let $u_1, u_2, \ldots, u_U$ be U elements from $1, 2, \ldots, M$ containing no three terms in an arithmetic progression. We consider the exponential sum

$$S = \sum_{k=1}^{U} e(\alpha u_k) \qquad [e(\theta) = e^{2\pi i\theta}],$$

where α is a real number. For each α, there exist two positive integers h and q such that

$$\alpha = \frac{h}{q} + \beta, \quad (h,q) = 1, \quad q \leq M^{\frac{1}{2}}, \quad q|\beta| \leq M^{-\frac{1}{2}}. \tag{1.4.15}$$

Here the notation (h,q) means the greatest common divisor of h and q and $|\beta|$ denotes the absolute value of β. Now, assume $m < M$, and put

$$S' = a(m)q^{-1}\left(\sum_{l=1}^{q} e\left(\frac{rh}{q}\right)\right)\left(\sum_{n=1}^{M} e(\beta n)\right),$$

(so that $S' = 0$ if $q > 1$). Then he proved that

$$|S - S'| < Ma(m) - U + O(mM^{\frac{1}{2}}). \tag{1.4.16}$$

Next he used the Hardy-Littlewood method to obtain a functional inequality

for the function $a(x)$. Let m be an even integer, $2N = m^4$, and let $u_1, u_2, \ldots, u_U$ be a maximal subset of $1, 2, \ldots, 2N$ containing no three terms in an arithmetic progression, so that $U = \#(A(2N))$. Let $2v_1, 2v_2, \ldots, 2v_V$ be the even integers among u_k. Therefore, by the definition of $a(x)$, we have,

$$U = 2Na(2N). \tag{1.4.17}$$

Also by (1.4.12), we have,

$$U \leq 2Na(m), \quad V \leq \#(A(N)) \leq Na(m). \tag{1.4.18}$$

Since the number of odd integers among the u_k does not exceed $\#(A(N))$, we have, by (1.4.12),

$$V \geq \#(A(2N)) - \#(A(N)) \geq 2Na(2N) - Na(m). \tag{1.4.19}$$

We define

$$f_1(\alpha) = \sum_{k=1}^{U} e(\alpha u_k), \qquad f_2(\alpha) = \sum_{k=1}^{V} e(\alpha v_k);$$
$$F_1(\alpha) = a(m) \sum_{n=1}^{2N} e(\alpha n), \quad F_2(\alpha) = a(m) \sum_{n=1}^{N} e(\alpha n).$$

By (1.4.18), we have

$$f_j(\alpha) = O(Na(m)), \quad F_j(\alpha) = O(Na(m)); \quad j = 1, 2. \tag{1.4.20}$$

Then he proved that, for any α,

$$f_j(\alpha) - F_j(\alpha) = O\left(N\{a(m) - a(2N)\} + N^{\frac{3}{4}}\right); \quad j = 1, 2. \tag{1.4.21}$$

He proved (1.4.21) using

$$F_j(\alpha) = O(N^{\frac{3}{4}}),$$

which follows from the fact that for any α,

$$\sum_{n=1}^{M} e(\alpha n) = O(\|\alpha\|^{-1}), \tag{1.4.22}$$

where $\|\alpha\|$ denotes the distance of α from the nearest integer.

Finally, by (1.4.21) and (1.4.22), if $0 < \eta < \alpha < 1 - \eta$ we have

$$f_1(\alpha) = O\left(a(m)\eta^{-1} + \{a(m) - a(2N)\} + N^{\frac{3}{4}}\right). \tag{1.4.23}$$

Then by following the method of Hardy and Littlewood and supposing that

$$0 < \eta = \eta(m) < \frac{1}{2}. \tag{1.4.24}$$

he proved

$$\begin{aligned} a^2(m) &= O\left(a^2(m)N^{-2}\eta^{-2}\right) + O\left(a(m)N^{-1}\eta^{-1}\right) \\ &\quad + O\left(\{\eta N a(m) + 1\}\{a(m) - a(2N) + N^{-\frac{1}{4}}\}\right) \end{aligned} \tag{1.4.25}$$

Hence writing

$$\delta = (N\eta)^{-1}, \tag{1.4.26}$$

we obtain, noting $2N = m^4$,

$$a^2(m) < c_1\left\{a(m)\delta + a^2(m)\delta^2 + \left(\delta^{-1}a(m) + 1\right)\left(a(m) - a(m^4) + m^{-1}\right)\right\}. \tag{1.4.27}$$

Here $\delta = \delta(m)$ is subject only to the restriction implied by (1.4.24). We now write $m = 2^{4^x}$, $b(x) = a(m)$, so that (1.4.27) becomes

$$b^2(x) < c_1\left\{b(x)\delta + b^2(x)\delta^2 + \left(\delta^{-1}b(x) + 1\right)\left(b(x) - b(x+1) + 2^{-4^x}\right)\right\}. \tag{1.4.28}$$

Then using (1.4.12), (1.4.14),(1.4.13) and (1.4.28) he proved

$$b(2^i) = O(2^{-i});$$

and hence, since $b(x)$ is monotonically decreasing function,

$$b(x) = O(x^{-1}). \tag{1.4.29}$$

Finally, corresponding to any large integer y we may choose x to satisfy

$$2^{4^x} < y \leq 2^{4^{x+1}}.$$

Then, by (1.4.13), we have

$$a(y) \leq 2a(2^{4^x}) = 2b(x),$$

so that (1.4.29) implies the theorem. In 1969, E. Szemerédi [Sze68] proved that $c_4 = 0$ and in 1975 he [Sze68] proved that $c_k = 0$ for all $k \geq 3$. His result is one of the most celebrated theorems in combinatorics.

Theorem 1.4.9. *We have $r_k(N) = o(N)$ i.e. $c_k = 0$ for any fixed $k \geq 3$.*

Gowers [Gow98,Gow01] made a major breakthrough in giving the upper bound for $r_k(N)$. We record his theorems and refer to his original papers for the proofs.

Theorem 1.4.10. *Let $k \geq 3$ be an integer. Then there is a constant $d_k > 0$ such that*

$$r_k(N) = O\left(N(\log\log N)^{-d_k}\right).$$

This is still a long way from the conjecture that $r_k(N) < \pi(N)$ for N sufficiently large. Here $\pi(N)$ denotes the number of primes less than or equal to N.

In chapter 2 we shall show, among other things, that P. Erdös conjecture [UL75] implies E. Szemerédi's theorem.

Chapter 2

Sequences of positive integers containing no k terms in an A. P. II

2.1 Introduction

This chapter is about some consequences of the following celebrated conjecture of Erdös [UL75]:

Conjecture 1 (Erdös)**.** *If the sum of the reciprocals of a set of positive integers is infinite then it contains arbitrarily long arithmetic progressions.*

This amounts to saying that if a subset of natural numbers does not contain any arithmetical progression of length $k \geq 3$, where k is a fixed positive integer, then the sum of the reciprocals of its elements is finite.

Joseph L. Gerver [Ger77] proved that for every $\varepsilon > 0$, there exists for all but a finite number of integers $k \geq 3$, sets S_k of positive integers, containing no arithmetic progression of k terms, such that $\sum_{a \in S_k} \frac{1}{a} > (1-\varepsilon)k \log k$. The set S_k is the sequence $\{a_n\}$ where $a_1 = 1$ and for $n \geq 1$, a_{n+1} is the smallest positive integer bigger than a_n such that no k elements of $a_1, a_2, \cdots a_{n+1}$ are in arithmetic progression. He guessed in that paper that for any prime p, the set S_p may indeed maximize the sum of the reciprocals of the elements of a set of positive integers having no p terms in arithmetic progression. Though he made this speculation, he did not give any reason for existence of such a subset of $\mathbb{N}$. In section 2 we use topological ideas to show that the Erdös conjecture is true if and only if there is a set of positive integers containing no k terms in arithmetic progression which maximizes the above sum.

On the other hand Joseph L. Gerver and L. Thomas Ramsey [GR79] showed heuristically that the set S_k is not maximizing the above sum for composite k. In section 3 we prove that the set S_p is not maximizing the above sum for any prime $p \geq 3$.

2.2 Existence of M_p

In this section we shall assume the Erdös conjecture and derive a much stronger consequence of it. We ask whether the sum above can be arbitrarily large as the sets A vary. Our first theorem answers the question in the negative. A corollary to our second theorem says that the Erdös conjecture implies the existence of a set of positive integers containing no p terms in arithmetic progression which maximizes the above sum.

Finally we shall prove Szemerédi's theorem as a consequence of the Erdös conjecture.

In the rest of this section, p is any fixed integer (not necessarily a prime) greater than or equal to 3.

2.2.1 Main results of this section

Theorem 2.2.1. *Let $\mathscr{A}_p$ be the collection of all subsets of $\mathbb{N}$ having no arithmetic progression of length p. Then, under the assumption of the Erdös conjecture, there is an absolute constant B_p such that*

$$\text{Sup}\left\{\sum_{a\in A}\frac{1}{a} : A \in \mathscr{A}_p\right\} \leq B_p. \tag{2.2.1}$$

For further discussion, we need a topological structure on $\mathscr{A}_p$. First we note that there is a natural one-to-one correspondence between the power set $\mathscr{P}(\mathbb{N})$ and the set $\{0,1\}^{\mathbb{N}}$ of all sequences of 0s and 1s ; namely, given any subset $A \subset \mathbb{N}$, we send it to the sequence $\{\delta_A(n)\}_{n=1}^{\infty}$, where

$$\delta_A(n) = \begin{cases} 1 \text{ if } n \in A \\ 0 \text{ otherwise .} \end{cases}$$

Since $\{0,1\}^{\mathbb{N}}$ is compact by Tychonoff's theorem, the above identification makes $\mathscr{P}(\mathbb{N})$ into a compact topological space. In this topology, a sequence $\{A_n\}$ of subsets converges to A if, for any given k, there is some N_k such that, whenever

$n \geq N_k$,

$$\delta_{A_n}(j) = \delta_A(j) \text{ for } j = 1, 2, \cdots, k. \tag{2.2.2}$$

Proposition 4 below says that $\mathscr{A}_p$ is a compact subspace of $\mathscr{P}(\mathbb{N})$. For any set $A \in \mathscr{A}_p$, let us denote the sum $\sum_{a \in A} \frac{1}{a}$ (which converges if we assume Erdös conjecture) by $\mu(A)$. Then we have the following theorem.

Theorem 2.2.2. *The map $A \longmapsto \mu(A)$ between $\mathscr{A}_p$ and $[0, B_p]$ is continuous.*

Since $\mathscr{A}_p$ is compact, theorem 2.2.2 implies the following corollary.

Corollary 2.2.3. *Under the assumption of the Erdös conjecture, there is a set $M_p \in \mathscr{A}_p$ such that*

$$\mu(X) \leq \mu(M_p) \text{ for all } X \in \mathscr{A}_p. \tag{2.2.3}$$

That is, the supremum of the set $\{\mu(X) : X \in \mathscr{A}_p\}$ is attained.

2.2.2 Proofs

In this section, we shall present the proofs of theorem 2.2.1 and theorem 2.2.2. First we prove a proposition that will be needed later.

Proposition 2.2.4. *$\mathscr{A}_p$ is a compact subspace of $\mathscr{P}(\mathbb{N})$.*

Proof. Since $\mathscr{P}(\mathbb{N})$ is compact, it is enough to show that $\mathscr{A}_p$ is closed. Let $\{A_n\}$ be sequence in $\mathscr{A}_p$ converging to some $A \in \mathscr{P}(\mathbb{N})$. We need to show that $A \in \mathscr{A}_p$. Let us denote

$A_n = \{a_1^{(n)}, a_2^{(n)}, \cdots\}$ and $A = \{a_1, a_2, \cdots\}$, where the terms in the sequences are written in the increasing order. Suppose, if possible, that $A \notin \mathscr{A}_p$. So there is an arithmetic progression $\{a_{k_1}, a_{k_2}, \cdots, a_{k_p}\} \subset A$. We shall obtain a contradiction from this. Since $A_n \longmapsto A$, by the criterion (2.2.2) for convergence, we must have, for any given k, some integer N_k such that,

$$a_j^{(n)} = a_j \text{ for } j = 1, 2, \cdots, k \tag{2.2.4}$$

for all $n \geq N_k$. In particular, if $k = k_p$, we have, for $n \geq N_{k_p}$,

$$a_{k_i}^{(n)} = a_{k_i} \text{ for } i = 1, 2, \cdots, p. \tag{2.2.5}$$

Since $\{a_{k_i} : i = 1, 2, \cdots, p\}$ is an arithmetic progression, the above implies that $A_n \notin \mathscr{A}_p$ for $n \geq N_{k_p}$, which is a contradiction. So $A \in \mathscr{A}_p$ as was required to be proved.

□

Proof of theorem 2.2.1

Proof. We shall prove this theorem by contradiction. Let $A_0 = A \in \mathscr{A}_p$ be any finite set with $\sum_{a\in A} \frac{1}{a} = L > 0$. For example, we can take $A_0 = \{1\}$. If we assume that the statement of the theorem is not true, then we shall show that there is a finite set $B \supset A$, $B \in \mathscr{A}_p$ with

$$\sum_{b\in B} \frac{1}{b} \geq L + 1. \tag{2.2.6}$$

This will result in a contradiction to the conjecture of Erdös in the following manner. Repeating this process that produces B recursively, we get an increasing sequence of sets $A_0 \subset A_1 \subset A_2 \subset \cdots$, each of them finite and they all are in $\mathscr{A}_p$. Moreover,

$$\sum_{a\in A_j} \frac{1}{a} \geq L + j.$$

Now the set $A_\infty = A_0 \cup A_1 \cup A_2 \cup \cdots$ must be in $\mathscr{A}_p$ since any given collection of p elements in A_∞ must also belong to A_n for some n, so those elements can not be in arithmetic progression. On the other hand, the sum $\sum_{a\in A} \frac{1}{a}$ must diverge as it is bigger than any fixed number. So all that is now left to prove the theorem is to produce such a set B, given A.

Let N be the maximum of the elements of A. If the theorem is untrue, then there must exist a set $E \in \mathscr{A}_p$ such that

$$\sum_{e\in E} \frac{1}{e} \geq 2N. \tag{2.2.7}$$

In fact, we may take E to be a finite set; since, if E is infinite, the tail of the convergent sum will be small. Now define

$$B = A \sqcup 2NE, \tag{2.2.8}$$

where $\sqcup$ denotes disjoint union, and $2NE = \{2Ne : e \in E\}$. Clearly B is a finite set containing A, and

$$\sum_{b\in B} \frac{1}{b} = \sum_{a\in A} \frac{1}{a} + \sum_{e\in E} \frac{1}{2Ne} \geq L + 1 \tag{2.2.9}$$

by (7 , 8). Now to show that $B \in \mathscr{A}_p$, we first note that since $A \in \mathscr{A}_p$ and $E \in \mathscr{A}_p$, no p elements of either A or $2NE$ can be in arithmetic progression.

Suppose, if possible, that $b_1, b_2, \cdots, b_p \in B$ are in A.P., where $b_1, b_2, \cdots, b_k \in A$, and $b_{k+1}, b_{k+2}, \cdots, b_p \in 2NE$. If $k \geq 2$, then

$$b_{k+1} - b_k = b_k - b_{k-1}. \tag{2.2.10}$$

Now, $b_k - b_{k-1} \leq N-1$ since $b_k, b_{k-1} \in A$ and N is the maximum of the elements of A. But the right hand side, $b_{k+1} - b_k \geq b_{k+1} - N \geq 2N - N = N$, a contradiction. If $k = 1$, then

$$b_2 - b_1 = b_3 - b_2, \tag{2.2.11}$$

or equivalently,

$$b_1 = 2b_2 - b_3. \tag{2.2.12}$$

But $b_1 \leq N$, while $2b_2 - b_3$ is a multiple of $2N$ as both $b_2, b_3 \in 2NE$. So we arrive at a contradiction again. Hence we conclude that B cannot have an arithmetic progression of length p.

□

For proving theorem 2.2.2, we first prove a lemma.

Lemma 2.2.5. *Given any $\varepsilon > 0$, there exist a natural number N such that for any $A \in \mathscr{A}_p$ with* Min $A \geq N$,

$$\sum_{a \in A} \frac{1}{a} < \varepsilon. \tag{2.2.13}$$

Note: In the above, Min A denotes the smallest element in A.

Proof. Suppose, if possible, the lemma is not correct. Then there exists some $\varepsilon > 0$ such that for any given integer $M \geq 1$, there is a set $R \in \mathscr{A}_p$ depending on M with the following properties:

$$\mu(R) = \sum_{r \in R} \frac{1}{r} > \varepsilon, \tag{2.2.14}$$

and

$$\text{Min } R \geq 2M. \tag{2.2.15}$$

For that ε, we choose a set $A \in \mathscr{A}_p$ satisfying

$$\mu(A) > M_p - \frac{\varepsilon}{12}. \tag{2.2.16}$$

where $M_p = \text{Sup}\{\mu(A) : A \in \mathscr{A}_p\} < \infty$ by Theorem 2.2.1. Let $A = \{a_1, a_2, \cdots\}$

where $a_1 < a_2 < \cdots$. Since $\sum_{a\in A} \frac{1}{a} < \infty$, there is some n_0 such that

$$\sum_{n=n_{0+1}}^{\infty} \frac{1}{a_n} < \frac{\varepsilon}{12} \tag{2.2.17}$$

for any $\varepsilon > 0$. Let $A_1 = \{a_1, a_2, \cdots, a_{n_0}\}$. Then

$$\mu(A_1) > M_p - \frac{\varepsilon}{6}. \tag{2.2.18}$$

by (2.2.16) and (2.2.17)

Now we take $M = a_{n_0}$ and write, $R = R_1 \sqcup R_2 \sqcup R_3 \sqcup R_4$ where

$$R_j = R \bigcap \{ \bigsqcup_{i=0}^{\infty} [(j+1)3^i M, (j+2)3^i M) \}; j = 1, 2, 3, 4. \tag{2.2.19}$$

In other words,

$$\begin{aligned}
R_1 &= R \bigcap \{[2M, 3M) \sqcup [6M, 9M) \sqcup [18M, 27M) \sqcup \cdots\}, \\
R_2 &= R \bigcap \{[3M, 4M) \sqcup [9M, 12M) \sqcup [27M, 36M) \sqcup \cdots\}, \\
R_3 &= R \bigcap \{[4M, 5M) \sqcup [12M, 15M) \sqcup [36M, 45M) \sqcup \cdots\}, \\
R_4 &= R \bigcap \{[5M, 6M) \sqcup [15M, 18M) \sqcup [45M, 54M) \sqcup \cdots\}.
\end{aligned}$$

We have,

$$\text{Max } A_1 = M < 2M \leq \text{Min } R, \tag{2.2.20}$$

which implies $R \cap A_1 = \phi$, the empty set. We notice that no p elements of R_j, $1 \leq j \leq 4$ are in arithmetic progression. Hence with the same argument as in theorem 1 it is easy to check that no p elements of $A_1 \sqcup R_j, 1 \leq j \leq 4$, can be in an arithmetic progression. So $A_1 \sqcup R_j \in \mathscr{A}_p$.

Since $\mu(R) > \varepsilon$, we must have

$$\mu(R_j) > \frac{\varepsilon}{4} \tag{2.2.21}$$

for some $j, 1 \leq j \leq 4$.

For that j,

$$\mu(A_1 \sqcup R_j) = \mu(A_1) + \mu(R_j) > M_p + \frac{\varepsilon}{12} \tag{2.2.22}$$

from (2.2.18). This is a contradiction to the fact that M_p is the supremum of the

set $\{\mu(A) : A \in \mathscr{A}_p\}$. This proves the lemma.

□

Now we present the proof of theorem 2.2.2.

