POINTS ON ELLIPTIC CURVE OVER FINITE FIELDS

By

Sumit Giri

MATH10201004003

The Institute of Mathematical Sciences, Chennai

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

For the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

April, 2015

Homi Bhabha National Institute

Recommendations of the Viva Voce Board

As members of the Viva Voce Board, we certify that we have read the dissertation prepared by Sumit Giri entitled "Points on elliptic curve over finite fields"and recommend that it may be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

____ Date:

Guide/Convener - R. Balasubramaniam

____ Date:

Member 1 - D. S. Nagaraj

____ Date:

Member 2 - A. Mukhopadhyay

____ Date:

Member 3 - Sanoli Gun

____ Date:

External Examiner - C. S. Rajan

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to HBNI.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it may be accepted as fulfilling the dissertation requirement.

Date:

Place: Guide

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under the rules of the HBNI.

Brief quotations from this dissertation are allowed without special permission, provided that accurate acknowledgement of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Sumit Giri

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part of a degree / diploma at this or any other Institution / University.

Sumit Giri

ACKNOWLEDGEMENTS

First and foremost, I would sincerely like to thank my supervisor Prof. R. Balasubramaniam for all his help to teach me analytic number theory and his patience and guidance in helping me write this thesis. He was always ready to help with his vast experience and command over the field of number theory and allowed me to have complete freedom in choosing my area of doctoral studies. I always had the luxury of landing in his office to ask silly questions and he, rather than getting offended, showed great enthusiasm in solving the problems instantly.

I would like to thank Dr. Anirban Mukhopadhyay for the fruitful discussions and his insightful comments related to my works and for taking the trouble of doing a proof reading of this thesis and other papers. I am thankful to Prof. Srinivas Kotyada for his comments related to relevant literatures. His course on Number theory and Cryptography was one of the first course in number theory for me and it motivated me to pursue this field of research. I would also like to thank Prof. Ram Murty and Dr. Sanoli Gun for their useful advices.

It will be a mistake if I dont mention Dr. Francesco Pappalardi, since his advice during a couple of discussions encouraged me to explore these specific types of questions related to elliptic curves. I would also like to thank Prof. Chantal David and Dr. Dimitris Koukoulopoulos for their patience in listening to my questions and suggesting accordingly.

The journey here would have never been so pleasant and memorable without the company of my friends at IMSc. My batchmates Chandan, Sandipan, Kamalakshya were closely associated and were fundamental to the dinner parties every now and then. I would also like to thank Priyamvad, Prasanna as well. Krishnan Rajkumar requires a special mention for many mathematical as well as non mathematical advices during tough times. Last, but not the least, I would like to thank Vidhyalakshmi, who made my life easier around the directors office, which ironically used to be my supervisors office as well.

Abstract

We divide our study into two parts. In the first part we study the main topic of our interest, that is same as the title of this thesis. While in the second part we study a problem related to additive representation function related to sum-set.

For an elliptic curve E over the rationals and a prime p, $E_p(\mathbb{F}_p)$ be the reduced curve modulo p. For a fixed positive integer N, $M_E(N)$ counts the number of primes p such that $|E_p(\mathbb{F}_p)| = N$. Under a well known conjecture regarding primes in short intervals, the average of $M_E(N)$ over an appropriate large class $\mathcal{C}$ of curves E is asymptotic to $\frac{K^*(N)}{\log N}$ for a constant $K^*(N)$ close to 1. In this thesis, we compute the average of $K^*(N)$ over $N \leq x$. This asymptotic result improves an earlier result significantly and checks the consistency of the conditional result with other unconditional ones. Further, we also investigate the distribution of $M_E(N)$, that is the probability of the event $\{M_E(N) = \ell\}$ for a fixed integer ℓ and N. For that purpose, we again take an average of the indicator function of the event $\{M_E(N) = \ell\}$ over a class $\mathcal{C}$ of curves and prove that $M_E(N)$ follows a Poisson distribution on average with a mean equals to the average of $M_E(N)$ over the same class $\mathcal{C}$.