Proof of theorem 2.2.2

Proof. Suppose $\{A_n\} \subset \mathscr{A}_p$ be a sequence and $A_n \longrightarrow A$. We need to show that $\mu(A_n) \longrightarrow \mu(A)$.

Let us write the set A as, $A = \{a_1, a_2, a_3, \cdots\}$ where $a_1 < a_2 < a_3 < \cdots$ and similarly for the sets A_n, we write them as, $A_n = \{a_1^{(n)}, a_2^{(n)}, \cdots\}$. Note that if the set A is finite, then $A_n = A$ for large enough n and there is nothing left to prove. Let $\varepsilon > 0$ be any given real number. The lemma above allows us to select an N such that for any set $X \in \mathscr{A}_p$ with Min $X \geq N$, we must have

$$\sum_{x \in X} \frac{1}{x} < \frac{\varepsilon}{2}. \tag{2.2.23}$$

Let n_0 be an integer such that $a_{n_0} \geq N$. Since $A_n \longrightarrow A$, there is some N_0 such that $a_k^{(n)} = a_k$ for $1 \leq k \leq n_0$ and all $n \geq N_0$. Now, for $n \geq N_0$,

$$\begin{aligned} \Big|\mu(A_n) - \mu(A)\Big| &= \Big| \sum_{k=n_0+1}^{\infty} \frac{1}{{a_k}^{(n)}} - \sum_{k=n_0+1}^{\infty} \frac{1}{a_k} \Big| \\ &\leq \sum_{k=n_0+1}^{\infty} \frac{1}{{a_k}^{(n)}} + \sum_{k=n_0+1}^{\infty} \frac{1}{a_k} < \varepsilon \end{aligned} \tag{2.2.24}$$

by (2.2.23). Hence $\mu(A_n) \longrightarrow \mu(A)$.

□

Remark

Here we have proved everything assuming the Erdös conjecture. But it is easy to see the Lemma 2.2.5 and the conclusions of Theorem 2.2.1, Theorem 2.2.2, and Corollary 2.2.3, each separately implies the conjecture. So, in fact, they are all equivalent to the Erdös conjecture.

We conclude this section by showing that the Erdös conjecture implies the E. Szemerédi's theorem [Sze68]. Since Erdös conjecture is equivalent to Lemma 5 above, we prove that Lemma 2.2.5 implies the Szemerédi's theorem.

Corollary 2.2.6. *Erdös conjecture implies Szemerédi's theorem.*

Proof. Let $\varepsilon > 0$. By lemma 2.2.5 there is a positive integer $N_0(\varepsilon)$ such that for all $A \in \mathscr{A}_p$ and for all $N \geq N_0$ we have

$$\varepsilon/2 > \sum_{a\in A,\quad a\geq N_0} \frac{1}{a} \geq \sum_{a\in A,\quad N_0\leq a\leq N} \frac{1}{a} > \frac{\#\left(A\bigcap[N_0, N]\right)}{N}.$$

Hence

$$\#\left(A\bigcap[N_0, N]\right) < N\varepsilon/2$$

for all $N \geq N_0$. Therefore

$$\#\left(A\bigcap[1, N]\right) < N_0 + \#\left(A\bigcap[N_0, N]\right) < N_0 + N\varepsilon/2 < N\varepsilon$$

for all sufficiently large N. Since $A \in \mathscr{A}_p$ is arbitrarily chosen, therefore we have $r_p(N) < N\varepsilon$ for all sufficiently large N. This is Szemerédi's theorem. □

2.3 Greedy sequences do not maximize the above sum

In section 2 we have proved that the Erdös conjecture is true only if there is a set in $\mathscr{A}_p$ which maximizes the function μ.

Joseph L. Gerver [Ger77] showed that the sum of the reciprocals of the elements of S_p is larger than that of other likely candidates studied in the literature, in particular Rankin's sets, which has the highest known asymptotic density for sets in $\mathscr{A}_p$. He also speculated in that paper that for any odd prime p, among all sets in $\mathscr{A}_p$, the set S_p may indeed be the one which gives the largest number when the reciprocals of its elements are added. On the other hand, Joseph L. Gerver and L. Thomas Ramsey [GR79] showed heuristically that the set S_p does not maximize the above sum if p is a composite number. In this section we prove that the set S_p does not maximize the above sum for odd primes p. In rest of this section, p is any fixed odd prime.

2.3.1 Main results of this section

Let us consider the increasing sequence $\{\alpha(n) : n \geq 0\}$ of non-negative integers defined as follows.

$\alpha(0) = 0$; and for $n \geq 1$, $\alpha(n)$ is the smallest positive integer greater than

$\alpha(n-1)$ such that no p terms of $0 = \alpha(0) < \alpha(1) < \ldots < \alpha(n-1) < \alpha(n)$ are in arithmetic progression. This kind of simplistic algorithm that we have used to define the sequence is often called a "greedy algorithm", and accordingly we shall refer to the sequence $\{\alpha(n)+1\}_{n\geq 0}$ as the greedy sequence. For any sequence $0 = \beta(0) < \beta(1) < \beta(2) < \ldots < \beta(n) < \ldots$ of integers, containing no p terms in arithmetic progression, we define, for all $N \geq 0$,

$$\mu_\beta(N) = \sum_{k=0}^{N} \frac{1}{1+\beta(k)} \tag{2.3.1}$$

For N fixed, we shall consider $\mu_\beta(N)$ as function of the sequences β. J. L. Gerver [Ger77] speculated that the greedy sequence maximizes the sum $\mu_\beta(N)$ among all sequences in $\mathscr{A}_p$ for all sufficiently large N. We disprove this speculation by proving that $\mu_\alpha(N)$ is maximum only for finitely many N. More precisely, we have the following theorem.

Theorem 2.3.1. *There is a positive integer N such that, for all $n \geq N$, there is a sequence $0 = \gamma(0) < \gamma(1) < \gamma(2) < \ldots < \gamma(n) < \ldots$ of integers containing no p terms in arithmetic progression with $\mu_\alpha(n) < \mu_\gamma(n)$, i.e. ,*

$$\sum_{k=0}^{n} \frac{1}{1+\alpha(k)} < \sum_{k=0}^{n} \frac{1}{1+\gamma(k)}. \tag{2.3.2}$$

Finally we disprove the main speculation of J. L. Gerver by exhibiting a sequence of positive integers the sum of the reciprocals of which is bigger than that of the greedy sequence. We have the following theorem.

Theorem 2.3.2. *There is a sequence $0 = \gamma(0) < \gamma(1) < \gamma(2) < \ldots < \gamma(n) < \ldots$ of integers containing no p terms in arithmetic progression such that*

$$\sum_{n=0}^{\infty} \frac{1}{1+\alpha(n)} < \sum_{n=0}^{\infty} \frac{1}{1+\gamma(n)}. \tag{2.3.3}$$

2.3.2 Properties of the greedy sequence

In this section we shall study some properties of the greedy sequence. These properties of the greedy sequence will be used to prove our main theorems.

1. For $n \geq 0$, if $n = \sum_{t=0}^{k} e_t(p-1)^t$ with $e_t \in \{0, 1, \ldots, p-2\}$ is the $(p-1)$-ary expansion of n then,

$$\alpha(n) = \sum_{t=0}^{k} e_t p^t. \tag{2.3.4}$$

2. For $m \geq 0$, $i \geq 0$, and $0 \leq k \leq (p-1)^m - 1$, we have,

$$\alpha(i(p-1)^m + k) = ip^m + \alpha(k). \tag{2.3.5}$$

3. We have

$$\sum_{n=0}^{\infty} \frac{1}{1+\alpha(n)} < 1 + p(p-2) < \infty. \tag{2.3.6}$$

4. For all $m \geq 0$, we have,

$$\sum_{k=0}^{(p-1)^m-1} \alpha(k) = \frac{(p-1)^m}{2} \alpha((p-1)^m - 1). \tag{2.3.7}$$

Proof. We shall prove property (1) by induction on n. For $n = 0$, 1, the result is trivially true. Let us assume that the result is true for all positive integers $\leq n$. Let $n = \sum_{t=0}^{k} e_t (p-1)^t$ be the $(p-1)$-ary expansion of n. Therefore $\alpha(0)$, $\alpha(1), \cdots, \alpha(n)$ are of the form $\sum_{t=0}^{k} e_t p^t$ for some $e_t = 0, 1, \cdots, p-2$.

Case1. Let $e_t = p-2$ for all t, $0 \leq t \leq k$. Therefore, we have,

$$\begin{aligned} n+1 &= 1 + (p-2) + \cdots + (p-2)(p-1)^k \\ &= 1 + (p-2)\frac{(p-1)^{k+1} - 1}{p-2} = (p-1)^{k+1}. \end{aligned} \tag{2.3.8}$$

We shall show

$$\alpha(n+1) = p^{k+1}. \tag{2.3.9}$$

We have

$$\begin{aligned} p^{k+1} - \alpha(n) &= p^{k+1} - \alpha((p-2) + (p-2)(p-1) + \cdots + (p-2)(p-1)^k) \\ &= p^{k+1} - \{(p-2) + (p-2)p + \cdots + (p-2)p^k\} \\ &= p^{k+1} - (p-2)\frac{p^{k+1} - 1}{p-1} = \frac{p^{k+1} - 1}{p-1} + 1. \end{aligned} \tag{2.3.10}$$

Hence,

$$p^{k+1} - \alpha(0) = p^{k+1} < (p-1)\left\{\frac{p^{k+1} - 1}{p-1} + 1\right\} = (p-1)(p^{k+1} - \alpha(n)). \tag{2.3.11}$$

Therefore, no p terms of $\alpha(0)$, $\alpha(1), \ldots, \alpha(n)$, p^{k+1} are in arithmetic progression. Therefore, $\alpha(n+1) \leq p^{k+1}$. If possible, let $\alpha(n+1) < p^{k+1}$.

Let $\alpha(n+1) = \sum_{t=0}^{k} \varepsilon_t p^t$, where, $0 \leq \varepsilon_t \leq p-1$, for $0 \leq t \leq k$. We note that at least one $\varepsilon_t = p-1$; otherwise we would have $\alpha(n+1) \in \{\alpha(0), \alpha(1), \ldots, \alpha(n)\}$ by induction hypothesis. But we know that $\alpha(n+1) > \alpha(n)$. Let $A = \{t : 0 \leq t \leq k, \text{ and } \varepsilon_t < p-1\}$ and $B = \{0, 1, 2, \ldots, k\} - A \neq \emptyset$. Let $T = \sum_{t \in A} \varepsilon_t p^t$ and $R = \sum_{t \in B} p^t \neq 0$, ($\because B \neq \emptyset$). The non-negative integers $T,\ T+R,\ T+2R, \ldots, T+(p-1)R$ are in arithmetic progression and $T,\ T+R,\ T+2R,\ \ldots, T+(p-1)R \in \{\alpha(0),\ \alpha(1), \ldots, \alpha(n+1)\}$. This contradicts the fact that no p terms of the greedy sequence are in arithmetic progression.

Case2. Let $e_t < p-2$ for some t, $0 \leq t \leq k$. Let $t_0 = \min\{t : 0 \leq t \leq k, \text{ and } e_t < p-2\}$. Therefore, $e_t = p-2$ for $0 \leq t < t_0$. Clearly $n = (p-2) + (p-2)(p-1) + \cdots + (p-2)(p-1)^{t_0-1} + \sum_{t=t_0}^{k} e_t (p-1)^t$. Therefore,

$$n+1 = (e_{t_0}+1)(p-1)^{t_0} + \sum_{t=t_0+1}^{k} e_t (p-1)^t. \tag{2.3.12}$$

We shall show

$$\alpha(n+1) = (e_{t_0}+1)p^{t_0} + \sum_{t=t_0+1}^{k} e_t p^t. \tag{2.3.13}$$

Let $m = \sum_{t=t_0+1}^{k} e_t (p-1)^t \leq n$. Therefore, by the induction hypothesis, $\alpha(m) = \sum_{t=t_0+1}^{k} e_t p^t$. Also $n+1-m = (e_{t_0}+1)(p-1)^{t_0}$. Define, $\beta(x) = \alpha(m+x) - \alpha(m)$, for $0 \leq x \leq n+1-m$. Note that $\beta(x) = \alpha(m+x) - \alpha(m) = \alpha(x)$ for $0 \leq x < n+1-m$. Since no p terms of $\beta(0) = \alpha(0)$, $\beta(1) = \alpha(1), \ldots, \beta(n-m) = \alpha(n-m)$, and $\beta(n+1-m)$ are in arithmetic progression and $\alpha(n+1-m) > \alpha(n-m)$ is the smallest positive integer such that no p terms of $\alpha(0)$, $\alpha(1), \ldots, \alpha(n+1-m)$ are in arithmetic progression then $\beta(n+1-m) \geq \alpha(n+1-m)$.

Therefore,

$$\begin{aligned} \alpha(n+1) = \alpha(m) + \beta(n+1-m) &\geq \alpha(m) + \alpha(n+1-m) \\ &= (e_{t_0}+1)p^{t_0} + \sum_{t=t_0+1}^{k} e_t p^t. \end{aligned} \tag{2.3.14}$$

On the other hand, it is easy to check that no p terms of $\alpha(0)$, $\alpha(1), \ldots, \alpha(n)$, and $(e_{t_0}+1)p^{t_0} + \sum_{t=t_0+1}^{k} e_t p^t$ are in arithmetic progression (see [Ger77]). This proves the property (1).

The property (2) follows from the property (1) directly.

By the property (1), we have,

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{1}{1+\alpha(n)} &= 1+\sum_{k=0}^{\infty}\sum_{n=(p-1)^k}^{(p-1)^{k+1}-1}\frac{1}{1+\alpha(n)} \le 1+\sum_{k=0}^{\infty}\frac{(p-1)^k(p-2)}{1+p^k}\\ &< 1+(p-2)\sum_{k=0}^{\infty}(1-\frac{1}{p})^k = 1+p(p-2)<\infty. \qquad (2.3.15)\end{aligned}$$

This proves the property (3).

We shall prove the property (4) by induction on $m \ge 0$. For $m = 0$, the result is obvious. Let us assume (2.3.7) for some $m \ge 0$. We shall prove it for $m+1$.

By the induction hypothesis,

$$\begin{aligned}\sum_{k=0}^{(p-1)^{m+1}-1}\alpha(k) &= \sum_{k=0}^{(p-1)^m-1}\alpha(k)+\sum_{k=(p-1)^m}^{(p-1)^{m+1}-1}\alpha(k)\\ &= \frac{(p-1)^m}{2}\alpha((p-1)^m-1)+\sum_{k=(p-1)^m}^{(p-1)^{m+1}-1}\alpha(k). \qquad (2.3.16)\end{aligned}$$

Also,

$$\begin{aligned}\sum_{k=(p-1)^m}^{(p-1)^{m+1}-1}\alpha(k) &= \sum_{i=1}^{p-2}\sum_{k=0}^{(p-1)^m-1}\alpha(i(p-1)^m+k)\\ &= \sum_{i=1}^{p-2}\sum_{k=0}^{(p-1)^m-1}\{ip^m+\alpha(k)\}\\ &= \sum_{i=1}^{p-2}\{ip^m(p-1)^m+\frac{(p-1)^m}{2}\alpha((p-1)^m-1)\\ &= \frac{(p-1)^m}{2}\{(p-2)(p-1)p^m+\alpha((p-1)^m-1)\} \qquad (2.3.17)\end{aligned}$$

by the induction hypothesis and (2.3.5).

Therefore, by (2.3.4), (2.3.5), (2.3.16) and (2.3.17), we have,

$$\begin{aligned}\sum_{k=0}^{(p-1)^{m+1}-1}\alpha(k) &= \frac{(p-1)^{m+1}}{2}\{(p-2)p^m+\alpha((p-1)^m-1)\}\\ &= \frac{(p-1)^{m+1}}{2}\{\alpha((p-2)(p-1)^m)+(p-1)^m-1)\}\\ &= \frac{(p-1)^{m+1}}{2}\{\alpha((p-1)^{m+1}-1)\}. \qquad (2.3.18)\end{aligned}$$

This proves the property (4). □

2.3.3 Construction of the sequence $(\gamma(n))$

In this section we shall construct a sequence in $\mathscr{A}_p$ which dominates the greedy sequence. We start with the following theorem due to R. A. Rankin [Ran60].

Theorem 2.3.3. *(R. A. Rankin).*

Let $p > 2^k$, where k is a positive integer. Let $c = (k+1)2^{k/2}(\log 2)^{\frac{k}{k+1}}$ and let ε be positive. Then there exists a positive real number X_1 depending on ε and k such that, for each $X > X_1$, we can construct a set $A \subseteq \{1, 2, \ldots, [X]\}$, $A \in \mathscr{A}_p$, with

$$\#(A) > X \exp\{-c(1+\varepsilon)(\log X)^{\frac{1}{1+k}}\}. \tag{2.3.19}$$

Note: In the above $[X]$ denotes the largest integer $\leq X$ and $\#(A)$ denotes number of elements of A.

We have the following lemma.

Lemma 2.3.4. *There is a positive integer m and a sequence $0 = \beta(0) < \beta(1) < \ldots < \beta((p-1)^m)$ of integers having no p terms in arithmetic progression such that,*

$$\beta((p-1)^m - 1) < \frac{1}{2}\alpha((p-1)^m - 1), \tag{2.3.20}$$

and

$$\sum_{k=0}^{(p-1)^m-1} \beta(k) < \sum_{k=0}^{(p-1)^m-1} \alpha(k). \tag{2.3.21}$$

Proof. We have, for all $m \geq 0$,

$$\begin{aligned} \alpha((p-1)^m - 1) &= \alpha\{(p-2)(p-1)^{m-1} + \cdots + (p-2)(p-1) + (p-2)\} \\ &= (p-2)p^{m-1} + \cdots + (p-2)p + (p-2) \\ &= (p-2)\frac{p^m - 1}{p-1}. \end{aligned} \tag{2.3.22}$$

by (2.3.4).

Let $X_1 = [\frac{p-2}{2}\frac{p^m-1}{p-1}] - 1$, $X = \frac{p-2}{2}\frac{p^m-1}{p-1}$ and let k be the largest positive integer satisfying $p > 2^k$.

Now, by Rankin's construction, for sufficiently large m, there is a subset A of

$\{1, 2, \ldots, X\}$, $A \in \mathscr{A}_p$ such that,

$$\begin{aligned}
\#(A) &> \frac{p-2}{2}\frac{p^m-1}{p-1}\exp\{-c(1+\varepsilon)(\log\frac{(p-2)(p^m-1)}{2(p-1)})^{\frac{1}{k+1}}\} \\
&> \frac{p-2}{2}\frac{p^m-1}{p-1}\exp\{-\frac{m+1}{2}\log\frac{p}{p-1}\} \\
&= \frac{p-2}{2}\frac{p^m-1}{p-1}\exp\{\log\left((\frac{p-1}{p})^{\frac{m+1}{2}}\right)\} = \frac{p-2}{2}\frac{p^m-1}{p-1}(\frac{p-1}{p})^{\frac{m+1}{2}} \\
&= \frac{p-2}{2}\frac{p^m}{p-1}(\frac{p-1}{p})^{\frac{m+1}{2}} - \frac{p-2}{2}\frac{1}{p-1}(\frac{p-1}{p})^{\frac{m+1}{2}} \\
&> \frac{p-2}{2}\frac{p^m}{p-1}(\frac{p-1}{p})^{\frac{m+1}{2}} - 1, \text{ (2nd term is } < 1) \\
&> \frac{p-2}{2(p-1)}(p-1)^m(\frac{p}{p-1})^{\frac{m-1}{2}} - 1 = V(p-1)^m - 1 \text{ (say)} \\
&> (p-1)^m - 1, \qquad (2.3.23)
\end{aligned}$$

since, $V = \frac{p-2}{2(p-1)}(\frac{p}{p-1})^{\frac{m-1}{2}} > 1$, for all sufficiently large m (as $\frac{p}{p-1} > 1$).

The 2nd inequality in (2.3.23) follows directly from the following inequalities

$$\begin{aligned}
\frac{m+1}{2}\log\frac{p}{p-1} &> c(1+\varepsilon)(m\log(p+1))^{\frac{1}{1+k}} \\
&> c(1+\varepsilon)(\log\frac{(p-2)(p^m-1)}{2(p-1)})^{\frac{1}{1+k}}. \qquad (2.3.24)
\end{aligned}$$

for all sufficiently large m.

The first inequality of (2.3.24) follows from the inequality

$m^{\frac{k}{k+1}} > 2c(1+\varepsilon)\frac{(\log p)^{\frac{1}{k+1}}}{\log\frac{p}{p-1}}$ for all sufficiently large m.

The 2nd inequality of (2.3.24) follows from the inequality $\frac{(p-2)(p^m-1)}{2(p-1)} < p^m$ for all m.

This proves (2.3.20).

Suppose (2.3.21) is not true. Then we have,

$$\begin{aligned}
\beta((p-1)^m-1) &> \frac{1}{(p-1)^m}\sum_{k=0}^{(p-1)^m-1}\beta(k) \geq \frac{1}{(p-1)^m}\sum_{k=0}^{(p-1)^m-1}\alpha(k) \\
&= \frac{1}{(p-1)^m}\frac{(p-1)^m}{2}\alpha((p-1)^m-1) \\
&= \frac{1}{2}\alpha((p-1)^m-1). \qquad (2.3.25)
\end{aligned}$$

by (2.3.7).

This contradicts (2.3.20). Thus we have proved (2.3.21). □

We need the following lemma to construct the sequence γ.

Lemma 2.3.5. *Let $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ be two sets of non-negative numbers with*

$$x_1 + x_2 + \cdots + x_n < y_1 + y_2 + \cdots + y_n. \tag{2.3.26}$$

Then there is some $M \geq 1$, such that for all $z \geq M$, we have,

$$\sum_{k=1}^{n} \frac{1}{z + x_k} > \sum_{k=1}^{n} \frac{1}{z + y_k}. \tag{2.3.27}$$

Proof. Suppose the lemma is not true. Then there is a monotonically increasing sequence $\{N_t\}_{t\geq 1}$ of positive numbers, with $N_t \to \infty$ as $t \to \infty$, such that,

$$\sum_{k=1}^{n} \frac{1}{N_t + x_k} \leq \sum_{k=1}^{n} \frac{1}{N_t + y_k}, \quad \text{for all } t \geq 1. \tag{2.3.28}$$

That is,

$$\frac{1}{N_t + x_1} - \frac{1}{N_t + y_1} \leq \sum_{k=2}^{n} \left(\frac{1}{N_t + y_k} - \frac{1}{N_t + x_k}\right), \quad \text{for all } t \geq 1. \tag{2.3.29}$$

That is,

$$y_1 - x_1 \leq \sum_{k=2}^{n} (x_k - y_k)\left(\frac{N_t + x_1}{N_t + x_k}\right)\left(\frac{N_t + y_1}{N_t + y_k}\right), \quad \text{for all } t \geq 1. \tag{2.3.30}$$

By taking limit as $t \to \infty$ in (2.3.30), we have,

$$y_1 - x_1 \leq \sum_{k=2}^{n} (x_k - y_k).$$

That is, $y_1 + y_2 + \cdots + y_n \leq x_1 + x_2 + \cdots + x_n$. This contradicts (2.3.26), and hence we have proved the lemma 2.3.5. □

Now by lemma 2.3.4 and lemma 2.3.5, there is a positive integer m, a number $M \geq 1$, and a sequence $0 = \beta(0) < \beta(1) < \ldots < \beta((p-1)^m - 1$ of integers such that,

$$\sum_{k=0}^{(p-1)^m - 1} \frac{1}{z + \beta(k)} > \sum_{k=0}^{(p-1)^m - 1} \frac{1}{z + \alpha(k)}, \quad \text{for all } z \geq M. \tag{2.3.31}$$

Let $n \geq m$ be the smallest positive integer such that $p^n + 1 \geq M$. Therefore, by (2.3.31), for all $t \geq (p-1)^n$, we have,

$$\sum_{k=0}^{(p-1)^m-1} \frac{1}{1+\alpha(t)+\beta(k)} > \sum_{k=0}^{(p-1)^m-1} \frac{1}{1+\alpha(t)+\alpha(k)}. \tag{2.3.32}$$

Now we define the sequence γ as follows.

$$\gamma(k) = \alpha(k), \text{ for } 0 \leq k \leq (p-1)^n - 1. \tag{2.3.33}$$

For $1 \leq l \leq p-2$, and for $l(p-1)^n \leq k \leq (l+1)(p-1)^n - 1$, write,

$$k = l(p-1)^n + s(p-1)^m + t, \text{ for } \begin{cases} 0 \leq s \leq (p-1)^{n-m} - 1 \\ \text{and } \ 0 \leq t \leq (p-1)^m - 1 \end{cases} \tag{2.3.34}$$

and define

$$\gamma(k) = \alpha(l(p-1)^n + s(p-1)^m) + \beta(t), \text{ for } \begin{cases} 1 \leq l \leq p-2, \\ 0 \leq s \leq (p-1)^{n-m} - 1 \\ \text{and } \ 0 \leq t \leq (p-1)^m - 1 \end{cases} \tag{2.3.35}$$

$$\gamma(k) = \alpha(k) \text{ for } k \geq (p-1)^{n+1}. \tag{2.3.36}$$

Proposition 2.3.6. *No p terms of the sequence γ defined above are in arithmetic progression.*

Proof. For simplicity we shall prove the proposition for $p = 3$ only. The proof extends to a general odd prime p using the argument similar to the one used in the proof of (2.3.4), but the details are too cumbersome to write.

For $p = 3$ the γ sequence is given by,

$$\gamma(k) = \alpha(k) \text{ for } 0 \leq k \leq 2^n - 1. \tag{2.3.37}$$

For $2^n \leq k \leq 2^{n+1} - 1$, write, $k = 2^n + 2^m s + t$, and define

$$\gamma(k) = \alpha(2^n + 2^m s)) + \beta(t). \tag{2.3.38}$$

for $0 \leq s \leq 2^{n-m} - 1$ and for $0 \leq t \leq 2^m - 1$.

$$\gamma(k) = \alpha(k), \text{ for } k \geq 2^{n+1}. \tag{2.3.39}$$

Now the proof of the proposition 2.3.6 will be followed by the following two

lemmas. □

Lemma 2.3.7. *No three $\gamma(k)$'s, for $0 \leq k \leq 2^{n+1}-1$, are in arithmetic progression.*

Proof. We have, by (2.3.4), (2.3.7) and (2.3.20), for $p = 3$,
$\gamma(0) + \gamma(2^n) = \alpha(0) + \alpha(2^n) = 3^n > 2\frac{3^n-1}{2} = 2\alpha(2^n - 1) = 2\gamma(2^n - 1)$.
And,

$$\begin{aligned}
\gamma(2^n-1) + \gamma(2^{n+1}-1) &= \alpha(2^n-1) + \alpha(2^{n+1}-2^m) + \beta(2^m-1) \\
&< \alpha(2^n-1) + \alpha(2^{n+1}-2^m) + \alpha(2^m-1) \\
&= \alpha(2^n-1) + \alpha(2^{n+1}-1) \\
&= \frac{1}{2}(3^n-1) + \frac{1}{2}(3^{n+1-1}) = \frac{1}{2}(1+3)3^n - 1 \\
&= 2.3^n - 1 < 2.3^n = 2\alpha(2^n) = 2\gamma(2^n).
\end{aligned}$$

Therefore, the average of a $\gamma(k)$, for $0 \leq k \leq 2^n - 1$ and a $\gamma(k)$, for $2^n \leq k \leq 2^{n+1} - 1$ lies in the open interval $(\gamma(2^n - 1),\ \gamma(2^n))$. Also, since, no three of $\gamma(k)$'s, for $0 \leq k \leq 2^n - 1$ are in arithmetic progression, then, to prove lemma 13, it is enough to show no three $\gamma(k)$'s, for $2^n \leq k \leq 2^{n+1} - 1$ are in arithmetic progression. For $2^n \leq k \leq 2^{n+1} - 1$, we define, $\delta(k) = \gamma(k) - \alpha(2^n)$.

We shall prove the following by induction on h.

For $0 \leq h \leq n - m$, no three of $\delta(k)$, $2^n \leq k \leq 2^n + 2^{m+h} - 1$ are in arithmetic progression.

For $2^n \leq k \leq 2^n + 2^m - 1$, $\delta(k) = \gamma(k) - \alpha(2^n) = \beta(k - 2^n)$, so the above statement holds for $h = 0$ (as no three of $\beta(k)$, $0 \leq k \leq 2^m - 1$, are in arithmetic progression). This starts the induction.

Now assume that the above statement is true for some h in the range $0 \leq h \leq n - m - 1$. We must prove that the statement remains true when h is replaced by $h + 1$, ie., we must show that no three of $\delta(k)$, $2^n \leq k \leq 2^n + 2^{m+h+1} - 1$, are in arithmetic progression.

Of course by induction hypothesis no three of $\delta(k)$ for $2^n \leq k \leq 2^n + 2^{m+h} - 1$ are in arithmetic progression. For $2^n + 2^{m+h} \leq k \leq 2^n + 2^{m+h+1} - 1$,

$$\begin{aligned}
\delta(k) = \gamma(k) - \alpha(2^n) &= \{\gamma(k) - \alpha(2^n + 2^{m+h})\} + \{\alpha(2^n + 2^{m+h}) - \alpha(2^n)\} \\
&= \beta(k - 2^n - 2^{m+h}) + \{\alpha(2^n + 2^{m+h}) - \alpha(2^n)\},
\end{aligned}$$

so no three $\delta(k)$, for $2^n + 2^{m+h} \leq k \leq 2^n + 2^{m+h+1} - 1$ are in arithmetic progression.

Induction will be completed if we can prove that average of any $\delta(k)$, $2^n \leq$

$k \leq 2^n + 2^{m+h} - 1$, and any $\delta(k)$, $2^n + 2^{m+h} \leq k \leq 2^n + 2^{m+h+1} - 1$ is not a $\delta(k)$ for $2^n \leq k \leq 2^n + 2^{m+h+1} - 1$.

We are proving this by showing that any such average lies in the open interval $\big(\delta(2^n + 2^{m+h} - 1),\ \delta(2^n + 2^{m+h})\big)$.

By properties of α, β, γ and δ sequences, we have,

$$\begin{aligned}
\text{Minimum value of such an average} &= \frac{1}{2}\{\delta(2^n) + \delta(2^n + 2m + h)\} \\
&= \frac{1}{2}\delta(2^n + 2^{m+h}),\ (\because\ \delta(2^n) = 0) \\
&= \frac{1}{2}\{\gamma(2^n + 2^{m+h}) - \alpha(2^n)\} \\
&= \frac{1}{2}\alpha(2^{m+h}) > \alpha(2^{m+h} - 1) \\
&= \alpha(2^{m+h} - 2^m) + \alpha(2^m - 1) \\
&> \alpha(2^{m+h} - 2^m) + \beta(2^m - 1) \\
&= \delta(2^n + 2^{m+h} - 1).
\end{aligned}$$

And, Maximum value of such an average

$$\begin{aligned}
&= \frac{1}{2}\{\delta(2^n + 2^{m+h} - 1) + \delta(2^n + 2^{m+h+1} - 1)\} \\
&= \frac{1}{2}\left\{\alpha(2^{m+h} - 2^m) + \beta(2^m - 1) + \alpha(2^{m+h+1} - 2^m) + \beta(2^m - 1)\right\} \\
&< \frac{1}{2}\left\{\alpha(2^{m+h} - 2^m) + \alpha(2^m - 1) + \alpha(2^{m+h+1} - 2^m) + \alpha(2^m - 1)\right\} \\
&= \frac{1}{2}\{\alpha(2^{m+h} - 1) + \alpha(2^{m+h+1} - 1)\} < \alpha(2^{m+h}) = \delta(2^n + 2^{m+h}).
\end{aligned}$$

This completes the proof of lemma 2.3.7. □

To complete the proof of the proposition 2.3.6, one proves the following lemma by induction on $h \geq 1$.

Lemma 2.3.8. *No three terms of $\gamma(k)$, for $0 \leq k \leq 2^{n+h} - 1$, are in arithmetic progression.*

Proof. The lemma 2.3.8 holds for $h = 1$ by lemma 2.3.7. This starts the induction. Let us assume that the statement of lemma 2.3.8 is true for some $h \geq 1$. To complete the induction we must show that the lemma 2.3.8 is true if we replace h by $h + 1$.

No three $\gamma(k)$ for $0 \leq k \leq 2^{n+h} - 1$ are in arithmetic progression (by induction

hypothesis). Since $\gamma(k) = \alpha(k)$, for $k \geq 2^{n+1}$, then no three of $\gamma(k)$ for $2^{n+h} \leq k \leq 2^{n+h+1} - 1$ are in arithmetic progression.

The proof will be completed if we can prove that the average of any $\gamma(k)$ for $0 \leq k \leq 2^{n+h} - 1$ and any $\gamma(k)$ for $2^{n+h} \leq k \leq 2^{n+h+1} - 1$ is not a $\gamma(k)$ for $0 \leq k \leq 2^{n+h+1} - 1$.

We may give same argument as in the proof of lemma 2.3.7 to show that any such an average lies in the open interval $(\gamma(2^{n+h} - 1),\ \gamma(2^{n+h}))$.

This completes the proof of lemma 2.3.8. □

2.3.4 Proofs of the main theorems

In this section we present the proofs of theorem 2.3.1 and theorem 2.3.2.

We have, by (2.3.32),

$$\begin{aligned}
&\sum_{k=0}^{(p-1)^{n+1}-1} \frac{1}{1+\gamma(k)} \\
&= \sum_{k=0}^{(p-1)^{n}-1} \frac{1}{1+\gamma(k)} \\
&\quad + \sum_{l=1}^{p-2} \sum_{s=0}^{(p-1)^{n-m}-1} \left[\sum_{k=s(p-1)^m}^{(s+1)(p-1)^m-1} \left\{ \frac{1}{1+\gamma\left(l(p-1)^n+k\right)} \right\} \right] \\
&= \sum_{k=0}^{(p-1)^{n}-1} \frac{1}{1+\alpha(k)} \\
&\quad + \sum_{l=1}^{p-2} \sum_{s=0}^{(p-1)^{n-m}-1} \left[\sum_{t=0}^{(p-1)^{m}-1} \frac{1}{1+\alpha\left(l(p-1)^n+s(p-1)^m\right)+\beta(t)} \right] \\
&> \sum_{k=0}^{(p-1)^{n}-1} \frac{1}{1+\alpha(k)} \\
&\quad + \sum_{l=1}^{p-2} \sum_{s=0}^{(p-1)^{n-m}-1} \left[\sum_{t=0}^{(p-1)^{m}-1} \left\{ \frac{1}{1+\alpha\left(l(p-1)^n+s(p-1)^m\right)+\alpha(t)} \right\} \right] \\
&= \sum_{k=0}^{(p-1)^{n+1}-1} \frac{1}{1+\alpha(k)}.
\end{aligned}$$

Therefore,

$$\sum_{k=0}^{(p-1)^{n+1}-1} \frac{1}{1+\gamma(k)} > \sum_{k=0}^{(p-1)^{n+1}-1} \frac{1}{1+\alpha(k)}. \tag{2.3.40}$$

Proof of theorem 2.3.1

Proof. Let $N = (p-1)^{n+1} - 1$. Then for $R \geq N$, by (2.3.36) and (2.3.40), we have,

$$\begin{aligned}\sum_{k=0}^{R} \frac{1}{1+\gamma(k)} &= \sum_{k=0}^{k=N} \frac{1}{1+\gamma(k)} + \sum_{k=N+1}^{k=R} \frac{1}{1+\gamma(k)} \\ &> \sum_{k=0}^{k=N} \frac{1}{1+\alpha(k)} + \sum_{k=N+1}^{k=R} \frac{1}{1+\alpha(k)} \\ &= \sum_{k=0}^{R} \frac{1}{1+\alpha(k)}\end{aligned}$$

And by proposition 2.3.6 we know no p terms of $\gamma(k)$ for $0 \leq k \leq R$ are in arithmetic progression.

This proves the theorem 2.3.1. □

Proof of theorem 2.3.2

Proof. We have, by (2.3.33), (2.3.35), (2.3.36) and (2.3.40),

$$\begin{aligned}\sum_{k=0}^{\infty} \frac{1}{1+\gamma(k)} &= \sum_{k=0}^{k=N} \frac{1}{1+\gamma(k)} + \sum_{k=N+1}^{k=\infty} \frac{1}{1+\gamma(k)} \\ &> \sum_{k=0}^{k=N} \frac{1}{1+\alpha(k)} + \sum_{k=N+1}^{k=\infty} \frac{1}{1+\alpha(k)} \\ &= \sum_{k=0}^{\infty} \frac{1}{1+\alpha(k)}\end{aligned}$$

And by proposition 2.3.6, no p terms of $\gamma(k)$ for $k \geq 0$ are in arithmetic progression.

This proves the theorem 2.3.2. □

Remark

Here we have constructed one sequence (viz, the sequence γ) of positive integers having no p terms in arithmetic progression whose sum of reciprocals is bigger than that of the terms of greedy sequence. We may construct better sequence than the sequence γ as follows.

Define the sequence θ as follows. For $0 \leq k \leq p^{n+1} - 1$, we define $\theta(k) = \gamma(k)$ and for each $h \geq 1$ we define $\theta(k)$, for $(p-1)^{n+h} \leq k \leq (p-1)^{n+h+1} - 1$, inductively as follows. For $1 \leq l \leq p-2$ and for $l(p-1)^{n+h} \leq k \leq (l+1)(p-1)^{n+h} - 1$, write

$k = l(p-1)^{n+h}+t$, for $0 \leq t \leq (p-1)^{n+h}-1$ and define $\theta(k) = \alpha(l(p-1)^{n+h})+\gamma(t)$. Then no p terms of the θ sequence are in arithmetic progression. But the sum of the reciprocals of the terms of the sequence $\{\theta(n)+1\}_{n\geq 0}$ is bigger that the sum of the reciprocals of the terms of the sequence $\{\gamma(n)+1\}_{n\geq 0}$.

We may improve this further. In lemma 2.3.4 we take that sequence β which minimizes $\sum_{k=0}^{(p-1)^m-1} \beta(k)$. Then by lemma 2.3.5 this sequence β will maximize $\sum_{k=0}^{(p-1)^m-1} \frac{1}{M+\beta(k)}$, for all sufficiently large $M > 0$. Then we define the sequences γ and θ with this sequence β.

2.4 Related problems

In this section we consider Graham's conjecture [Gra04], the two dimensional version of the Erdös conjecture.

Conjecture 2 (Graham)**.** *If $A \subset \mathbb{N} \times \mathbb{N}$ satisfy*

$$\nu(A) = \sum_{(x,y)\in A} \frac{1}{x^2+y^2} = \infty$$

then A contains 4 vertices of an axes-parallel square.

More generally, A will always contain a homothetic image of $\{1,2,\ldots,p\} \times \{1,2,\ldots,p\}$ for all $p \in \mathbb{N}$ i.e. A contains a $p \times p$ square grid.

Assuming Graham's conjecture we can derive the theorems similar to theorem 2.2.1 and theorem 2.2.2 corresponding to Erdös conjecture.

Let Θ_p be the collection of all subsets of $\mathbb{N} \times \mathbb{N}$ containing no $p \times p$ square grid.

Theorem 2.4.1. *If Graham's conjecture is true then there is a positive absolute constant B_p such that*

$$\mathrm{Sup}\{\nu(A) : A \in \Theta_p\} \leq B_p.$$

Proof. Let $A_0 = \{(1,1)\} \in \Theta_p$. If we assume that the statement of the theorem is not true, then inductively we produce a sequence of increasing finite sets $\{A_k\}_{k\geq 0} \subset \Theta_p$ as follows.