In the second part of the thesis, we discuss a problem in additive number theory. Let $\mathcal{A} = \{a_1 < a_2 < a_3 \cdots < a_n < \cdots\}$ be an infinite sequence of non-negative integers and let $R_2(n) = |\{(i,j) : \quad a_i + a_j = n; \quad a_i, a_j \in \mathcal{A}; \quad i \leq j\}|$. We define $S_k = \displaystyle\sum_{l=1}^{k}(R_2(2l) - R_2(2l+1))$. We prove that if the L^∞ norm of $S_k^+ (= \max\{S_k, 0\})$ is small, then the L^1 norm of $\frac{S_k^+}{k}$ is large.

Contents

List of Publications

- (with R. Balasubramanian) On Additive Representation Functions. International Journal of Number Theory. Vol. 11, No. **4** (2015) 1165-1176.

- (with R. Balasubramanian) Mean-value of product of shifted multiplicative functions and average number of points on elliptic curves. J. Number Theory 157 (2015), 37-53.

- (with R. Balasubramanian) Poisson Distribution of a Prime Counting Function Corresponding to Elliptic Curves. Submitted. arXiv:1503.01018 [math.NT].

Chapter 1

Introduction

In this chapter we shall discuss the background of the problems that we are interested in and state the results. In the later chapters, we shall have more elaborate discussions on those results.

1.1 Reduction modulo prime

Consider an elliptic curve

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{1.1.1}$$

where $a, b \in \mathbb{Q}$ and discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. Under a suitable change of variable of the type $X \mapsto X/c^2$ and $Y \mapsto Y/c^3$, without loss of generality, one can assume that a and b are integers. Also, if c is chosen in such a way that $|\Delta|$ is minimal, then the equation is said to be minimal Weierstrass equation. For a curve E, a prime $p \neq 2$ is called prime of good reduction if $p \nmid \Delta$, where Δ is the discriminant of the minimal Weierstrass equation for E.

So, if we assume that (1.1.1) is minimal form, then the reduction of E modulo p is given by

$$E_p : Y^2Z = X^3 + a_pXZ^2 + b_pZ^3, \tag{1.1.2}$$

where a_p and b_p are the images of a and b in $\mathbb{F}_p$.

Here we also recall that the points on elliptic curve over a field k gives rise to an abelian group under addition of points over curves. So, $E/\mathbb{Q}$ is an abelian group and $E_p/\mathbb{F}_p$, where p is a prime of good reduction for E, is an abelian group.

With these notations, we proceed to define the following prime counting function.

1.2 The prime counting function $M_E(N)$

Let E be an elliptic curve defined over the field of rationals $\mathbb{Q}$. For a prime p where E has good reduction, we denote by E_p the reduction of E modulo p. Let $\mathbb{F}_p$ be the finite field with p elements and $E_p(\mathbb{F}_p)$ is the group of $\mathbb{F}_p$ points of E_p.

It is well known that $E_p(\mathbb{F}_p)$ admits the structure of an abelian group of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, where m divides $(p-1)$. We denote such groups by $G_{m,k}$. The question related to density of elliptic curve groups among all groups of the form $G_{m,k}$ has been addressed in [BPS12].

We know $|E_p(\mathbb{F}_p)| = p+1-a_p(E)$ where $a_p(E)$ is the trace of the Frobenius morphism at p. By Hasse's theorem we know that $|a_p(E)| < 2\sqrt{p}$. The question related to the primality of $E_p(\mathbb{F}_p)$ has been discussed in [BCD11]. Now, for a fixed positive integer N, we define the following prime counting function

$$M_E(N) := \#\{p \text{ prime} : \ E \text{ has good reduction over } p \text{ and } |E_p(\mathbb{F}_p)| = N\}. \tag{1.2.1}$$

Here we note that the Hasse's theorem implies

$$(\sqrt{p}-1)^2 < N < (\sqrt{p}+1)^2$$

or equivalently,

$$N^- := (\sqrt{N}-1)^2 < p < (\sqrt{N}+1)^2 := N^+. \tag{1.2.2}$$

This in turn implies that

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}. \tag{1.2.3}$$

Using Chinese Reminder theorem, it is not difficult to construct a curve E such that the upper bound in (1.2.3) is attained.

Also, it is not difficult to prove that

$$\sum_{N \leq x} M_E(N) = \pi(x) + O(\sqrt{x}). \tag{1.2.4}$$

To see this, note that when N varies over the range $[1, x]$, $M_E(N)$'s corresponds to mutually exclusive sets of primes. But, by Hasse's theorem the primes are in the range $[N^-, N^+]$ and hence in the range $[x^-, x^+]$. By the same arguments, all the primes except $O(\sqrt{x})$ many in the range $[x^-, x^+]$ appear at least once. Hence each prime occurs exactly once. Since $\pi(x) = \pi(x^+) + O(\sqrt{x})$, the above equality holds.

Consequently, $M_E(N)$ is zero for most of the N's. Under the assumption that $E_p(\mathbb{F}_p)$ is uniformly distributed over the range $[p^-, p^+]$ when E varies, heuristically, the average order of $M_E(N)$ is expected to be $\sim \frac{c}{\log N}$; See equation (4) in [DS13] for more details.

Now, we are interested in the behavior of $M_E(N)$ for a fixed N. For a single E,

$M_E(N)$ can range from 0 to $\frac{\sqrt{N}}{\log N}$ as discussed above. So a sensible way to approach the problem is to take an average of $M_E(N)$ over a reasonably large class of curves E.

For a pair of integers (a, b), let $E_{a,b}$ be the elliptic curve defined by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b.$$

Also for $A, B > 0$, we define the class of curves $\mathcal{C}(A, B)$ by

$$\mathcal{C}(A, B) := \{E_{a,b} : \ |a| \leq A, |b| \leq B, \Delta(E_{a,b}) \neq 0\}. \tag{1.2.5}$$

Before we present the relevant results, we need to state the following well known conjecture related to short interval distribution of primes in arithmetic progression.

Conjecture 1 (*Barban-Davenport-Halberstam*)**.** *Let* $\theta(x; q, a) = \sum_{p \leq x, p \equiv a (mod\ q)} \log p$. *Let* $0 < \eta \leq 1$ *and* $\beta > 0$ *be real numbers. Suppose that* X, Y, *and* Q *are positive real numbers satisfying* $X^\eta \leq Y \leq X$ *and* $Y/(\log X)^\beta \leq Q \leq Y$. *Then*

$$\sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} |\theta(X + Y; q, a) - \theta(X; q, a) - \frac{Y}{\phi(q)}|^2 \ll_{\eta,\beta} YQ \log X.$$

For $\eta = 1$, this is the classical Barban-Davenport-Halberstam theorem. Languasco, Perelli, and Zaccagnini [LPZ10] have proved the Conjecture for $\eta = \frac{7}{12} + \epsilon$, which is the best known result. Also, in the same paper [LPZ10], they have proved the conjecture for $\eta = \frac{1}{2} + \epsilon$ under the generalized Riemann hypothesis.

Now, under the above hypothesis, David and Smith [DS13],[DS14] proved that

Theorem A. *Let Conjecture 1 be true for some* $0 < \eta < \frac{1}{2}$. *Let* γ *be a positive constant. Choose* A, B *such that* $A, B \geq \sqrt{N}(\log N)^{1+\gamma} \log\log N$ *and* $AB \geq$

$N^{\frac{3}{2}}(\log N)^{2+\gamma}\log\log N$, *then for any odd integer* N, *we have*

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{E\in\mathcal{C}(A,B)} M_E(N) = K(N)\frac{N}{\phi(N)\log N} + O(\frac{1}{(\log N)^{1+\gamma}}), \tag{1.2.6}$$

with

$$K(N) := \prod_{p\nmid N}\left(1-\frac{(\frac{N-1}{p})^2p+1}{(p-1)^2(p+1)}\right)\prod_{p\mid N}\left(1-\frac{1}{p^{\nu_p(N)}(p-1)}\right), \tag{1.2.7}$$

where ν_p *denotes the usual* p*-adic valuation.*

Heuristically one would expect this result where the function $\frac{NK(N)}{\phi(N)}$ can be considered to be a constant close to 1 for most of N's.