Let $m_k = \max_{(x,y)\in A_k}(|x|+|y|)$. Choose $n_k \in \mathbb{N}$ and $B_k \in \Theta_p$, such that

$$\nu(B_k) \geq m_k^2.$$

Let $A_{k+1} = A_k \bigsqcup m_k B_k$. It is easy to verify that $A_{k+1} \in \Theta_p$ and

$$\nu(A_{k+1}) - \nu(A_k) = \sum_{(x,y)\in B_k} \frac{1}{(m_k x)^2 + (m_k y)^2} = \frac{\nu(B_k)}{m_k^2} \geq 1.$$

Now $A_\infty = \bigcup A_k \in \Theta_p$ and $\nu(A_\infty) = \infty$. This contradicts the Graham conjecture. Hence we have the theorem. □

2.4.1 ν is continuous

Lemma 2.4.2. *Suppose the Graham conjecture is true. Given any $\varepsilon > 0$, there exists a natural number N such that for all $A \in \Theta_p$ with*

$$\gamma(A) \doteq \min_{(x,y)\in A} \sqrt{x^2+y^2} \geq N : \nu(A) < \varepsilon.$$

Proof. We argue by contradiction and assume that there exists some $\varepsilon > 0$ such that for any given $M \geq 1$, there exists a set $R \in \Theta_p$ such that $\gamma(R) \geq 2M$ and $\nu(R) > \varepsilon$. For that ε, we choose a set $A \in \Theta_p$ satisfying $\nu(A) > M_p - \frac{\varepsilon}{12}$ where $M_p = \sup\{\nu(A) : A \in \Theta_p\} < \infty$.

Furthermore, one can choose $M \geq 1$ and corresponding R such that

$$\nu\left(A \bigcap \{(x,y) \in \mathbb{N}\times\mathbb{N} : \sqrt{x^2+y^2} \leq M\}\right) > M_p - \frac{\varepsilon}{6}.$$

Now we divide $R = R_1 \sqcup R_2 \sqcup R_3 \sqcup R_4$ where

$$R_j = R \bigcap \left\{(x,y) \in \mathbb{N}\times\mathbb{N} : \sqrt{x^2+y^2} \in \bigsqcup_{i=0}^{\infty} [(j+1)3^i M, (j+2)3^i M]\right\};$$

j=1,2,3,4.

It is easy to check that $R_j \sqcup A_M \in \Theta_p$, for $j = 1,2,3,4$, where

$$A_M = A \bigcap \{(x,y) \in \mathbb{N}\times\mathbb{N} : \sqrt{x^2+y^2} \leq M\}$$

Also for some j, $1 \leq j \leq 4$, we have

$$\nu(R_j) > \frac{\varepsilon}{4}, \quad \nu(A_M \sqcup R_j) > M_p + \frac{\varepsilon}{12}.$$

□

Corollary 2.4.3. *Under the assumption of the Graham conjecture, there is a set*

$M_p \in \Theta_p$ such that

$$\nu(X) \leq \nu(M_p) \text{ for all } X \in \Theta_p.$$

That is, the supremum of the set $\{\nu(X) : X \in \Theta_p\}$ is attained.

It is natural to guess the following:

Conjecture 3. *If $A \subset \mathbb{N}^m$ satisfy*

$$\nu(A) = \sum_{(x_1,x_2,\ldots,x_m)\in A} \frac{1}{x_1^m + x_2^m + \cdots + x_m^m} = \infty$$

then A contains 2^m vertices of an axes-parallel m-dimensional cube.

More generally, A will always contain a homothetic image of $\{1, 2, \ldots, p\}^m$ for all p, i.e., A contains an m-dimensional $p \times \cdots \times p$ (m times*) cubic grid.*

Dr. Lianagpan Li has communicated to me the proof of the fact that the higher dimensional Graham conjecture implies lower dimensional Graham conjecture.

Chapter 3

Smooth numbers I.

3.1 Introduction

Smooth numbers are positive integers having only small prime factors, and hence, they are, in some sense, opposite of almost primes which are numbers having only a few prime factors. Given a positive number y, an integer n is said to be a y-smooth if all the prime factors of n are less than or equal to y. Smooth numbers play an important role in prime number theory and in many other applied fields. For example the results on smooth numbers are used to construct large gaps between consecutive primes [Ran38] and in the analysis of algorithm and primality testing as in the works of Pomerance [Pom87] and Lenstra [Len87]. The results on smooth numbers are also used in some other problems in number theory: On Waring's problem by Vaughan [Vau89] and Wooley [Woo92]; On Fermat's conjecture by H. Lehmer and E. Lehmer [LL41]; On Bounds of the least kth power non-residues by Vinogradov [Vin26]. It is of considerable importance for various applications to count the number of y-smooth numbers in interval $[1, x]$. This number is denoted by $\Psi(x, y)$. Apart from the applicable side, studying the asymptotic behaviour of $\Psi(x, y)$ is by itself very interesting. In 1938, Rankin [Ran38] found the following upper bound for the function $\Psi(x, y)$:

$$\Psi(x, y) \ll xe^{-u/2} \log y \quad (x \geq 1, \quad y \geq 2), \tag{3.1.1}$$

where, $u = \frac{\log x}{\log y}$. By carefully handling Rankin's method, Tenenbaum (see [Ten95] or [Ten90]) was able to remove the $\log y$ factor from (3.1.1) and he proved

$$\Psi(x, y) \ll xe^{-u/2} \quad (x \geq y \geq 2). \tag{3.1.2}$$

We shall discuss this method in section 2.

In 1930, Dickman [Dic30] obtained the following asymptotic formula for $\Psi(x,y)$. For each fixed u, there is a constant $\rho(u)$ such that

$$\Psi(x,y) \sim x\rho(u) \text{ as } x \to \infty. \tag{3.1.3}$$

This ρ, considered as a function of u is monotonically decreasing, continuous, and satisfies the following differential- difference equation:

$$u\rho'(u) = -\rho(u-1) \quad (u>1), \tag{3.1.4}$$

$$\text{with the initial condition} \quad \rho(u) = 1 \quad (0 \le u \le 1). \tag{3.1.5}$$

This functions is called the Dickman function and sometimes, the Dickman-de Bruijn function; and we shall study this function in some details.

In 1951, de Bruijn [Bru51b] showed that

$$\Psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\} \tag{3.1.6}$$

holds uniformly in the range

$$y \ge 2, \ \ 1 \le u \le (\log y)^{3/5-o(1)}; \ \text{ that is, for } \ y > \exp\left((\log x)^{5/8+o(1)}\right). \tag{3.1.7}$$

In 1986 Hildebrand [Hil86a] improved the range (3.1.7) to

$$y \ge 2, \ \ 1 \le u \le \exp\left\{(\log y)^{3/5-o(1)}\right\}; \ \text{ that is, for } \ y > \exp\left((\log\log x)^{5/3+o(1)}\right). \tag{3.1.8}$$

In what range is the above asymptotic is valid? Hildebrand [Hil84] showed that the above asymptotic formula holds uniformly for

$$1 \le u \le y^{1/2-o(1)}; \ \text{ that is, for } \ y \ge (\log x)^{2+o(1)}, \tag{3.1.9}$$

if and only if the Riemann Hypothesis is true.

In 1983, Canfield, Erdös, and Pomerance [CEP83] proved that

$$\Psi(x,y) = \frac{x}{u^{u+o(u)}} \tag{3.1.10}$$

holds for

$$u \le y^{1-o(1)} \text{ with } u \to \infty; \ \text{ that is, for } \ y \ge (\log x)^{1+o(1)} \text{ as } x \to \infty. \tag{3.1.11}$$

In 1986, Hildebrand [Hil86b] improved the asymptotic formula (3.1.10) to

$$\Psi(x,y) = x\rho(u)\exp\left\{O\left(u\exp\left(-(\log u)^{3/5-o(1)}\right)\right)\right\} \tag{3.1.12}$$

in the same range.

We shall discuss briefly some of the methods used to prove these results in section 2.

For two positive numbers x, z, $\Psi(x+z,y) - \Psi(x,y)$ counts the number of y-smooth numbers in the interval $(x, x+z]$. We have good estimate of this quantity if both z/x and y are large enough. Granville has conjectured [Gra00] that the following should hold:

$$\Psi(x+c\sqrt{x},y) - \Psi(x,y) \gg \sqrt{x}/u^{u+o(u)}, \tag{3.1.13}$$

for $y > L(x)^{c'}$ for some fixed c, $0 < c < 4$ and for all sufficiently small $c' > 0$. Here $u = \frac{\log x}{\log y}$ and $L(x) \doteq \exp\{\sqrt{\log x \log\log x}\}$. Having such a bound will have application to Lenstra's elliptic curve factoring method [Gra00]. In fact, a well-known problem in this theory (see, for example [Gra00], page 26) is to show that for every $\alpha > 0$, there is at least one x^α-smooth number in an interval of length $\sqrt{x}$ around x for all sufficiently large x. In chapter 5 we have proved this conjecture under the hypothesis that $\zeta(1/2+it) \ll (t+2)^{\alpha/2+o(1)}$. This was not known even assuming the Riemann Hypothesis (see [Xuan99]).

3.2 Estimates for $\Psi(x,y)$.

Let x be a positive number and $S(x,y)$ be the set of all y-smooth numbers not exceeding x. In this section we exhibit briefly many important techniques introduced by several authors to estimate $\Psi(x,y)$. Most of these are taken from the article [Gra00] by A. Granville and the book [Ten95] by G. Tenenbaum. In the rest of the chapter we let $u = \frac{\log x}{\log y}$ and let the first $k = \pi(y)$ primes be $2 = p_1 < 3 = p_2 < p_3 < \ldots < p_{k-1} < p_k$.

3.2.1 Elementary combinatorics.

Clearly $n \in S(x,y)$ if and only if we can write n as $n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k} \le x$ where $a_i's$ are non-negative integers. Therefore evidently $\Psi(x,y)$ is the number of non-negative integer solutions in $a_i's$ of the following inequality.

$$a_1\log p_1 + a_2\log p_2 + \cdots + a_k\log p_k \le \log x. \tag{3.2.1}$$

Since $\log 2 \leq \log p_i \leq \log p_k$, for $1 \leq i \leq k$, we have

$$\left(\begin{array}{c} [u]+k \\ k \end{array} \right) \leq \quad \Psi(x,y) \quad \leq \left(\begin{array}{c} A+k \\ k \end{array} \right),$$

where $A = \left[\frac{\log x}{\log 2}\right]$. Now using prime number theorem $[k = \pi(y) \sim \frac{y}{\log y}]$ we have, if $c \log x < k < \varepsilon \frac{\log x}{\log \log x}$ and y is large enough then

$$\frac{A^k}{k!} \gg \Psi(x,y) \gg \frac{u^k}{k!}. \tag{3.2.2}$$

For details of this method we refer to the survey article of Andrew Granville [Gra00].

3.2.2 Geometric method: lattice points.

We note that $\Psi(x,y)$ is the number of solution of the inequality (3.2.1) which is equal to the number of lattice points inside the k dimensional tetrahedron given by $a_i \geq 0$ and inequality (3.2.1). This quantity is equal to the number of unit boxes (hence the total volume of the unit boxes) whose side are parallel to the axes and which have one corner one of this lattice points as the nearest point to the origin. These boxes contain the above k-dimensional tetrahedron and hence the total volume of the tetrahedron is less than or equal to the total volume of these unit boxes. On the other hand, these unit boxes are contained inside the tetrahedron

$\{(a_1, a_2, \cdots, a_k) : \quad a_i \geq 0, \quad \sum_{i=1}^{k} (a_i - 1) \log p_i \leq \log x\}$

and hence the volume of this k-dimensional tetrahedron is greater than or equal to the 'total volume' of those unit boxes.

Therefore, we have

$$\frac{1}{k!} \prod_{p \leq y} \frac{\log x}{\log p} \leq \Psi(x,y) \leq \frac{1}{k!} \prod_{p \leq y} \frac{\log X}{\log p} \tag{3.2.3}$$

where $\log X = \log x + \sum_{p \leq y} \log p$.

Using the prime number theorem ($\sum_{p \leq y} \log p \sim y$) coupled with the ideas as above, Ennola [Enn69] proved the following asymptotic formula.

Theorem 3.2.1 (Ennola, 1969)**.**

$$\Psi(x,y) = \frac{1}{\pi(y)!} \prod_{p \leq y} \left(\frac{\log x}{\log p} \right) \left\{ 1 + O\left(\frac{y^2}{\log x \log y} \right) \right\} \tag{3.2.4}$$

which holds in the range $2 \leq y \leq \sqrt{(\log x \log\log x)}$ *uniformly.*

For the details of the proof, the reader is referred to the book [Ten95] by Tenenbaum (page 363).

3.2.3 Rankin's upper bound method.

In 1938, Rankin introduced [Ran38] the following clever technique to obtain an upper bound of $\Psi(x,y) = \#(S(x,y))$. Let $P(n)$ be the largest prime factor of n and define the function $\chi(n,y)$ by

$$\chi(n,y) = \begin{cases} 1 & \text{if } P(n) \leq y \\ 0 & \text{otherwise} \end{cases} \tag{3.2.5}$$

Clearly for any $\sigma > 0$ we have,

$$\Psi(x,y) = \sum_{n \leq x} \chi(n,y) \leq \sum_{n \leq x} \left(\frac{x}{n}\right)^{\sigma} \chi(n,y) = x^{\sigma} \prod_{p \leq y} \left(1 - \frac{1}{p^{\sigma}}\right)^{-1}.$$

Now the idea is to minimize the last expression as a function of $\sigma > 0$ using calculus. Taking logarithm of this function and differentiating it with respect to σ and equating that with 0 we get

$$\log x = \sum_{p \leq y} \frac{\log p}{p^{\sigma} - 1}. \tag{3.2.6}$$

The equation (3.2.6) in σ has a unique solution (say $\alpha(x,y)$) as the right hand side of (3.2.6) is a continuous and decreasing function of σ and it decreases from ∞ to 0. In fact one can show that (see the above mentioned book, page 360)

$\alpha(x,y) = \frac{\log(1+y/\log x)}{\log y} \left\{1 + O\left(\frac{\log\log y}{\log y}\right)\right\} \approx 1 - \frac{u \log u}{\log y}$,

where the last approximation is valid if $\alpha > 1/2$.

In 1966, a more careful analysis of Rankin's upper bound method by de Bruijn [Bru66] (and later more precisely by Tenenbaum [Ten90]), resulted in the following theorem.

Theorem 3.2.2 (de Bruijn)**.** *We have uniformly for $x \geq y \geq 2$,*

$$\log \Psi(x,y) = Z\left\{1 + O\left(\frac{1}{\log y} + \frac{1}{\log\log 2x}\right)\right\}, \tag{3.2.7}$$

$$\text{where, } Z := \frac{\log x}{\log y}\log\left(1+\frac{y}{\log x}\right) + \frac{y}{\log y}\log\left(1+\frac{\log x}{y}\right)$$

$$= u\int_0^1 \log\left(1+\frac{y}{v\log x}\right)dv. \tag{3.2.8}$$

Using the same method, C. Pomerance, in 1989, taking $y = (\log x)^A$ for $A > 1$ and $\sigma = 1 - 1/A$, derived the following estimate

$$\Psi(x,(\log x)^A) = x^{1-1/A+O(1/\log\log x)}. \tag{3.2.9}$$

3.2.4 Functional equation.

$\Psi(x,y)$ satisfies the following functional equation.

Theorem 3.2.3. *For $x,\ y \geq 1$, we have*

$$\Psi(x,y) = 1 + \sum_{p\leq y}\Psi(x/p,p). \tag{3.2.10}$$

Proof. $n > 1$ is counted in $\Psi(x,y)$ if and only if we can write $n = mp$, where $P(n) = p$ and $P(m) \leq p$. Therefore for each $n > 1$, $n \in S(x,y)$, there is unique pair (p,m) satisfies the conditions $n = pm$, $P(n) = p$ and $P(m) \leq p$. Hence

$$\Psi(x,y) - 1 = \sum_{p\leq y}\sum_{\{n\leq x,\ P(n)=p\}} 1 = \sum_{p\leq y}\sum_{\{m\leq x/p,\ P(m)\leq p\}} 1 = \sum_{p\leq y}\Psi(x/p,p).$$

The theorem follows. □

It is straightforward that the above theorem implies the following identity.

Corollary 3.2.4 (Buchstab's Identity)**.** *For $x \geq 1$, $z \geq y \geq 1$, we have*

$$\Psi(x,z) = \Psi(x,y) + \sum_{y<p\leq z}\Psi(x/p,p). \tag{3.2.11}$$

Using Buchstab Identity, De Bruijn proved the following theorem by induction on $[u] = \left[\frac{\log x}{\log y}\right]$

Theorem 3.2.5. *For every $\varepsilon > 0$, we have,*

$$\Psi(x,y) \sim x\rho(u) \qquad (x^{\varepsilon} < y \leq x). \tag{3.2.12}$$

Once again using Buchstab's Identity one can prove [Ten95] by induction on $[u] = \left[\frac{\log x}{\log y}\right]$ the following theorem.

Theorem 3.2.6. *Uniformly for $x \geq y \geq 2$ we have,*

$$\Psi(x,y) = x\rho(u) + O\left(\frac{x}{\log y}\right). \tag{3.2.13}$$

The proof of the asymptotic formula (3.1.6) in the range (3.1.8) due to Hildebrand based on another functional equation.

Theorem 3.2.7 (Hildebrand Identity)**.** *For $x \geq 1$ and $y \geq 2$, $\Psi(x,y)$ satisfies the following functional equation.*

$$\Psi(x,y)\log x = \int_1^x \frac{\Psi(t,y)}{t}dt + \sum_{p^m \leq x,\ p \leq y} \Psi(\frac{x}{p^m}, y)\log p. \tag{3.2.14}$$

Proof. We consider the sum

$$S := \sum_{n \in S(x,y)} \log n = \sum_{n \leq x,\ P(n) \leq y} \log n = \sum_{n \leq x} \chi(n,y)\log n.$$

Now we evaluate it in two different ways. On one hand, an application of the partial summation formula gives us

$$S = \sum_{n \leq x} \chi(n,y)\log n = \Psi(x,y)\log x - \int_1^x \frac{\Psi(t,y)}{t}dt.$$

On the other hand, by writing $\log n = \sum_{p^m | n} \log p$ in S and interchanging the order of the summation, we have

$$\begin{aligned} S &= \sum_{n \leq x} \chi(n,y)\log n = \sum_{n \leq x} \sum_{p^m | n} \log p \ \ \chi(n,y) \\ &= \sum_{p^m \leq x} \sum_{n \leq \frac{x}{p^m}} \chi(n,y) = \sum_{p^m \leq x,\ p \leq y} \Psi(\frac{x}{p^m}, y). \end{aligned}$$

We get the identity (3.2.14) by equating these two expressions of S. Hence we have the result. □

3.2.5 The saddle point method.

In 1986 Hildebrand and Tenenbaum [HT86] proved the following theorem.

Theorem 3.2.8. *Uniformly in the range $x \geq y \geq 2$, we have*

$$\Psi(x,y) = \frac{x^{\alpha}\zeta(\alpha,y)}{\alpha\sqrt{2\pi\phi_2(\alpha,y)}}\left\{1 + O\left(\frac{1}{u} + \frac{\log y}{y}\right)\right\}, \tag{3.2.15}$$

where
$$\zeta(s,y) = \prod_{p \leq y}(1-p^{-s})^{-1} \tag{3.2.16}$$

$$\phi(s,y) = \log\zeta(s,y), \quad \phi_k(s,y) = \frac{d^k}{ds^k}\phi(s,y) \ \ (k \geq 1) \tag{3.2.17}$$

and $\alpha(x,y)$ is given by the unique positive solution of the equation (3.2.6).

They start with the well-known contour integral used in the Perron formula. Fix $\alpha > 0$. Then

$$\frac{1}{2\pi i}\int_{Re(s)=\alpha}\frac{y^s}{s}ds = \begin{cases} 0 & \text{if } 0 < y < 1 \\ 1/2 & \text{if } y = 1 \\ 1 & \text{if } y > 1 \end{cases}$$

Using the above, we have

$$\begin{aligned} \Psi(x,y) &= \sum_{n \leq x}\chi(n,y) = \frac{1}{2\pi i}\sum_{n \geq 1}\int_{Re(s)=\alpha}\frac{(x/n)^s}{s}ds + O(1) \\ &= \frac{1}{2\pi i}\int_{Re(s)=\alpha}\left(\sum_{n \geq 1}\frac{\chi(n,y)}{n^s}\right)\frac{x^s}{s}ds + O(1) \\ &= \frac{1}{2\pi i}\int_{Re(s)=\alpha}\zeta(s,y)\frac{x^s}{s}ds + O(1), \end{aligned} \tag{3.2.18}$$

where $\zeta(s,y) := \prod_{p \leq y}(1-p^{-s})^{-1}$. Take $\alpha = \alpha(x,y)$, the optimization point in Rankin's Method. One can show that the main contribution to the above integral comes from a very short interval close to $\alpha(x,y)$, the saddle point, and so that

$$\Psi(x,y) = \frac{1}{2\pi i}\int_{\alpha(x,y)-i/\log y}^{\alpha(x,y)+i/\log y}\zeta(s,y)\frac{x^s}{s}ds + \text{small error}.$$

Evaluation of the above integral gives the asymptotic formula (3.2.15). For the details of the proof of this theorem we refer to their paper [HT86].

One can make some interesting deductions from this asymptotic formula. For example, if $1 \leq c \leq y$ then

$$\Psi(cx,y) = \Psi(x,y)c^{\alpha(x,y)}\left\{1 + O\left(\frac{1}{u} + \frac{\log y}{y}\right)\right\}. \tag{3.2.19}$$

Using this, one can solve an old conjecture of Erdös. It says

$$\Psi(2x,y)/\Psi(x,y) \sim \left(1+\frac{y}{\log x}\right)^{\log 2/\log y} \sim \begin{cases} 1 & \text{iff } y \le (\log x)^{1+o(1)} \\ 2 & \text{iff } y > (\log x)^{\infty} \end{cases}$$

Here 'iff' means 'if and only if', and $y > (\log x)^{\infty}$ means $y > (\log x)^A$ for every $A > 0$. In between, we have

$$\Psi(2x,y)/\Psi(x,y) \sim 2^{1-1/\alpha} \quad \text{if} \quad y = (\log x)^{\alpha+o(1)} \quad \text{with} \quad \alpha > 1.$$

3.3 The Dickman function ρ.

We have mentioned earlier that the Dickman function ρ is a non-negative continuous and monotonically decreasing function and it satisfies the differential-difference equation (3.1.4) with the initial condition (3.1.5). We have the following theorem for the Dickman function ρ.

Theorem 3.3.1. *The Dickman's function ρ satisfies the following properties.*

$$\rho(u) = \frac{1}{u}\int_{u-1}^{u} \rho(t)dt \quad (u \ge 0) \quad \text{(Integral-delay equation).} \tag{3.3.1}$$

$$\rho(u) > 0 \qquad (u > 0). \tag{3.3.2}$$

$$\rho'(u) < 0 \qquad (u > 1). \tag{3.3.3}$$

$$\rho(u) \le \frac{1}{\Gamma(u+1)} \qquad (u \ge 0). \tag{3.3.4}$$

Proof. Let us first prove the differential-difference equation (3.1.4). We shall prove by induction on $N \ge 0$ that for $N < u \le N+1$,

$$\rho(u) = \rho(N) - \int_{t=N}^{u} \rho(t-1)\frac{dt}{t}. \tag{3.3.5}$$

Clearly the result is true for $0 \le u \le 1$ as $\Psi(x,y) = x$ (since $u \le 1 \Leftrightarrow x \le y$). Let us assume the result for $N-1 < u \le N$ for some $N \ge 1$. We shall prove the result for $N < u \le N+1$. By Corollary 4, for $N < u \le N+1$ (by taking $z = x^{1/N}$ and $y = x^{1/u}$ resp.), we have

$$\begin{aligned} \Psi(x,x^{1/u}) &= \Psi(x,x^{1/N}) - \sum_{x^{1/u}<p<x^{1/N}} \Psi(\frac{x}{p},p) \\ &\approx x\rho(N) - \sum_{x^{1/u}<p<x^{1/N}} \frac{x}{p}\rho\left(\frac{\log(x/p)}{\log p}\right) \end{aligned} \tag{3.3.6}$$

as $\frac{\log(x/p)}{\log p} = \frac{\log x}{\log p} - 1 < \frac{\log x}{\log(x^{1/u})} - 1 = u - 1 \leq N$ and so we have applied the induction hypothesis. Let χ be the characteristic function of the set of all primes. Now by using the prime number theorem $\theta(T) := \sum_{p \leq T, prime} \log p = T + O(T/\log T)$ we have

$$\begin{aligned}
\sum_{x^{1/u}<p<x^{1/N}} \frac{1}{p}\rho\left(\frac{\log(x/p)}{\log p}\right) &= \sum_{x^{1/u}<n<x^{1/N}} \frac{1}{n\log n}\rho\left(\frac{\log(x/n)}{\log n}\right)(\log n)\chi(n) \\
&= \int_{T=x^{1/u}}^{x^{1/N}} \rho\left(\frac{\log x}{\log T} - 1\right)\frac{d\theta(T)}{T\log T} \\
&\approx \int_{T=x^{1/u}}^{x^{1/N}} \rho\left(\frac{\log x}{\log T} - 1\right)\frac{dT}{T\log T} \\
&= -\int_{t=u}^{N} \rho(t-1)\frac{dt}{t} \quad \text{(Putting } T = x^{1/t}\text{).} \quad (3.3.7)
\end{aligned}$$

Hence by (3.3.6) we have (3.3.5). Differentiating (3.3.5) with respect to u, we have the differential difference equation for ρ.

Now we shall prove the Integral-delay equation by induction as follows. The result is true for $0 \leq u \leq 1$ (just set $\rho(u) = 0$ for $-1 < u < 0$). Let us assume that the result is true for some $u > 0$. We shall prove that the result is true for $u + 1$. Since it is true for u then by using differential-difference equation we have

$$\begin{aligned}
u\rho(u) &= \int_{u-1}^{u} \rho(t)dt = -\int_{u-1}^{u} (t+1)\rho'(t+1)dt \\
&= -(u+1)\rho(u+1) + u\rho(u) + \int_{u}^{u+1} \rho(t)dt.
\end{aligned}$$

Therefore, $\int_u^{u+1} \rho(t)dt = (u+1)\rho(u+1)$. This completes the induction and we have proved the integral-delay equation.

Let $\theta = \inf\{t : \rho(t) = 0\} < \infty$. Since $\rho(u) = 1 > 0$ for $0 < u \leq 1$ then $\theta > 1$. But then $0 = \theta\rho(\theta) = \int_{\theta-1}^{\theta} \rho(t)dt$. This implies that $\rho(t) = 0$ for $\theta - 1 \leq t \leq \theta$ as ρ is continuous and non-negative. This contradicts the definition of θ. This proves (3.3.2).

From the differential-difference equation of ρ and (3.3.2) we get (3.3.3). This also proves that ρ is strictly monotonically decreasing function.

Clearly if $0 \leq u \leq 1$ then $\rho(u) = 1 \leq 1/\Gamma(u+1)$. Let us assume that the result is true for all u, $k - 1 \leq u \leq k$, for some $k \geq 1$. We shall show that the result is true for $u + 1$. By (3.3.1), (3.3.2), (3.3.3), and induction hypothesis we

have,

$$\begin{aligned}\rho(u+1) &= \frac{1}{u+1}\int_u^{u+1}\rho(t)dt \le \frac{1}{u+1}\rho(u)\\ &\le \frac{1}{u+1}\frac{1}{\Gamma(u+1)} = 1/\Gamma(u+2).\end{aligned}$$

This proves (3.3.4). □

3.3.1 The Laplace transform method.

One may use Laplace transform to evaluate the value of $\rho(u)$. We have the following theorem.

Theorem 3.3.2.

$$\rho(u) = \left\{1 + O\left(\frac{1}{u}\right)\right\}\sqrt{\frac{\xi'(u)}{2\pi}}\exp\left\{\gamma - u\xi(u) + \int_0^{\xi(u)}\frac{e^t-1}{t}dt\right\}, \qquad (3.3.8)$$

where γ is Euler's constant, and $\xi(u)$ is the unique positive solution of the equation $e^{\xi(u)} = 1 + u\xi(u)$.

This asymptotic formula first proved by de Bruijn [Bru51b] using contour integration and saddle point method. Canfield [Can82] proved it by combinatorial methods, Hildebrand and Tenenbaum [HT86] gave an arithmetic proof using the function $\Psi(x,y)$. The above quantitative result is due to Alladi [All82b]. A different, but complicated expansion has been given by Xuan [Xuan93].

Let $L(\rho,s)$ be the Laplace transform of ρ and let $L'(\rho,s)$ be its derivative. Using integral-delay equation we have,

$$\begin{aligned}\int_{u=0}^{\infty} u\rho(u)e^{-su}du &= \int_{u=0}^{\infty} e^{-su}\left(\int_{t=u-1}^{u}\rho(t)dt\right)du\\ &= \int_{u=0}^{\infty}\left(\int_{t=u-1}^{u}\rho(t)e^{-st}e^{-s(u-t)}dt\right)du\\ &= \int_{t=0}^{\infty}\left(\rho(t)e^{-st}\int_{u=t}^{t+1}e^{-s(u-t)}du\right)dt\\ &= \int_{t=0}^{\infty}\rho(t)e^{-st}dt\int_{v=0}^{1}e^{-sv}dv \quad (v=u-t)\\ &= L(\rho,s)\left(\frac{1-e^{-s}}{s}\right).\end{aligned}$$

Therefore,

$$-L'(\rho,s) = L(\rho,s)\left(\frac{1-e^{-s}}{s}\right)$$

Integrating this differential equation we get,

$$L(\rho,s) = L(\rho,0)\exp\left(-\int_{t=0}^{s}\frac{1-e^{-t}}{t}\right) \tag{3.3.9}$$

Using Laplace inversion formula we get,

$$\begin{aligned}\rho(u) &= \frac{1}{2\pi i}\int_{Re(s)=\alpha} L(\rho,s)e^{us}ds \\ &= \frac{e^{\gamma}}{2\pi i}\int_{Re(s)=\alpha}\exp\left(us-\int_{t=0}^{s}s\frac{1-e^{-t}}{t}dt\right)ds. \end{aligned}\tag{3.3.10}$$

One can deduce (3.3.8) from (3.3.10). In 1983 Canfield, Erdös and Pomerance [CEP83] derived the following useful asymptotic for ρ.

$$\rho(u) = 1/u^{u+o(u)} \quad \text{as} \quad (u\to\infty). \tag{3.3.11}$$

One may write the last equation with more precisely as

$$\rho(u) = \left(\frac{e+o(1)}{u\log u}\right)^{u} \quad \text{as} \quad (u\to\infty). \tag{3.3.12}$$

For the proofs we refer their original paper [CEP83].

3.4 Smooth numbers in short intervals.

In the preceding section, we have discussed the distribution of smooth numbers globally. In this section, we shall discuss the distribution of smooth numbers in a short interval. More precisely we like to investigate the distribution of y-smooth numbers in an interval $(x, x+z]$ for large enough x and z quite small compared to x. Since $\Psi(x,y)\sim x\rho(u)$, one may expect that the asymptotic relation

$$\Psi\left((x,x+z],y\right) := \Psi(x+z,y)-\Psi(x,y) \sim (z/x)\Psi(x,y) = z\rho(u)$$

should hold in wide ranges of y and z.

In 1986 Hildebrand [Hil86a] proved such an asymptotic relation in the range $x\geq z\geq x/y^{5/12}$. Let us record his result here and we refer to the original paper

for the proof.

Theorem 3.4.1 (Hildebrand, 1986)**.** *For any fixed $\varepsilon > 0$, uniformly in the range*

$$y \geq 2, \quad 1 \leq u \leq \exp\left\{(\log y)^{3/5-\varepsilon}\right\}, \quad x \geq z \geq x/y^{5/12}, \tag{3.4.1}$$

we have

$$\Psi(x+z,y) - \Psi(x,y) = z\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}. \tag{3.4.2}$$

One can improve this range to $x \geq z \geq x/y^{1-o(1)}$. Since we do not know the truth of global asymptotic relation $\Psi(x,y) \sim x\rho(u)$ beyond the range (3.4.1), one cannot find, at present, the asymptotic for $\Psi(x+z,y) - \Psi(x,y)$ beyond this range in terms of $\rho(u)$. One can look, however, for an asymptotic formula beyond the above range in terms of $\Psi(x,y)$. Hildebrand and Tenenbaum [HT86] found one such.

Theorem 3.4.2 (Hildebrand-Tenenbaum, 1986)**.** *For every fixed $\varepsilon > 0$, and uniformly for $x \geq y \geq 2$ and $1 \leq z \leq x$, we have*

$$\Psi(x+z,y) - \Psi(x,y) = \frac{z\alpha(x,y)}{x}\Psi(x,y)\left\{1 + O\left(\frac{z}{x} + \frac{1}{u} + \frac{\log y}{y}\right)\right\} + O\left(\Psi(x,y)R_\varepsilon\right), \tag{3.4.3}$$

where $\alpha(x,y)$ is the saddle point of Rankin's Method and

$$R_\varepsilon(x,y) = \exp\left\{-(\log y)^{3/2-\varepsilon}\right\} + (\log y)\exp\left\{-cu/(\log(u+2))^2\right\},$$

for some constant $c > 0$.

It is easy to prove that the second error term is dominated by the first error term if $z \geq x\exp\left\{-(\log y)^{3/2-\epsilon}\right\}$. The above theorem gives very good estimates for the function $\Psi(x+z,y) - \Psi(x,y)$, provided z is close enough to x. The question is how far the asymptotic $\Psi(x+z,y) - \Psi(x,y) \sim z\rho(u)$ holds. In 1993, Friedlander and Granville [FG93] proved such a formula in the range

$$\exp\left((\log x)^{5/6+o(1)}\right) \leq y \leq x \quad \text{and} \quad \sqrt{x}y^2\exp\left((\log x)^{1/6}\right) \leq z \leq x. \tag{3.4.4}$$

A challenging problem in this area is to prove the above when z is an arbitrary power of x. More specifically if $\beta < 1$, $\alpha > 0$ then one wants to show that

$$\Psi(x + x^\beta, x^\alpha) - \Psi(x, x^\alpha) \sim x^\beta\rho(1/\alpha). \tag{3.4.5}$$

Thus equation (3.4.4) gives this for $\beta > 1/2 + 2\alpha$.

Due to inaccessibility of such an asymptotic relation (3.4.5) by current techniques, one modifies the problem in two directions. Find upper and lower bounds of $\Psi(x+z,y)-\Psi(x,y)$ in the same range with correct order of magnitude. One also looks for the asymptotic formula (3.4.5) with a "small" exceptional set. In 1971, Wolke [Wol71] and in 1985, Hildebrand [Hil85] gave upper bounds for $\Psi(x+z,y)-\Psi(x,y)$. Here more difficult problem is to obtain a lower bound with the right size and in a wide range. In 1987, Friedlander and Lagarias [FL87] gave the following lower bound for $\Psi(x+z,y)-\Psi(x,y)$.

Theorem 3.4.3. *There exists a constant $c>0$ such that, for any fixed $\alpha\in(0,1)$ and $\beta>1-\alpha-c\alpha(1-\alpha)$ and for all sufficiently large x, we have*

$$\Psi(x+x^{\beta},x^{\alpha})-\Psi(x,x^{\alpha})\gg_{\alpha,\beta} x^{\beta}. \tag{3.4.6}$$

The equation (3.4.4) gives such a lower bound for $\beta>1/2+2\alpha$ and $\alpha>0$. It seems very hard to prove such a lower bound for $\beta=1/2$. In fact, proving $\Psi(x+x^{1/2},x^{\alpha})-\Psi(x,x^{\alpha})>0$ is itself one of the most challenging problem in this area (see [Gra00], page 26). Despite the difficulty, some progress has been made towards solving the problem. In 1987, A. Balog [Balo87] proved that for every $\alpha>0$, there is an x^{α}-smooth number in the interval $(x,x+x^{1/2+o(1)}]$. In 1991, Harman [Har91] improved the smoothness of Balog's result by showing that for every $\varepsilon>0$ and $y\geq\exp\left((\log x)^{2/3+\varepsilon}\right)$, there is a y-smooth number in the interval $(x,x+x^{1/2+o(1)}]$. In 1993 Lenstra, Pila and Pomerance [LPP93] made it stronger by giving explicit lower bound of correct order of magnitude. In 1999, Xuan [Xuan99] improved Balog's result conditionally by proving that if the Riemann Hypothesis is true then there is an x^{α} smooth number in any interval $(x,x+\sqrt{x}(\log x)^{1+o(1)}]$ for all sufficiently large x. In chapter 5, we shall prove, under an assumption weaker than Lindelöf, that there is an x^{α}th smooth number in the interval $(x,x+(\log x)^{-1/2+o(1)}\sqrt{x}]$, for all sufficiently large x.

In the other direction, in 1987, Friedlander and Lagarias [FL87] proved the following results.

Theorem 3.4.4. *For any fixed $\varepsilon>0$, $0<\beta\leq\alpha\leq1$, and for all sufficiently large X, the estimate*

$$\Psi(x+x^{\beta},x^{\alpha})-\Psi(x,x^{\alpha})\geq\frac{1}{64}\beta\rho(1/\alpha)x^{\beta} \tag{3.4.7}$$

holds for all $x\in[1,X]$ with the exception of a set of measure bounded by $\ll_{\varepsilon,\alpha,\beta} X\exp\{-(\log x)^{1/3-\varepsilon}\}$.

Theorem 3.4.5. *For any fixed $\varepsilon > 0$, for all sufficiently large X, in the range*

$$\exp\{(\log X)^{5/6+\varepsilon}\} \le y \le X, \quad y \exp\{(\log X)^{1/6}\} \le z \le X \tag{3.4.8}$$

the estimate

$$\Psi(x+z,y) - \Psi(x,y) \gg \rho\left(\frac{\log X}{\log y}\right) z \tag{3.4.9}$$

holds for all $x \in [1,X]$ with the exception of a set of measure bounded by $\ll_\varepsilon X \exp\{-\frac{1}{2}(\log X)^{1/6}\}$.

Note that in Theorem 3.4.5, we have the estimate with a better smoothness as well as a shorter interval around x compared with Theorem 3.4.4. The price one pays for this is a larger exceptional set compared with Theorem 3.4.4.

The range (3.4.8) in Theorem 3.4.5 is a consequence of Vinogradov's zero-free region for the Riemann zeta function and can be made wider if one assumes a large zero-free region. Indeed, Hafner [Haf93] proved, in 1993, that under the Riemann Hypothesis, the conclusion of Theorem 3.4.5 holds for $L(x) \le y \le x$ and $\sqrt{L(x)} \le z \le x$, where $L(x) := \exp\{\sqrt{\log x \log\log x}\}$.

An asymptotic of this type has been given by Hildebrand and Tenenbaum [HT93]. They prove the following very useful theorem.