In [CDKS14], Chandee, David, Koukoulopoulos and Smith extended this result over all N.

Note that the above theorem is based on the assumption of Barban-Davenport-Halberstam conjecture for a particular range. In order to verify the consistency of *Theorem A* with unconditional results such as (1.2.4), one needs to compute the mean value of $\frac{NK(N)}{\phi(N)}$, which is the main topic to be discussed in the next chapter.

1.3 Average of $K^*(N)$

If we denote $\frac{NK(N)}{\phi(N)}$ by $K^*(N)$, then in [MPS14], Smith, Martin and Pollack proved

Theorem B. *For* $x \geq 2$,

$$\sum_{N\leq x} K^*(N) = x + O\left(\frac{x}{\log x}\right) \quad \textit{and} \quad \sum_{\substack{N\leq x\\ N\ odd}} K^*(N) = \frac{x}{3} + O\left(\frac{x}{\log x}\right).$$

Using the first part of *Theorem B* and Abel's partial summation one can verify that

$$\sum_{N\le x}\frac{K^*(N)}{\log N}=\frac{x}{\log x}+O(\frac{x}{(\log x)^2}). \tag{1.3.1}$$

Then (1.2.6) together with 1.3.1 gives

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{E\in\mathcal{C}(A,B)}\sum_{N\le x}M_E(N)=\frac{x}{\log x}+O\left(\frac{x}{(\log x)^2}\right). \tag{1.3.2}$$

So *Theorem A* is consistent with (1.2.4) as $\pi(x)=\frac{x}{\log x}+O\left(\frac{x}{(\log x)^2}\right)$. Hence an average over E in the equation (1.2.4) also gives the above equality. Similarly, using the second part of *Theorem B*, we also get

$$\sum_{\substack{N\le x\\ N\text{ odd}}}\frac{K^*(N)}{\log N}=\frac{1}{3}\pi(x)+O\left(\frac{x}{(\log x)^2}\right)$$

Here, we note that, a special case of an unconditional result (Theorem 19, [BS09]) by Banks and Shparlinski gives

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{E\in\mathcal{C}(A,B)}\sum_{\substack{N\le x\\ N\text{ odd}}}M_E(N)=\frac{1}{3}\pi(x)+O_R\left(\frac{x}{(\log x)^R}\right), \tag{1.3.3}$$

where R is a fixed positive real number. See equation (9) in [MPS14] for more details.

We observe that appropriate improvements in the asymptotic results in *Theorem B* would give

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{E\in\mathcal{C}(A,B)}\sum_{N\le x}M_E(N)=\pi(x)+O\left(\frac{x}{(\log x)^R}\right), \tag{1.3.4}$$

as well as (1.3.3).

These improvements are contained in *Theorem 1.3.1* below. This provides further support to the Barban-Davenport-Halberstam conjecture. We prove

Theorem 1.3.1. *If $x \geq 2$, then*

$$\sum_{N \leq x} K^*(N) = x + O(\log x) \quad \textit{and} \quad \sum_{\substack{N \leq x \\ N \ odd}} K^*(N) = \frac{x}{3} + O(\log x).$$

To get (1.3.3) and (1.3.4), one can combine Theorem A and Theorem 1.3.1 by using partial summation formula. Note the improvements in the error term in (1.3.4) compared to the error term in (1.3.2).

Before going to the next section, we shall see what special structure the function $K^*(N)$ posses. An arithmetic function $F : \mathbb{N} \to \mathbb{C}$ is called multiplicative if

$$F(mn) = F(m)F(n) \quad \text{for } (m, n) = 1.$$

Although the function $K^*(N)$ looks far from being multiplicative, it can be written as a product of two shifted multiplicative functions, i.e.

$$K^*(N) = C_2^* F^*(N-1) G^*(N) \tag{1.3.5}$$

where

$$C_2^* = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \tag{1.3.6}$$

$$F^*(N) = \prod_{\substack{p|N \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p|N} \left(1 - \frac{1}{(p-1)^2(p+1)}\right) \tag{1.3.7}$$

$$G^*(N) = \frac{N}{\varphi(N)} \prod_{\substack{p|N \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p|N} \left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right). \tag{1.3.8}$$

Note that, both F^* and G^* are multiplicative functions. So the problem reduces to computing the average of the product of two shifted multiplicative functions. In order to prove the above theorem, we use a new technique to compute the mean value of fairly general shifted multiplicative functions.