Theorem 3.4.6 (Hildebrand-Tenenbaum 1993)**.** *For any fixed $\varepsilon > 0$, for all sufficiently large X, and for y, z satisfying (3.4.8), the estimate*

$$\Psi(x+z,y) - \Psi(x,y) = z\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}, \tag{3.4.10}$$

holds for all $x \in [1,X]$ with the exception of a set of measure bounded by $\ll_\varepsilon X \exp\{-(\log X)^{1/6-\varepsilon}\}$.

For the proof of this theorem we refer to their original paper. The proof of (3.4.4) entirely depends on this theorem.

Chapter 4

Properties of the Riemann ζ function and the Perron formula

4.1 Introduction.

In this chapter we shall present some useful results on the Riemann ζ function in the critical strip under different conjectures. We shall use these results on the ζ function in next chapter to improve the results on smooth numbers in short intervals.

4.2 Introduction to the Riemann ζ function.

The Riemann ζ function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{4.2.1}$$

for $\operatorname{Re} s > 1$.

It has a meromorphic continuation to the entire plane with only one pole at $s = 1$. The pole is of order one and of residue 1. $\zeta(s)$ satisfies the following functional equation :

$$\zeta(s) = 2^s \pi^s \sin\frac{\pi s}{2} \Gamma(1-s)\zeta(1-s), \tag{4.2.2}$$

The ζ function has zeros at the negative even integers which can be seen from the functional equation. These are called trivial zeros. All other zeros of the ζ function lie in the critical strip, $0 \leq \sigma \leq 1$. These non-trivial zeros are symmetrically distributed in the critical strip with respect to the real axis and the line $\sigma = \frac{1}{2}$.

It is known that $\zeta(s)$ has no zero on the line $\sigma = 1$. Hence, by the functional equation, all the non-trivial zeros are in the strip $0 < \sigma < 1$. The Riemann Hypothesis says that all the non-trivial zeros lie on the critical line $\sigma = \frac{1}{2}$. Let $T > 0$ and let $N(T)$ denote the number of zeros in the region $0 < \sigma < 1, 0 < t \leq T$. If T is not the ordinate of a zero, let $S(T)$ denote the value of $\pi^{-1} \arg \zeta(1/2 + it)$ obtained by continuous variation along the straight line joining 2, $2+iT$, $1/2+iT$, starting with the value 0. If T is the ordinate of a zero, let $S(T) = S(T + 0)$. Let

$$L(T) = \frac{1}{2\pi} T \log T - \frac{1 + \log 2\pi}{2\pi} T + \frac{7}{8}. \tag{4.2.3}$$

Then we have the following theorem due to Backlund [Bac14, Bac18], .

Theorem 4.2.1. *As* $T \to \infty$

$$N(T) = L(T) + S(T) + O(\frac{1}{T}). \tag{4.2.4}$$

We have $S(T) = O(\log T)$ unconditionally and $S(T) = O(\frac{\log T}{\log \log T})$ under the Riemann Hypothesis. Hence, for any fixed $h > 0$, we have,

$$N(T + h) - N(T) = O(\log T). \tag{4.2.5}$$

Also,

$$N(T + \frac{1}{\log \log T}) - N(T) = O(\log T), \tag{4.2.6}$$

unconditionally and

$$\begin{aligned} & N(T + \frac{1}{\log \log T}) - N(T) \\ = \; & \frac{1}{2\pi} \left\{ (T + \frac{1}{\log \log T}) \log(T + \frac{1}{\log \log T}) - T \log T \right\} \\ & - \frac{1 + \log 2\pi}{2\pi} \frac{1}{\log \log T} + \left\{ S(T + \frac{1}{\log \log T}) - S(T) \right\} \\ = \; & O(\frac{\log T}{\log \log T}) + O(S(T)) = O(\frac{\log T}{\log \log T}), \end{aligned} \tag{4.2.7}$$

under the Riemann Hypothesis. Again,

$$N(T + \frac{1}{\log T}) - N(T) = O(\log T), \tag{4.2.8}$$

unconditionally and

$$N(T+\frac{1}{\log T})-N(T)=O(\frac{\log T}{\log\log T}) \tag{4.2.9}$$

under the Riemann Hypothesis. Thus stronger bounds on $S(T)$ give better estimates on the distribution of the non-trivial zeros of the ζ function.

H. L. Montgomery [Mon77] proved (under the Riemann Hypothesis) that

$$\begin{aligned} S(T)=\Omega_+((\frac{\log T}{\log\log T})^{\frac{1}{2}}) \text{ i.e. } S(T)>A((\frac{\log T}{\log\log T})^{\frac{1}{2}}) \\ S(T)=\Omega_-((\frac{\log T}{\log\log T})^{\frac{1}{2}}) \text{ i.e. } S(T)<-A((\frac{\log T}{\log\log T})^{\frac{1}{2}}), \end{aligned} \tag{4.2.10}$$

for infinitely many T, and for some $A>0$. In the same paper he has conjectured that (4.2.10) represents the right rate of growth. It is thought [Odl87] likely that

$$S(T)\ll(\log T)^{1/2+\epsilon}, \tag{4.2.11}$$

for every $\epsilon>0$. Under this conjecture, we have,

Theorem 4.2.2.

$$N(T+\frac{1}{\log T})-N(T)=O((\log T)^{1/2+\epsilon}), \tag{4.2.12}$$

for every $\epsilon>0$.

Proof. Let $\epsilon>0$ be fixed. Let $T>0$. We have

$$\begin{aligned} N(T+\frac{1}{\log T})-N(T) &= \frac{1}{2\pi}\left\{(T+\frac{1}{\log T})\log(T+\frac{1}{\log T})-T\log T\right\} \\ &\quad -\frac{1+\log\ 2\pi}{2\pi}\frac{1}{\log T}+S(T+\frac{1}{\log T})-S(T) \\ &\ll \frac{1}{2\pi}T\log(1+\frac{1}{T\log T})+(\log T)^{1/2+\epsilon} \\ &\ll (\log T)^{1/2+\epsilon}, \end{aligned}$$

as $T\to\infty$. The theorem follows. □

4.3 Bounds on ζ and ζ'

The following bounds on ζ and ζ' in the critical strip are known (see Theorem 5.12, Theorem 3.5, Equation 6.19.2, Equation 3.11.7, and page 135 of [Tit86]).

$$\zeta(\frac{1}{2}+it) \ll t^{1/6}\log t, \tag{4.3.1}$$

$$\zeta(\sigma+it) \ll \log t, \ \ (\sigma \geq 1/2,\ \sigma > 1-\frac{A}{\log t},\ t \geq e) \tag{4.3.2}$$

$$\zeta(\sigma+it) \ll (1+t^{100(1-\sigma)^{3/2}})(\log t)^{2/3},\ (0 \leq \sigma \leq 2,\ t \geq 2) \tag{4.3.3}$$

$$\zeta'(\sigma+it) \ll (\log t)^2, \ \ (\sigma \geq 1/2,\ \sigma > 1-\frac{A}{\log t},\ t \geq e) \tag{4.3.4}$$

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} \ll (\log t)^{2/3}(\log\log t)^{1/3},\ \sigma \geq 1-\frac{A}{(\log t)^{2/3}(\log\log t)^{1/3}}, \tag{4.3.5}$$

$$\frac{1}{\zeta(\sigma+it)} \ll (\log t)^{2/3}(\log\log t)^{1/3},\ \sigma \geq 1-\frac{A}{(\log t)^{2/3}(\log\log t)^{1/3}}, \tag{4.3.6}$$

for some $A > 0$. The last two bounds are due to I. N. Vinogradov.

Under the Riemann Hypothesis, we have the following bounds (see theorem 14.14(A) and theorem 14.5. of [Tit86]):

$$\zeta(1/2+it) = O\left\{\exp(A\frac{\log t}{\log\log t})\right\}, \tag{4.3.7}$$

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} = O\{(\log t)^{2-2\sigma}\}, \tag{4.3.8}$$

$$\log\zeta(\sigma+it) = O\left\{\frac{(\log t)^{2-2\sigma}}{\log\log t}\right\}, \tag{4.3.9}$$

uniformly for $1/2 < \sigma_0 \leq \sigma \leq \sigma_1 < 1$.

We shall extend the range of σ to $1/2 + \frac{1}{\log\log t} \leq \sigma \leq \sigma_1 < 1$ under the Riemann Hypothesis.

Theorem 4.3.1. *If the Riemann Hypotesis is true then we have*

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} = O(\log t), \tag{4.3.10}$$

uniformly for $\frac{1}{2} + \frac{1}{\log\log t} \leq \sigma \leq \sigma_1 < 1$.

Proof. By (14.15.2) of [Tit86], we have,

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} = \sum_{|t-\gamma|<1/\log\log t} \frac{1}{s-\rho} + O(\log t), \tag{4.3.11}$$

where $\rho = \frac{1}{2} + i\gamma$ varies over the non-trivial zeros of the ζ function. But by (4.2.7) there are $O(\frac{\log t}{\log\log t})$ zeros $1/2 + i\gamma$ of the ζ function such that $\gamma \in (t - \frac{1}{\log\log t}, t + \frac{1}{\log\log t})$ and hence

$$\begin{aligned}\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} &= \sum_{|t-\gamma|<1/\log\log t} \frac{1}{\sqrt{(\frac{1}{\log\log t})^2 + (\gamma - t)^2}} + O(\log t),\\ &\ll O(\frac{\log t}{\log\log t})(\log\log t) + O(\log t) = O(\log t),\end{aligned}$$

uniformly for $1/2 + \frac{1}{\log\log t} \le \sigma \le \sigma_1 < 1$. □

With the above argument, we can say that (Under the Riemann Hypothesis)

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} = O\{(\log t)^2\}, \tag{4.3.12}$$

uniformly for $\frac{1}{2} + \frac{1}{\log t} \le \sigma \le \sigma_1 < 1$.

We can give better bound on $\frac{\zeta'}{\zeta}$ near $\frac{1}{2} + \frac{1}{\log t}$ under the conjecture $S(t) \ll (\log t)^{1/2+\epsilon}$.

Theorem 4.3.2. *Under the Riemann Hypothesis and the above conjecture, we have*

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} = O\{(\log t)^{\frac{3}{2}+\epsilon}\}, \tag{4.3.13}$$

uniformly for $\frac{1}{2} + \frac{1}{\log t} \le \sigma \le \sigma_1 < 1$.

Proof. Let $R = \left[\frac{\log t}{\log\log t}\right]$ and $\frac{1}{2} + \frac{1}{\log t} \le \sigma \le \sigma_1 < 1$.

Then by (4.3.11), we have

$$\begin{aligned}
\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} &= \sum_{|t-\gamma|<1/\log\log t} \frac{1}{s-\rho} + O(\log t), \\
&\ll \sum_{t<\gamma<t+\frac{1}{\log\log t}} \frac{1}{\sqrt{\frac{1}{(\log t)^2}+(\gamma-t)^2}} + O(\log t) \\
&\leq \sum_{k=0}^{R} \sum_{t+\frac{k}{\log t}<\gamma\leq t+\frac{k+1}{\log t}} \frac{1}{\sqrt{\frac{1}{(\log t)^2}+(\gamma-t)^2}} + O(\log t) \\
&\leq \sum_{k=0}^{R} \sum_{t+\frac{k}{\log t}<\gamma\leq t+\frac{k+1}{\log t}} \frac{\log t}{\sqrt{1+k^2}} + O(\log t) \\
&\ll \sum_{k=0}^{R} \frac{(\log t)^{\frac{3}{2}+\epsilon}}{\sqrt{1+k^2}} + O(\log t), \quad \text{(by theorem 4.2.2)} \\
&\ll (\log t)^{\frac{3}{2}+\epsilon} \int_{u=0}^{R} \frac{1}{\sqrt{1+u^2}} du + O(\log t) \\
&\ll (\log t)^{\frac{3}{2}+\epsilon} \log R \ll (\log t)^{\frac{3}{2}+\epsilon} \log\log t.
\end{aligned}$$

Hence the result follows. □

4.4 The Perron formula.

Let us record the Perron formula which will be used in several places in the next chapter.

Let $\{a_n\}$ be a sequence with $a_n \ll n^\epsilon$ for any fixed $\epsilon > 0$ and let $c > 1$. We shall write the sum $\sum_{n\leq X} a_n$ as a contour integral. The main contour integral we need is:

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s \frac{ds}{s} = E(y) + \begin{cases} 0 & \text{if } 0<y<1 \\ \frac{1}{2} & \text{if } y=1 \\ 1 & \text{if } y>1 \end{cases} \tag{4.4.1}$$

where the error estimate $E(y)$ is given by

$$|E(y)| < \begin{cases} y^c \min\{1, \frac{1}{T|\log y|}\} & \text{if } y \neq 1 \\ \frac{c}{T} & \text{if } y = 1 \end{cases} \tag{4.4.2}$$

It follows that

$$\sum_{n\leq X} a_n = \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left(\sum_{n=1}^{\infty}\frac{a_n}{n^s}\right)\frac{X^s}{s}ds + E(X), \tag{4.4.3}$$

where

$$E(X) \ll \sum_{n=1}^{\infty} a_n \left(\frac{X}{n}\right)^c \min\left\{1, \frac{1}{T|\log(X/n)|}\right\} \tag{4.4.4}$$

if X is not an integer. If X is an integer, then the X-th term in the above sum is replaced by $a_X(\frac{c}{T}+\frac{1}{2})$. For estimating the error, we break up the above sum into three parts $\{n/X > 3/2\}$, $\{n/X < 1/2\}$ and $\{1/2 \leq n/X \leq 3/2\}$. For the first two parts, $|\log(X/n)|$ is bounded from below by a fixed constant and the total contribution from these two parts is $O\left(\frac{X^{c+\epsilon}}{T}\right)$ since $\sum_{n=1}^{\infty}\frac{a_n}{n^c}$ is convergent. For the third part, write

$$|\log(X/n)| = |\log(n/X)| = |\log(1-(1-n/X))| > |1-n/X| = \frac{X}{|X-n|}.$$

Let $\{X\}$ = the integer nearest to X, if X is not an integer, and X if it is.

Define $||X|| := |X - \{X\}|$. In the third part, we can bound $\left(\frac{X}{n}\right)^c$ by $2^c \ll 1$. Each a_n is $O(X^\epsilon)$. Hence the sum over all integers in the third part except $\{X\}$ is bounded by

$$O\left(\frac{X^{1+\epsilon}}{T}\sum_{1\leq m\leq[\frac{X}{2}]}\frac{1}{m}\right) = O\left(\frac{X^{1+\epsilon}\log X}{T}\right)$$

which is absorbed in $O\left(\frac{X^{c+\epsilon}}{T}\right)$ coming from the first two parts. The term for $n = \{X\}$ has to be kept separate because $||X||$ can be arbitrarily small.

Case $X \notin \mathbb{N}$.

For the third part, using the above bound, we finally have

$$\begin{aligned} E(X) &\ll \frac{X^{c+\epsilon}}{T} + a_{\{X\}}\left(\frac{X}{\{X\}}\right)^c \min\left\{1, \frac{X}{T||X||}\right\} \\ &\ll \frac{X^{c+\epsilon}}{T} + a_{\{X\}}\min\left\{1, \frac{X}{T||X||}\right\}. \end{aligned}$$

Note that we have assumed $\left(\frac{X}{\{X\}}\right)^c \ll 1$.

So, finally we have

$$E(X) \ll \frac{X^{c+\epsilon}}{T} + a_{\{X\}} \min\left\{1, \frac{X}{T||X||}\right\}.$$

Case $X \in \mathbb{N}$

If X is an integer, then for $n \neq X$, $|X - n| > 1/2$, so we can bound all terms in the third part by $O\left(X^{1+\epsilon}/T\right)$ except the X-th term which is bounded by $a_X O(\frac{c}{T}) + \frac{a_X}{2}$ because in the sum in the left hand side, the X-th term is not a_X but $\frac{a_X}{2}$ and the corresponding error term is not $O\left(X^c \min\left\{1, \frac{1}{T|\log X|}\right\}\right)$ but $O(\frac{c}{T})$. Finally,

$$E(X) = O\left(\frac{X^{c+\epsilon}}{T}\right) + \frac{a_X}{2}$$

and letting $T \to \infty$,

$$\sum_{n \leq X} a_n = \int_{c-i\infty}^{c+i\infty} \left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right) X^s \frac{ds}{s} + \frac{a_X}{2}.$$

So for any X,

$$\sum_{n \leq X} a_n = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right) + \left(\frac{X^{c+\epsilon}}{T}\right) + O(X^{\epsilon}). \tag{4.4.5}$$

Chapter 5

Smooth Numbers II

5.1 Introduction

In this chapter we shall present the major new work we have done on the distribution of smooth numbers in short intervals. What we are interested is the following conjecture (see Smooth Numbers: Computational Number Theory and Beyond, Page 8, section 1f of A. Granville).

Conjecture 4 (A. Granville.)**.** *For some c, $0 < c < 4$, and sufficiently small $c' > 0$, we have*

$$\Psi(X + c\sqrt{X}, y) - \Psi(X, y) \gg \sqrt{X}/u^{u+o(u)} \text{ where } u = \frac{\log X}{\log y} \tag{5.1.1}$$

for $y > L(X)^{c'}$ and for all sufficiently large X.

Under the assumption of Riemann Hypothesis, Xuan [Xuan99] proved that there is an X^{α}-smooth number in any interval $(X, X + (\log X)^{1+o(1)}\sqrt{X}]$ for sufficiently large X. The best unconditional result in this direction is due to Granville and Friedlander [FG93] who proved that there are X^{α}-smooth numbers in an interval $(X, X + \sqrt{X}f(X)]$, for all sufficiently large X, where $f(X) = \exp(2(\log X)^{\frac{5}{6}+\varepsilon} + (\log X)^{\frac{1}{6}})$ for any $\varepsilon > 0$. In fact they proved this result with a better smoothness, namely, with $y = \exp((\log X)^{\frac{5}{6}+\varepsilon})$. Unfortunately, in the essential application to the Lenstra's elliptic curve factoring method, we must have $c < 4$; result for larger c have no such consequences. Lenstra's elliptic curve factoring method proceeds as follows.

Let $n \geq 2$ be a composite integer and we want to find a factor of n.

Step 1. Check that $\gcd(n, 6) = 1$ and that n does not have the form m^r for some $m, r \geq 2$. [If the $\gcd(n, 6)$ is not 1 then we have got a factor of n, viz., the

gcd and we are done.] If it is 1 then go to Step 2.

Step 2. Choose random integers b, x_1, y_1 between 1 and n. Go to Step 3.

Step 3.

$$\text{Let } \gamma = y_1^2 - x_1^3 - bx_1 \pmod{n} \text{ and let } \Gamma \text{ be the cubic curve}$$
$$\Gamma : y^2 = x^3 + bx + \gamma, \quad \text{and let } P = (x_1, y_1) \in \Gamma.$$

Step 4. Check that $\gcd(4b^3, 27\gamma^2) = 1$ [If it equals to n, go to Step 2. and choose a new b. If it is strictly between 1 and n, then it is a non-trivial factor of n, and so we are done.] If it is 1 then go to Step 5.

Step 5. Choose a number $k = LCM[1, 2, 3, \ldots, B]$, where B is any arbitrary number. Go to Step 6.

Step 6. Compute $kP = P + \cdots + P$, the k-fold sum of P.

$$\text{Let } \; kP = \left(\frac{a_k}{d_k^2}, \; \frac{b_k}{d_k^3}\right).$$

[Given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the curve

$$y^2 = x^3 + \alpha x^2 + \beta x + \gamma,$$

we define the sum $P_1 + P_2$ by the point $P_3 = (x_3, y_3)$, where x_3, y_3 are given by the following formulas.

$$x_3 = \lambda^2 - \alpha - x_1 - x_2 \quad \text{and} \quad y_3 = -\lambda x_3 - \nu,$$
$$\text{where } \; \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2\alpha x_1 + \beta}{2y_1} & \text{if } P_1 = P_2 \end{cases},$$
$$\text{and} \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.]$$

One can compute kP in $\log_2 k$ steps. But for large k one performs all computations modulo n. For the details of the computational procedure look at pages 134-136 of the book [ST92]].