1.4 Shifted multiplicative functions

Let F and $G : \mathbb{N} \to \mathbb{C}$ be non zero multiplicative functions . Here we are interested in finding the mean value of $F(n-h)G(n)$ for a fixed integer h. More precisely, we consider

$$M_{x,h}(F,G) = \frac{1}{x}\sum_{n\leq x} F(n-h)G(n). \tag{1.4.1}$$

A lot of work has been done to find the asymptotic behavior of $M_{x,h}(F,G)$ under various conditions, (see for example [CS01], [Kat69], [SS07], [Ste97a], [Ste97b], [Ste01]). In many of those cases, the functions are required to be close to 1 on the set of primes. In some cases (for example [Kat69]) convergence of suitable series involving F and G has been assumed.

When the functions grow fast, then the problem becomes more difficult. In [EI90], divisor function and other fast-growing functions are discussed. $M_x(\phi,\phi)$, corresponding to the Euler totient function $\phi(n)$, has been studied in [Ing27] and [Mir49].

Here we consider this problem for a wide class of functions with generalized growth conditions. The types of functions that we consider in *Theorem 1.4.1* need not be multiplicative. But they can be written as

$$F(n) = A(n)\sum_{d|n} f(d) \quad \text{and} \quad G(n) = B(n)\sum_{d|n} g(d), \tag{1.4.2}$$

where

$$\sum_{d=1}^{\infty} \frac{|f(d)|}{d} < +\infty, \quad \sum_{d=1}^{\infty} \frac{|g(d)|}{d} < +\infty. \tag{1.4.3}$$

Further, we assume the existence of two function $M(x)$ and $E_1(x)$, such that for any positive integers a and m,

$$\sum_{\substack{n \leq x \\ n \equiv a (\text{mod } m)}} A(n-h)B(n) = \frac{1}{m} M(x) + O_h(E_1(x)), \tag{1.4.4}$$

where the main term $M(x)$ depends only on x; and not on a and m; Also the implied constant in the error term depends on h only.

We show that, under the above conditions, one can prove an asymptotic estimate of $M_{x,h}(F,G)$. Further, in order to write the error term explicitly, we introduce two suitable monotonic functions $E_1(x)$ and $E_2(x)$ such that

$$\sum_{d \leq x} |f(d)| = O(E_2(x)), \quad \sum_{d \leq x} |g(d)| = O(E_3(x)). \tag{1.4.5}$$

With these notations, we state the following theorem.

Theorem 1.4.1. *Let F and G be two arithmetic functions, satisfying (1.4.2), (1.4.3), (1.4.4) and (1.4.5), where f and g are multiplicative. Suppose there is a $0 < c < 2$ such that for any large positive real number y, $E_i(2y) \leq cE_i(y)$ for $i = 2, 3$. Then for any fixed positive integer h,*

$$\sum_{n \leq x} F(n-h)G(n) = C_h M(x) + O_h\left(E_1(x)E_2(x)E_3(x)\right) + O_h\left(\frac{c}{2-c}\frac{|M(x)|}{x}(|E_2(x)| + |E_3(x)|)\right), \tag{1.4.6}$$

with

$$C_h = \prod_p \left(1 + \sum_{j\geq 1} \frac{f(p^j)+g(p^j)}{p^j}\right) \prod_{p|h} \left(1 + \frac{\sum\limits_{i=1}^{\nu_p(h)} p^i S_p(p^i)}{S_p(1)}\right)$$

where $S_p(p^i) := \sum\limits_{\min\{e_1,e_2\}=i} \frac{f(p^{e_1})g(p^{e_2})}{p^{e_1+e_2}}$*, for* $i \geq 0$ *and the implied constant in the error term depends only on* h*.*

Before proceeding further, we shall note down some application of the above theorem apart from its application on the function $K^*(N)$ defined above. One can directly apply it on classical Euler's totient function ϕ and Jordan's totient function J_k . See [ES51] and [AS90] for more on the error term related to ϕ and J_k.