Step 7. Calculate $D = \gcd(d_k, n)$. If $1 < D < n$, then D is a non-trivial factor of n and we are done. If $D = 1$, either go to Step 5 and take larger k or go to Step 2 and choose a new curve. If $D = n$ go to Step 5 and take a smaller k.

If p is a prime factor of n such that $\#\Gamma(\mathbb{F}_p)$ divides k, then this procedure is likely to factor n.

We note that if Γ is a non-singular cubic curve with coefficients in the finite

field $\mathbb{F}_p$, then

$$\#\Gamma(\mathbb{F}_p) = p + 1 + \varepsilon_p, \quad \text{where} \quad |\varepsilon_p| \leq 2\sqrt{p}.$$

Furthermore, one can show that as Γ varies over all possible such curves, the numbers $|\varepsilon_p|$ are quite well spread out over the interval $[-2\sqrt{p}, -2\sqrt{p}]$. Now if in an interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ we have a smooth number then we will run across a curve Γ with $\#\Gamma(\mathbb{F}_p)$ having a smooth factor fairly rapidly. Thus under the above assumption we shall get a smooth factor of n fairly rapidly. In fact, under this assumption, algorithm takes expected time $L(p)^{\sqrt{2}+o(1)}$ to find a factor of n.

The problem of finding a factor of n has come from a very important practical reason. Recently, mathematicians have devised new short of codes (really ciphers) based on trap-door functions built around the problem of factoring large integers. In this thesis, I am not interested to describe these new ciphers, but let us say that if a message is enciphered using the composite integer n, then one can read the message if he can factor n. So the question of factoring large integers is of great interest to the governments and businesses that wish to keep their message secret. Our main interest is on the above conjecture. In next section We shall prove that under Riemann Hypothesis and Montgomery conjecture that there are X^α-smooth numbers in an interval $(X, X + (\log X)^{1/2+o(1)}\sqrt{X}]$, for all sufficiently large X. In section 3 we have proved that under a conjecture weaker than Lindelöf Hypothesis that there are X^α-smooth numbers in an interval $(X, X + (\log X)^{-1/2+o(1)}\sqrt{X}]$, for all sufficiently large X.

5.2 Smooth numbers in short intervals.

Balog [Balo87] proved that there is always an X^α-smooth number in the interval $(X - X^{1/2+o(1)}, X]$ for all sufficiently large X. He proved it by proving the following lemma.

Lemma 5.2.1 (Balog 1987)**.** *Let $k \geq 1$ be an integer, $\frac{1}{8k} \geq \delta > 0$, $X > X_0$ be real numbers, $|a_m| \leq 1$ be arbitrary complex numbers and we define $M = X^{1/2-1/4k}$, $Y = 1/2 + 1/8k + \delta$, and finally,*

$$d_n = \sum_{m_1 m_2 | n, M < m_1, m_2 \leq 2M} a_{m_1} a_{m_2}. \tag{5.2.1}$$

Then for any $A > 0$ we have

$$\sum_{X-Y<n\leq X} d_n = Y\left(\sum_{M<m\leq 2M} \frac{a_m}{m}\right)^2 + o\left(\frac{Y}{(\log X)^A}\right). \tag{5.2.2}$$

Now if we choose $k > \max\{1/2\alpha, 1/8\varepsilon\}$ for a given $\varepsilon > 0$ and $0 < \alpha \leq 1$ and take $a_m = 1$ or 0 according as m is X^α-smooth or not, then the lemma guarantees that the interval $(X - X^{1/2+\varepsilon}, X]$ contains X^α-smooth numbers. In fact, a more careful consideration show us (as $\sum_{M<m\leq M} \frac{a_m}{m} \gg 1$) that the above interval contains $\gg X^{1/2+\varepsilon-o(1)}$ number of X^α-smooth numbers. To see this, we just put $Y = X^{1/2+\varepsilon}$ in (5.2.2). Then $\sum_{(X-Y)<n\leq X} d_n \gg X^{1/2+\varepsilon}$ and for each n, $X - Y < n \leq X$ there are at most $X^{o(1)}$ choice of triples (m_1, m_2, l) with $n = m_1 m_2 l$. By modifying Balog's argument Granville and Friedlander [FG93] proved that in any interval $(X, X + X^{1/2+\varepsilon}]$ there are $\gg_{\alpha,\varepsilon} X^{1/2+\varepsilon}$ number of X^α-smooth numbers, for all sufficiently large X.

Harman [Har91] obtained a quantitative refinement of Balog's result by showing that the smoothness in the Balog's result [Balo87] may be reduced to $\exp\left\{(\log X)^{2/3+\varepsilon}\right\}$. Lenstra, Pila and Pomerance [LPP93] slightly strengthened this result and gave an explicit lower bound of the correct order of magnitude. Xuan [Xuan99] showed, assuming the Riemann Hypothesis, that there is an X^α smooth number in any interval $[X, X + \sqrt{X}(\log X)^{1+o(1)}]$. We record his result below.

Theorem 5.2.2 (Xuan, 1999)**.** *If the Riemann Hypothesis is true, then for any $\varepsilon > 0$, $\alpha > 0$ and $X \geq X_0(\varepsilon, \alpha)$, the interval $(X, X + Y]$, where $\sqrt{X}(\log X)^{1+\varepsilon} \leq Y \leq X$, contains an integer having no prime factors exceeding X^α.*

He proved this result by proving the following lemma.

Lemma 5.2.3 (Xuan, 1999)**.** *Let $0 < \varepsilon < 1/8$ be fixed and put*

$$\begin{aligned} M &= X^{1/2}(\log X)^{-1-\varepsilon}, \qquad N = (\log X)^{2+2\varepsilon}, \\ Y &\geq \frac{X}{M} = X^{1/2}(\log X)^{1+\varepsilon}, \qquad y = X^\alpha \\ a(m) &= \begin{cases} 1 & \text{if } m \text{ is } y\text{-smooth} \\ 0 & \text{otherwise,} \end{cases} \qquad M(s) = \sum_{M<m\leq 2M} \frac{a(m)}{m}. \end{aligned}$$

Then under the Riemann Hypothesis we have

$$\int_{x=X}^{X+Y}\left(\sum\nolimits^{\star} a(m_1)a(m_2)\Lambda(r)\right)dx = Y^2M^2(1)+O\left(Y^2(\log X)^{-\varepsilon}/4\right), \quad (5.2.3)$$

where $\star$ represents the summation conditions

$$\begin{aligned} m_1m_2r &\in (x,x+Y], \quad X\le x\le X+Y,\\ M &< m_i\le 2M, \quad i=1,2. \end{aligned}$$

Remark

We note that under the lemma, for all $Y\ge \frac{X}{M}=X^{1/2}(\log X)^{1+\varepsilon}$ left side of (5.2.3) is $\gg Y^2$ as $M^2(1)\gg 1$. But the integrand $\sum^{\star}$ in (5.2.3) is non-negative. Hence there is one $x\in(X,X+Y]$ for which $\sum^{\star}\gg Y$. But for each $n\in(x,x+Y]$ number of triples (m_1,m_2,r) is $\ll X^{o(1)}$ and each such triple will contribute $\ll X^{o(1)}\log X$ to the sum. Hence there are at least $\gg X^{1/2-o(1)}$ number of different smooth numbers of the form $n=m_1m_2r$ where m_1,m_2 are y-smooth and $r\le y$ in the interval $(x,x+Y]$. Therefore number of y-smooth numbers in any interval $(X,X+Y]\gg X^{1/2-o(1)}$.

Now we shall present our main theorem. We assume the bound (5.4.12).

Theorem 5.2.4. *Assume that $\zeta(1/2+it)\ll |1+t|^{\alpha/2}$. Then for all sufficiently large X, there is an X^{α}-smooth number in the interval $(X,X+Y]$ for any $Y\gg X^{1/2}(\log X)^{-1/2+o(1)}$.*

The initial steps in our proof is similar to Xuan's [Xuan99], but in estimating an integral, we get a better bound by breaking up the interval into many small pieces according to the size of the value of the zeta function (see the estimation of I_1).

5.3 Preliminary steps

Along with the preliminaries of section 2 we record the following result on mean value of Dirichlet polynomial due to Montgomery and Vaughan [MV74].

Theorem 5.3.1. *For any sequence $\{b_n\}$ of complex numbers and any positive real number R, we have*

$$\int_0^T\left|\sum_{n\le N}b_nn^{it}\right|^2dt\ll\sum_{n\le N}|b_n|^2\{T+O(n)\}.$$

Here we use the same technique of Balog for counting the smooth numbers. Let α be fixed positive number. Define a sequence $\{a_m\}$ where

$$a_m = \begin{cases} 1 \text{ if } p|m \Rightarrow p \leq X^{\alpha}, \\ 0 \text{ otherwise.} \end{cases}$$

Let $M_1 = \sqrt{2}X^{\frac{1}{2}-\frac{\alpha}{2}}$ and $M_2 = X^{\frac{1}{2}-\frac{\alpha}{4}}$. Define a Dirichlet polynomial

$$M(s) = \sum_{M_1 \leq m \leq M_2} \frac{a_m}{m^s},$$

and define, for any positive integer n,

$$A_n = \{(m_1, m_2) : M_1 < m_1, m_2 \leq M_2, m_1 m_2 | n\}$$

and

$$d_n = \sum_{\substack{n=m_1 m_2 r, \\ (m_1,m_2)\in A_n}} a_{m_1} a_{m_2}.$$

If we can show that

$$\sum_{X < n \leq X+Y} d_n > 0,$$

with $Y < X$, then there must be some integer $n = m_1 m_2 r$ between X and $X+Y$, with m_1 and m_2 smooth and therefore n itself is smooth, because, $r = n/m_1 m_2 \leq (X+Y)/M_1^2 = X^{\alpha}$.

Now, for any $x \in [X, X+Y]$, by the Perron formula,

$$\begin{aligned} \sum_{x < n \leq x+Y} d_n &= \frac{1}{2\pi i} \int_{2-iT_0}^{2+iT_0} \zeta(s) M^2(s) \frac{(x+Y)^s - x^s}{s} ds \\ &+ O\left(\frac{X^{2+\frac{1}{100}}}{T_0}\right) + O(X^{\frac{1}{100}}), \end{aligned}$$

where T_0 is some positive real number for the moment, but later we shall choose $T_0 \gg X^4$.

We integrate this with respect to x, getting,

$$\int_X^{X+Y}\left(\sum_{x<n\le x+Y} d_n\right)dx = \frac{1}{2\pi i}\int_{2-iT_0}^{2+iT_0}\zeta(s)M^2(s)A(s)ds + O\left(\frac{YX^{2+\frac{1}{100}}}{T_0}\right) + O(YX^{\frac{1}{100}}),$$

where

$$A(s) = \frac{(X+2Y)^{s+1} - 2(X+Y)^{s+1} + X^{s+1}}{s(s+1)}.$$

Now, to show that there is a smooth number between X and $X+2Y$, it is enough to show that the left hand side is positive (for all X large enough), which is shown in the next section. This integration results in saving one $\log X$ factor.

5.4 The proof

Our goal in this section is to show that $\int_X^{X+Y}\left(\sum_{x<n\le x+Y} d_n\right)dx > 0$ for all X sufficiently large, and $Y \gg X^{1/2}(\log X)^{-1/2+o(1)}$

We move the contour to Re $s = \frac{1}{2}$, and apply the residue theorem of Cauchy, getting,

$$\int_X^{X+Y}\left(\sum_{x<n\le x+Y} d_n\right)dx = Y^2M^2(1) + \frac{1}{2\pi i}\int_{2-iT_0}^{\frac{1}{2}-iT_0} + \frac{1}{2\pi i}\int_{\frac{1}{2}-iT_0}^{\frac{1}{2}+iT_0} + \frac{1}{2\pi i}\int_{\frac{1}{2}+iT_0}^{2+iT_0} + O\left(\frac{X^{2+\frac{1}{100}}Y}{T_0}\right) + O(YX^{\frac{1}{100}}) \tag{5.4.1}$$

since $\mathrm{Res}_{s=1}\zeta(s) = 1$, and $A(1) = Y^2$. Now, by (**??**),

$$M(1) = \sum_{M_1\le m\le M_2}\frac{a_m}{m} = \int_{M_1}^{M_2}\frac{1}{t}d\left(\sum_{m\le t} a_m\right)$$

$$\gg \int_{M_1}^{M_2}\frac{1}{t}\rho(1/\alpha)dt \gg \log X. \tag{5.4.2}$$

So the first term, $Y^2M^2(1) \gg Y^2(\log X)^2$, and we shall show that this term dominates all other terms. We have the bound

$$\frac{(X+Y)^s - X^s}{s} \ll \min\left\{YX^{\sigma-1}, \frac{X^\sigma}{|t|}\right\},$$

where $s = \sigma + it$ as usual. This implies,

$$A(s) \ll \min\left\{Y^2 X^{\sigma-1}, \frac{X^{\sigma+1}}{|t|^2}\right\}. \tag{5.4.3}$$

The horizontal integrals have T_0 in the denominator and will be shown to be very small by trivial estimation. Namely, using the second bound for $A(s)$, and the bound $|\zeta(\sigma + iT)| \ll T_0$ for $0 \le \sigma \le 1$,

$$\begin{aligned}\frac{1}{2\pi i}\int_{2-iT_0}^{\frac{1}{2}-iT_0} \zeta(s)M^2(s)A(s)ds &\ll \int_2^{\frac{1}{2}} |\zeta(\sigma + iT_0)M^2(\sigma + iT_0)A(\sigma + iT)|d\sigma \\ &\ll X^{3+\frac{1}{2}}{T_0}^{-1} \ll X^{-\frac{1}{2}},\end{aligned}$$

by choosing $T_0 \gg X^4$ and similarly for the other integral $\int_{\frac{1}{2}+iT_0}^{2+iT_0}$.

Now, for estimating the vertical integral from $\frac{1}{2} - iT_0$ to $\frac{1}{2} + iT_0$, we break up the interval $[0, T_0]$ into $[0, X/Y]$ and $[X/Y, T_0]$.

$$\begin{aligned}\frac{1}{2\pi i}\int_{\frac{1}{2}-iT_0}^{\frac{1}{2}+iT_0} |\zeta(s)M^2(s)A(s)|ds &\ll \int_0^{T_0} |\zeta(\frac{1}{2} + it)M^2(\frac{1}{2} + it)A(\frac{1}{2} + it)| \\ &= \quad I_1 \quad + \quad I_2,\end{aligned}$$

where

$$I_1 = \int_0^{X/Y},$$

and

$$I_2 = \int_{X/Y}^{T_0}.$$

For $T > 2$ and positive integers $k \ge 2$, define

$$I^{(k)}(T) = \left\{0 \le t \le T : (\log T)^k \le |\zeta(1/2 + it)| \le (\log T)^{k+1}\right\}. \tag{5.4.4}$$

Let $L_1 t = \log t$ and $L_2 t = \log\log t$.

For $l \ge 0$, define

$$\begin{aligned}J^{(l)}(T) = \{&0 \le t \le T : \\ &(L_1 T)^{1/2}(L_2 T)^l \le |\zeta(\frac{1}{2} + it)| \le (L_1 T)^{1/2}(L_2 T)^{l+1}\}.\end{aligned} \tag{5.4.5}$$

$$J^{(\frac{1}{2})}(T) = \{0 \le t \le T : 0 \le |\zeta(1/2 + it)| \le (\log T)^{1/2}\}. \tag{5.4.6}$$

Note that

$$[0, \frac{X}{Y}] = J^{(\frac{1}{2})}(X/Y) \bigcup \left(\bigcup_{l=0}^{R_J} J^{(k)}(X/Y) \right) \bigcup \left(\bigcup_{k=0}^{R_I} I^{(k)}(X/Y) \right),$$

where $R_I \ll \frac{\beta \log X/Y}{\log\log X/Y}$ and $R_J \ll \frac{\beta \log\log X/Y}{\log\log\log X/Y}$ if we make the hypothesis that $|\zeta(1/2+it)| \ll |t|^\beta$ for $|t| > 1$.

Lemma 5.4.1. *The measure of the set $I^{(k)}(T)$ satisfies the bound*

$$\mu(I^{(k)}(T)) \ll \frac{T}{(\log T)^{2k-1}}. \tag{5.4.7}$$

Proof. We know that,

$$\int_0^T |\zeta(1/2+it)|^2 dt \ll T \log T. \tag{5.4.8}$$

Hence,

$$\mu(I^{(k)}(T))(\log T)^{2k} \leq \int_0^T |\zeta(1/2+it)|^2 dt \ll T \log T. \tag{5.4.9}$$

The lemma follows. □

Lemma 5.4.2. *We have, for $0 \leq k \leq R_J$,*

$$\mu(J^{(k)}(T)) \ll \frac{T}{(\log\log T)^{2k}} \tag{5.4.10}$$

Proof. By the mean value result (5.4.8), we have

$$\mu(J^{(k)}(T))(\log\log T)^{2k} \log T \leq \int_0^T |\zeta(1/2+it)|^2 dt \ll T \log T. \tag{5.4.11}$$

The lemma follows. □

Let, for $k \geq 2$,

$$I^{(k)} = \{0 \leq t \leq T_0 : (\log \frac{X}{Y})^k \leq |\zeta(1/2+it)| \leq (\log \frac{X}{Y})^{k+1}\},$$
$$I_1^{(k)} = \{0 \leq t \leq \frac{X}{Y} : (\log \frac{X}{Y})^k \leq |\zeta(1/2+it)| \leq (\log \frac{X}{Y})^{k+1}\},$$
$$I_2^{(k)} = \{\frac{X}{Y} \leq t \leq T_0 : (\log \frac{X}{Y})^k \leq |\zeta(1/2+it)| \leq (\log \frac{X}{Y})^{k+1}\}.$$

Let, for $l \geq 0$,

$$\begin{aligned}
J^{(l)} &= \{0 \leq t \leq T_0 : \\
&\quad (L_1\frac{X}{Y})^{1/2}(L_2\frac{X}{Y})^l \leq |\zeta(1/2+it)| \leq (L_1\frac{X}{Y})^{1/2}(L_2\frac{X}{Y})^{l+1}\}, \\
J_1^{(l)} &= \{0 \leq t \leq \frac{X}{Y} : \\
&\quad (L_1\frac{X}{Y})^{1/2}(L_2\frac{X}{Y})^l \leq |\zeta(1/2+it)| \leq (L_1\frac{X}{Y})^{1/2}(L_2\frac{X}{Y})^{l+1}\}, \\
J_2^{(l)} &= \{\frac{X}{Y} \leq t \leq T_0 : \\
&\quad (L_1\frac{X}{Y})^{1/2}(L_2\frac{X}{Y})^l \leq |\zeta(1/2+it)| \leq (L_1\frac{X}{Y})^{1/2}(L_2\frac{X}{Y})^{l+1}\}.
\end{aligned}$$

Let

$$\begin{aligned}
J^{(1/2)} &= \{0 \leq t \leq T_0 : 0 \leq |\zeta(1/2+it)| \leq (\log\frac{X}{Y})^{1/2}\}, \\
J_1^{(1/2)} &= \{0 \leq t \leq \frac{X}{Y} : 0 \leq |\zeta(1/2+it)| \leq (\log\frac{X}{Y})^{1/2}\}, \\
J_2^{(1/2)} &= \{\frac{X}{Y} \leq t \leq T_0 : 0 \leq |\zeta(1/2+it)| \leq (\log\frac{X}{Y})^{1/2}\}.
\end{aligned}$$

Now,

$$\begin{aligned}
I_1 &= \int_0^{X/Y} \zeta(1/2+it)M^2(1/2+it)A(1/2+it)dt \\
&\ll Y^2X^{-\frac{1}{2}}\sum_{k=2}^{R_I}\int_{I_1^{(k)}} \zeta(1/2+it)M^2(1/2+it)dt \\
&+ Y^2X^{-\frac{1}{2}}\sum_{l=0}^{R_J}\int_{J_1^{(l)}} \zeta(1/2+it)M^2(1/2+it)dt \\
&+ Y^2X^{-\frac{1}{2}}\int_{J_1^{(1/2)}} \zeta(1/2+it)M^2(1/2+it)dt \\
&\ll Y^2X^{-\frac{1}{2}}\sum_{k=2}^{R_I}(\log\frac{X}{Y})^{k+1}\int_{I_1^{(k)}} |M(1/2+it)|^2dt \\
&+ Y^2X^{-\frac{1}{2}}\sum_{l=0}^{R_J}(\log\frac{X}{Y})^{1/2}(\log\log\frac{X}{Y})^{l+1}\int_{J_1^{(l)}} |M(1/2+it)|^2dt \\
&+ Y^2X^{-\frac{1}{2}}(\log\frac{X}{Y})^{1/2}\int_{J_1^{(1/2)}} |M(1/2+it)|^2dt \\
&\ll Y^2X^{-\frac{1}{2}}\sum_{k=2}^{R_I}(\log\frac{X}{Y})^{k+1}\{\mu(I_1^{(k)})\log X + X^{1/2-\alpha/4}\} \\
&+ Y^2X^{-\frac{1}{2}}\sum_{l=0}^{R_J}(\log\frac{X}{Y})^{1/2}(\log\log\frac{X}{Y})^{l+1}\{\mu(J_1^{(l)})\log X + X^{1/2-\alpha/4}\} \\
&+ Y^2X^{-\frac{1}{2}}(\log\frac{X}{Y})^{1/2}\{\mu(J_1^{(1/2)})\log X + X^{1/2-\alpha/4}\}.
\end{aligned}$$

In the third step above we have assumed that the bound

$$\int_U \left|\sum_{n\le N} b_n n^{it}\right|^2 dt \ll \sum_{n\le N}|b_n|^2\{T+O(n)\} \tag{5.4.12}$$

holds for $U = I_1^{(k)}, J_1^{(l)}, J_1^{(\frac{1}{2})}$ with the special sequence $b_n = a_n$.

Therefore,

$$\begin{aligned}
I_1 &\ll \left\{ Y^2X^{-\frac{1}{2}}\log X\sum_{k=2}^{R_I}\frac{X}{Y}\frac{(\log\frac{X}{Y})^{k+1}}{(\log\frac{X}{Y})^{2k-1}} + Y^2X^{-\frac{\alpha}{4}}\sum_{k=2}^{R_I}(\log\frac{X}{Y})^{k+1}\right\}\\
&+ Y^2X^{-\frac{1}{2}}(\log\frac{X}{Y})^{1/2}\sum_{l=0}^{R_J}\frac{X}{Y}\frac{(\log\log\frac{X}{Y})^{l+1}}{(\log\log\frac{X}{Y})^{2l}}\log X\\
&\quad +Y^2X^{-\frac{1}{2}}(\log\frac{X}{Y})^{1/2}\sum_{l=0}^{R_J}(\log\log\frac{X}{Y})^{l+1}X^{1/2-\alpha/4}\\
&+ \left\{Y^2X^{-\frac{1}{2}}(\log\frac{X}{Y})^{1/2}(\log X)\frac{X}{Y} + Y^2X^{-\alpha/4}(\log\frac{X}{Y})^{1/2}\right\}\\
&\ll YX^{\frac{1}{2}}\log X\frac{1}{1-\frac{1}{\log\frac{X}{Y}}} + YX^{1/2}(\log\frac{X}{Y})^{1/2}\log X\frac{\log\log\frac{X}{Y}}{1-\frac{1}{\log\log\frac{X}{Y}}}\\
&+ YX^{\frac{1}{2}}(\log\frac{X}{Y})^{1/2}\log X + Y^2X^{-\alpha/4}(\log X)^2(\frac{X}{Y})^{\beta}\\
&\ll YX^{1/2}(\log X)^{3/2}\log\log\frac{X}{Y} + Y^2X^{-\alpha/4}(\log X)^2(\frac{X}{Y})^{\beta}.
\end{aligned}$$

Also,

$$\begin{aligned}
I_2 &= \int_{\frac{X}{Y}}^{T_0}\zeta(1/2+it)M^2(1/2+it)A(1/2+it)dt\\
&\ll X^{3/2}\sum_{k=1}^{R_I}(\log\frac{X}{Y})^{k+1}\int_{I_2^{(k)}}\frac{|M(1/2+it)|^2}{t^2}dt\\
&+ X^{3/2}\sum_{k=0}^{R_J}(\log\frac{X}{Y})^{1/2}(\log\log\frac{X}{Y})^{k+1}\int_{J_2^{(k)}}\frac{|M(1/2+it)|^2}{t^2}dt\\
&+ X^{3/2}(\log\frac{X}{Y})^{1/2}\int_{J_2^{(1/2)}}|M(1/2+it)|^2dt
\end{aligned}$$

Now,

$$\begin{aligned}
&\int_{X/Y}^{T_0}\frac{|M(1/2+it)|^2}{t^2}dt\\
&= \left[\frac{\int_0^u|M(1/2+it)|^2dt}{u^2}\right]_{u=X/Y}^{T_0} + \int_{X/Y}^{T_0}\frac{\int_0^u|M(1/2+it)|^2dt}{u^3}du\\
&\ll \frac{1}{T_0^2}\int_0^{T_0}|M(1/2+it)|^2dt - \frac{Y^2}{X^2}\int_0^{X/Y}|M(1/2+it)|^2dt\\
&\ll \frac{Y^2}{X^2}\int_0^{X/Y}|M(1/2+it)|^2dt.
\end{aligned}$$

Therefore, denoting the characteristic function of the set $I^{(k)}$ by $\chi_k(t)$, we have,

$$\begin{aligned}\int_{I_2^{(k)}} \frac{|M(1/2+it)|^2}{t^2}dt &= \int_{X/Y}^{T_0} \frac{\chi_k(t)|M(1/2+it)|^2}{t^2}dt \\ &\ll \frac{1}{T_0^2}\int_0^{T_0} |M(1/2+it)|^2\chi_k(t)dt - \frac{Y^2}{X^2}\int_0^{X/Y} |M(1/2+it)|^2\chi_k(t)dt \\ &\ll \frac{Y^2}{X^2}\int_0^{X/Y} |M(1/2+it)|^2\chi_k(t)dt = \frac{Y^2}{X^2}\int_{I_1^{(k)}} |M(1/2+it)|^2dt,\end{aligned}$$

and similarly for the integrals over $J_2^{(k)}$s and $J_2^{(1/2)}$.

Hence,

$$\begin{aligned}I_2 &\ll Y^2X^{-\frac{1}{2}}\sum_{k=2}^{R_I}(\log\frac{X}{Y})^{k+1}\int_{I_1^{(k)}} |M(1/2+it)|^2dt \\ &+ Y^2X^{-\frac{1}{2}}\sum_{k=0}^{R_J}(\log\frac{X}{Y})^{1/2}(\log\log\frac{X}{Y})^{k+1}\int_{J_1^{(k)}} |M(1/2+it)|^2dt \\ &+ Y^2X^{-\frac{1}{2}}(\log\frac{X}{Y})^{1/2}\int_{J_1^{(1/2)}} |M(1/2+it)|^2dt \\ &\ll YX^{1/2}(\log X)^{3/2}\log\log\frac{X}{Y} + Y^2X^{-\alpha/4}(\log X)^2(\frac{X}{Y})^{\beta}\end{aligned}$$

by the estimate for I_1

So, the integral

$$\begin{aligned}\frac{1}{2\pi i}\int_{\frac{1}{2}-iT_0}^{\frac{1}{2}+iT_0} \zeta(s)M^2(s)A(s)ds &= I_1 \quad + \quad I_2 \\ &\ll YX^{1/2}(\log X)^{3/2}\log\log\frac{X}{Y} + Y^2X^{-\alpha/4}(\log X)^2(\frac{X}{Y})^{\beta}.\end{aligned}$$

Choosing $\beta = \alpha/2 - o(1)$ and $Y \geq X^{\frac{1}{2}}(\log X)^{-\frac{1}{2}+o(1)}$, we see that the above integral is only $o(Y^2(\log X)^2)$.

Remark

As before, we actually can get that the number of X^{α}-smooth numbers in the interval $(X, X + (\log X)^{-\frac{1}{2}+o(1)}\sqrt{X}] \gg X^{1/2-o(1)}$.

Bibliography

[All82b] K. Alladi, *The Turán-Kubilius inequality for integers without large prime factors*, J. Reine Angew. Math. 335, (1982), pp. 180-196.

[Bac14] R. J. Backlund, *Sur les zéros de la fonction $\zeta(s)$ de Riemann*, C. R. 158, (1914), pp. 1979-81.

[Bac18] R. J. Backlund, *Über die Nullstellen der Riemannschen Zetafunktion*, A. M. 41, (1918), pp. 345-75.

[Balo87] A. Balog, *On the distribution of integers having no large prime factors*, Astérisque 147-148, (1987), pp. 27-31.

[Beh38] F. A. Behrend, *On sequences of integers containing no arithmetic progression*, Cas. Mat. Fys. Praha, 67 (1938), pp. 235-239.

[Beh46] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci., 23 (1946), pp. 331-332.

[Ber68] E. R. Berlekamp, *A construction for partitions which avoid long arithmetic progressions*, Canad. Math. Bull. 11 (1968), pp. 409-415.

[BP92] A. Balog, C. Pomerance; *The distribution of smooth numbers in arithmetic progressions*, Proc. Amer. Math. Soc. 115, (1992), pp. 33-43.

[Bru51a] N. G. de Bruijn, *The asymptotic behaviour of a function occurring in the theory of primes*, J. Indian Math. Soc. (N.S.) 15, (1951), pp. 25-32.

[Bru51b] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A 54, (1951), pp. 50-60.

[Bru66] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, II, Nederl. Akad. Wetensch. Proc. Ser. A 69, (1966), pp. 239-247 = Indag. Math. 28, pp. 239-247.

[Buc49] A. A. Buchstab, *On those numbers in an arithmetic progression all prime factors of which are small in magnitude* (Russian), Dokl. Akad. Nauk SSSR 67, (1949), pp. 5-8.

[Can82] E. R. Canfield, *On asymptotic behaviour of the Dickman-de Bruijn function*, Congr. Numer. 38, (1982), pp. 139-148.

[CEP83] E. R. Canfield, P. Edrös and C. Pomerance, *On a problem of Oppenheim concerning "Factorisatio Numerorum"*, J. Number Theory 17, (1983), pp. 1-28.

[Dav00] H. Davenport, *Multiplicative number theory*, Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, (2000).

[Dic30] K. Dickman, *On frequency of numbers containing prime factors of a certain relative magnitude*, Ark. Mat. Astr. Fys. 22, (1930), pp. 1-14.

[Enn69] V. Ennola, *On numbers with small prime divisor*, Ann. Acad. Sci. Fenn. Ser. AI 440, (1969), pp. 16.

[ET36] P. Erdös and P. Turán, *On some sequences of integers*, J.London Math. Soc. 11 (1936), pp. 261-264.

[FG93] J. B .Friedlander and A. Granville, *Smoothing of "smooth" numbers*, Philos. Trans. Roy. Soc. London Ser. A345, (1993), pp. 339-347.

[FL87] J. B. Friedlander and J. C. Lagarias, *On the distribution in short intervals of integers having no large prime factot*, J. Number Theory, (1987), pp. 249-273.

[Fri84b] J. B. Friedlander, *Integers without large prime factors. III*, Arch. Math. 43, (1984), pp. 32-36.

[Ger77] Joseph L. Gerver; *The sum of the reciprocals of a set of integers with no arithmetic progression of k terms*, Proc. Amer. Math. Soc., Vol. 62, No. 2, Feb. 1977, pp. 211-214 .

[Gou08] G. Pal; *Sequences of positive integers containing no p terms in arithmetic progression*, Journal of the Ramanujan Mathematical Society, Vol. 23, No. 2., (June, 2008), pp. 970-1249 .

[Gow98] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progression of length four*, GAFA 8 (1998), pp. 529-551.

[Gow01] W. T. Gowers, *A new proof of Szemerédi's theorem*, GAFA 11 (2001), pp. 465-551.

[GR74] R. L. Graham and B.L. Rothschild, *A short proof of van der Waerden's theorem on arithmetic progressions*, Proc. Amer. Math. Soc. (1974)

[GR79] Joseph L. Gerver; L. Thomas Ramsey, *Sets of Integers With No Long Arithmetic Progression Generated by the Greedy Algorithm*, Mathematics of Computation, Vol. 33, No. 148. (Oct., 1979.), pp. 1353-1359.

[Gra04] R. L. Graham, *Euclidean Ramsey theory*, Handbook of Discrete and Computational Geometry, 2nd Ed., J.E. Goodman and J.O' Rourke, eds., CRC Press, Boca Raton, NY, 2004, pp. 239-254.

[Gra93a] A. Granville, *Integers, without large prime factors, in arithmetic progressions. I*, Acta Math. 170, (1993), pp. 255-273.

[Gra93b] A. Granville, *Integers, without large prime factors, in arithmetic progressions. II*, Philso. Trans. Roy. London Ser. A 345, (1993), pp. 349-362.

[Gra00] A. Granville, *Smooth Numbers: Computational Number Theory and Beyond*, Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Berkeley, (2000), J. Buhler and P. Stevenhagen, eds., Cambridge University Press, pp. 1-56.

[GT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2), 167 (2008), no. 2, pp. 481-547.

[Haf93] J. L . Hafner, *On smooth numbers in short intervals under the Riemann Hypothesis*, preprint.

[Har91] G. Harman, *Short intervals containing numbers without large prime factors*, Math. Proc. Cambridge Philos. Soc. 109, (1991), pp. 1-5.

[Har99] G. Harman, *Integers without large prime factors in short intervals and arithmetic progressions*, Acta Arith. 91, (1999), pp. 279-289.

[Hil84] A. Hildebrand, *Integers free of large prime factors and the Riemann Hypothesis*, Mathematika 31, (1984), pp. 258-271.

[Hil85] A. Hildebrand, *Integers free of large prime factors in short intervals*, Quart. J. Math. (Oxford) (2), 36, (1985), pp. 57-69.

[Hil86a] A. Hildebrand, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, J. Number Theory 22, (1986), pp. 289-307.

[Hil86b] A. Hildebrand, *On the local behavior of $\Psi(x, y)$*, Trans. Amer. Math. Soc. 297, (1986), pp.729-751.

[HT86] A. Hildebrand and G. Tenenbaum, *On integers free of large prime factors*, Trans. Amer. Math. Soc. 296, (1986), pp. 265-290.

[HT93] A. Hildebrand and G. Tenenbaum, *Integers with out large prime factors*, Journal de Théorie des Nombers de Bordeaux, tome 5, n^o, (1993), pp. 411-484.

[IK04] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, 53, American Mathematical Society, Providence, RI, (2004).

[Len87] H. W. Lenstra, *Factoring integers with elliptic curves*, Ann. Math. 126, (1987), 649-673.

[LF67] B. V. Levin and A. S. Fainleib, *Application of some integral equations to problems in number theory*, Rusian Math. Surveys 22, (1967), pp. 119-204.

[LL41] D. H. Lehmer and E. Lehmer, *On the first case on Farmat's last theorem*, Bull. Amer. Math. Soc. 47, (1941), pp. 139-142.

[LPP93] H. W. Lenstra, Jr., J. Pila and C. Pomerance,*A hyperelliptic smoothness test, I*, Philo. Trans. Roy. Soc. London Ser. A345, (1993), pp. 397-408.

[Mon77] H. L. Montgomery, *Extreme values of the Riemann zeta function*, Comm. Math. Helv. 52(1977), 511-518.

[Mos53] L. Moser, *On non-averaging sets of integers*, Canad. J. Math. 5 (1953), pp. 245-252.

[MV74] H. L. Montgomery and R. C. Vaughan, *Hilbert's inequality*, J. London Math. Soc. (2) 8 (1974), 73–82.

[Nor71] K. K. Norton, *Numbers with small prime factors and the least kth power non residue*, Memoirs of the Amer. Math. Soc. 106, (1971).

[Odl87] A. M. Odlyzko, *On the distribution of spacings between zeros of the zeta function*, Mathematics of Computation, Vol. 48, No. 177. (1987), pp. 273-308.

[Pom87] C. Pomerance, *Fast, rigorous factorization and discrete logarithm algorithms*, Discrete Algorithms and Complexity (Kyoto, 1986), Academic Press, Boston.

[Ram51] V. Ramaswami, *Number of positive integers in an assigned arithmetic progression,$\leq$ x and prime to primes greater than x^{ε}*, Proc. Amer. Math. Soc. 2, (1951), pp. 318-319.

[Ran38] R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc.,(1938) 13, pp. 242-247.

[Ran60] R. A. Rankin; *Sets of integers containing not more than a given number of terms in arithmetic progression*, Proc.Roy.Soc.Edinburgh Sect.A 65 (1960/61), pp. 332-344.

[Rot53] K. F. Roth, *On certain sets of integers (I)*, J. Lond. Math. Soc.,28, (1953), pp. 104-109.

[Rot54] K. F. Roth, *On certain sets of integers (II)*, J. Lond. Math. Soc.,29, (1954), pp. 20-26.

[Rot70] K. F. Roth, *Irregularities of sequences relative to arithmetic progressions(III)*, J. Number Theory 2(1970), pp. 125-142.

[Rot72] K. F. Roth, *Irregularities of sequences relative to arithmetic progressions(IV)*, Per. Math. Hungar. 2(1972), pp. 301-326.

[SS42] R. Salem and D. C. Spencer, *On sets of integers which contain no three in arithmetical progression*, Proc. Nat. Acad. Sci., 28 (1942), pp. 561-563.

[ST92] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag New York, Inc., (1992).

[Sze68] E. Szemerédi, *On sets of integers no four elements in arithmetic progression*, Acta Math. Acad. SCi. Hungar. 20 (1968),pp. 89-104.

[Sze75] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. XXVII, 1975, pp. 199-245.

[Ten90] G. Tenenbaum, *Introduction á la théorié analytique et probabiliste des nombers*, Publ. Inst. Elie Cartan, Vol. 13, Uni. Nancy 1., (1990).

[Ten95] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Press Syndicate of the University of Cambridge, First published in English (1995).

[Tit86] E. C. Titchmarsh, *The theory of the Riemann zeta-function*. Second edition. Edited and with a preface by D. R. Heath-Brown. The Clarendon Press, Oxford University Press, New York, (1986).

[UL75] *Unpublished lecture*, Faculte des Sciences, Paris, Dec. 4, (1975).

[Wae28] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw. Arch. Wisk. 15 (1928), pp. 212-216.

[Vau89] R. C. Vaughan, *A new iterative method in Waring's problem*, Acta Math., 162, (1989), pp. 1-71.

[Vin26] I. M. Vinogradov, *On a bound for the least nth power non-residue* (Russian), Izv. Akad. Nauk SSSR 20, (1926), pp. 47-58; English transl: Trans. Amer. Math. Soc. 29, (1927), pp. 218-226.

[Wol71] D. Wolke, *Polynomial values with small prime divisors*, Acta Arith. 19, (1971), pp. 327-333.

[Woo92] T. Wooley, *Large improvements in Waring's problem*, Annals Math.(2) 135, no 1, (1992), 135-164.

[Xuan93] T. Z. Xuan, *On asymptotic behavior of the Dickman-de Bruijn function*, Math. Ann. 297, (1993), pp. 519-533.

[Xuan99] T. Z. Xuan, *On smooth integers in short intervals under the Riemann Hypothesis*, Acta Arith. 88, (1999), pp. 327-332.