Corollary 1.4.1. *(a) If* $\phi(n)$ *is the Euler totient function, i.e.* $\phi(n) = n\prod\limits_{p|n}(1-1/p)$*, then for any positive integer* $h \leq x$*,*

$$\sum_{n\leq x} \phi(n)\phi(n-h) = \frac{1}{3}x^3 \prod_p (1 - \frac{2}{p^2}) \prod_{p|h} (1 + \frac{1}{p(p^2-2)}) + O(hx^2(\log x)^2).$$

(b) If $J_k(n)$ *is the Jordan's totient function, defined as* $J_k(n) = n^k\prod\limits_{p|n}(1-1/p^k)$*, then for* $k \geq 2$ *and a positive integer* $h \leq x$*,*

$$\sum_{n\leq x} J_k(n)J_k(n-h) = \frac{x^{2k+1}}{2k+1} \prod_p (1 - \frac{2}{p^{k+1}}) \prod_{p|h} \left(1 + \frac{1}{p^k(p^{k+1}-2)}\right) + O(hx^{2k}).$$

Part (a) of the previous corollary is as strong as the best known result which was due to L. Mirsky [Mir49]. While the result related to $J_k(n)$ in part (b) appears to be the first of this kind.

Now, we discuss the original expression of $K(N)$ as defined in [Theorem 3 ; [DS13]].

We denote it by $\hat{K}(N)$. It was defined as

$$\hat{K}(N) := \frac{N}{\phi(N)} \prod_{p \nmid N} \left(1 - \frac{(\frac{N-1}{p})^2 p + 1}{(p-1)^2(p+1)}\right) \prod_{\substack{p \mid N \\ 2 \nmid \nu_p(N)}} \left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right) \prod_{\substack{p \mid N \\ 2 \mid \nu_p(N)}} \left(1 - \frac{p - \left(\frac{-N_p}{p}\right)}{p^{\nu_p(N)+1}(p-1)}\right) \tag{1.4.7}$$

where ν_p denotes the usual $p-$adic valuation, $N_p := \frac{N}{p^{\nu_p(N)}}$ denotes the $p-$free part of N and $\left(\frac{a}{p}\right)$ is the quadratic residue symbol for a modulo p.

This function cannot be written as a product of two shifted multiplicative functions. In [MPS14], the mean value of $\hat{K}(N)$ over odd N has been computed. Using a different method, we prove an average of $\hat{K}(N)$ over all N up to x.

Theorem 1.4.2. *For $x \geq 2$,*

$$\sum_{N \leq x} \hat{K}(N) = x + O(\log x).$$

In [MPS14], Smith, Martin and Pollack also computed a similar average of $\hat{K}(N)$ over odd N's with an error term $O\left(\frac{x}{\log x}\right)$. Although the function above in the main theorem does not have any relevance to any any natural question, the main reason to prove this theorem separately, is to show that *Theorem 1.4.1* can be useful, even when one of the shifted functions is not multiplicative.

In *Chapter 2*, we shall continue the discussion on the above mentioned functions such as $K^*(N)$ and $\hat{K}(N)$.

In the last section of this chapter, we come back to the distribution of the function as defined in 1.2.1.

1.5 Distribution of $M_E(N)$

In [Kow06], Kowalski raised a question related to the behavior of sums of the type

$$\sum_{N \le x} M_E(N)^r \quad \text{and} \sum_{\substack{N \le x \\ M_E(N) \ge 2}} M_E(N). \tag{1.5.1}$$

To answer this question, we focus on the distribution of the function $M_E(N)$. In other words, if N is a fixed integer and E be any arbitrary chosen curve from a large class of curves, then what is the probability of the event $\{M_E(N) = \ell\}$, where ℓ is a given positive integer.

Under the assumption that primes are randomly distributed and reduction modulo two different primes are two independent events, from *Theorem 1.3.1*, one would expect the event $\{E \in \mathcal{C} : M_E(N) = \ell\}$ occurs with a probability $\sim \frac{1}{(\log N)^\ell}$. But such a result is possibly going to be dependent on assumption such as the one assumed in *Theorem 1.3.1.* As before, by taking the average over a class , we can get the following unconditional result.

Theorem 1.5.1. *Let $\mathcal{C}(A, B)$ be as defined as in (1.2.5) and N be a positive integer greater than 7. If L be a positive integer and $\gamma > 0$, such that $A, B > N^{L/2}(\log N)^{1+\gamma}$ and $AB > N^{3L/2}(\log N)^{2+\gamma}$ for some $\gamma > 0$, then for $1 \le \ell \le L$*

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{\substack{E \in \mathcal{C}(A,B) \\ M_E(N) = \ell}} 1 = \frac{1}{\ell!} \left(\frac{1}{\#\mathcal{C}(A,B)} \sum_{E \in \mathcal{C}(A,B)} M_E(N) \right)^\ell \left(1 + O\left(\frac{N}{\phi(N) \log N} \right) \right) + O\left(\frac{1}{N^{\frac{L-\ell}{2}} (\log N)^\gamma} \right),$$

where the 'O'constant in the last error term is independent of γ.

From [Theorem 1.7, [CDKS14]] we also have

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{E\in\mathcal{C}(A,B)} M_E(N) \ll \frac{N}{\phi(N)\log N} = O\left(\frac{\log\log N}{\log N}\right), \tag{1.5.2}$$

for large enough A, B.

Now we know that if $X_N \sim \text{Poisson}(\lambda_N)$, for $N = 1, 2, \cdots$, then the probability mass function of X_N is

$$f_{X_N}(\ell) = \frac{(\lambda_N)^\ell e^{-\lambda_N}}{\ell!} \qquad \text{for } \ell = 0, 1, 2, \cdots .$$

If we take $\lambda_N = \frac{1}{\#\mathcal{C}(A,B)} \sum\limits_{E\in\mathcal{C}(A,B)} M_E(N)$, then in view of (1.5.2), one can see that if L is large, then on an average $M_E(N)$ follows a limiting Poisson distribution with mean $\frac{1}{\#\mathcal{C}(A,B)} \sum\limits_{E\in\mathcal{C}(A,B)} M_E(N)$ as $N \to \infty$. The integer L in *Theorem 1.5.1* is introduced to ensure the finiteness of the class $\mathcal{C}(A, B)$.

One can immediately see that if one also assumes *Conjecture 1*, as in *Theorem A*, then the right hand side of *Theorem 1.3.1* is asymptotic to $\frac{1}{\ell!}\left(\frac{NK(N)}{\phi(N)\log N}\right)^\ell$.

Further, one can think of the following generalization of the quantities defined in (1.5.1), namely

$$\frac{1}{\#\mathcal{C}} \sum_{E\in\mathcal{C}} \sum_{\substack{M_E(N)\geq \ell \\ N\leq x}} M_E(N)^r \tag{1.5.3}$$

for two non negative integers r and ℓ.

Proving an asymptotic for (1.5.3) would provide a possible answer for Kowalski's question related to (1.5.1).

Before stating our result related to (1.5.3), we shall introduce a sequence of constants $\{C(m)\}_{m=\ell}^{\infty}$, where $C(m)$ corresponds to the $m-$th moment of the function

$NK(N)/\phi(N)$ where $K(N)$ as defined in (1.2.7). More precisely,

$$C(m) = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)^m \prod_p (1 + f_m(p)),$$

where,

$$\begin{aligned} f_m(2) &= \frac{1}{2}\left(\left(\frac{2}{3}\right)^m - 1\right) + 2^m \sum_{j\geq 2} \frac{1}{2^j}\left(\left(1-\frac{1}{2^j}\right)^m - \left(1 - \frac{1}{2^{j-1}}\right)^m\right), \\ f_m(p) &= \frac{1}{p}\left[\left(1-\frac{1}{(p-1)^2}\right)^{-m}\left(\left(1-\frac{1}{(p-1)^2(p+1)}\right)^m + \left(\frac{p}{p-1}\right)^m\left(1-\frac{1}{p(p-1)}\right)^m\right) - 2\right] \\ &\quad + \left(\frac{p}{p-1}\right)^m\left(1-\frac{1}{(p-1)^2}\right)^m \sum_{j\geq 2}\frac{1}{p^j}\left(\left(1-\frac{1}{p^j(p-1)}\right)^m - \left(1-\frac{1}{p^{j-1}(p-1)}\right)^m\right). \end{aligned} \tag{1.5.4}$$

It is easy to check that $C(1) = 1$. It seems difficult to simplify the expression when $m > 1$.

Also, for two integers $r \leq \ell$, we construct a sequence $\{d_{\ell,r}(m)\}_{m=\ell}^{\infty}$ as follows.

$$d_{\ell,r}(m) = \sum_{k=\ell}^{m} \frac{k^r}{k!}\frac{(-1)^{m-k}}{(m-k)!} \tag{1.5.5}$$

Here we note that $d_{\ell,r}(\ell) = \frac{\ell^r}{\ell!}$; Also $d_{1,1}(1) = 1$ and $d_{1,1}(m) = 0$ for $m \geq 2$.

With these notations, our next theorem is as follows.

Theorem 1.5.2. *Let r and ℓ be two positive integers with $r \leq \ell$. Also suppose γ_1 be nonnegative integer and γ_2 is a positive real number with $1 + \gamma_1 \leq \gamma_2$. Now if $\mathcal{C}(A, B)$ be defined as in (1.2.5) with $A, B > x^{\frac{\ell+\gamma_1}{2}}(\log x)^{1+\ell+\gamma_2}$ and $AB >$*

$x^{\frac{3(\ell+\gamma_1)}{2}}(\log x)^{2+\ell+\gamma_2}$, then for any positive real number x,

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{E\in\mathcal{C}}\sum_{\substack{N\leq x\\ M_E(N)\geq\ell}} M_E(N)^r = \sum_{m=\ell}^{\ell+\gamma_1} C(m)d_{\ell,r}(m)Li_m(x) + O\left(\frac{x}{(\log x)^{1+\ell+\gamma_1}}\right),$$

where $C(m)$ and $d_{\ell,r}(m)$ are defined in (1.5.4) and (1.5.5) respectively and $Li_m(x) = \int_2^x \frac{1}{(\log t)^m}\,dt$.

If we focus on the right hand side in the above theorem, we observe that the highest order term, as a function of x, corresponds to the contribution coming from $\{M_E(N) = \ell\}$. This contributes a factor ℓ^r, along with the $\frac{1}{\ell!}$ as stated in *Theorem 1.5.1.* Also the constant $C(m)$ is the m'th moment of $\frac{NK(N)}{\phi(N)}$, which is defined in *Theorem A.*

Further conditionally as in *Theorem A*, one has

Theorem 1.5.3. *Let* Conjecture 1 *be true for some $\eta < \frac{1}{2}$. Also, let γ_1 be a non negative integer and $\gamma_2 > 0$. Now if $A, B > x^{\frac{\ell+\gamma_1}{2}}(\log x)^{1+\ell+\gamma_2}$ and $AB > x^{\frac{3(\ell+\gamma_1)}{2}}(\log x)^{2+\ell+\gamma_2}$, then for $r \leq \ell$*

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{E\in\mathcal{C}(A,B)}\sum_{M_E(N)\geq\ell} M_E(N)^r = \sum_{m=\ell}^{\ell+\gamma_1} d_{\ell,r}(m)\left(\frac{K(N)N}{\phi(N)\log N}\right)^m + O\left(\frac{N}{\phi(N)\log N}\right)^{1+\ell+\gamma_1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right),$$

where $\mathcal{C}(A,B)$ is as before.

Remark 1. *Let $\mathcal{H}$ denote a ℓ-tuple of distinct integers and $\upsilon_{\mathcal{H}}(p)$ is the number of residue classes modulo p represented by elements of $\mathcal{H}$. Suppose $\upsilon_{\mathcal{H}}(p) < p$ for all prime p. Then the Hardy-Littlewood conjecture states that the number of integers $n \leq x$ such that $n+h$ is prime for each $h \in \mathcal{H}$ is asymptotic to $\mathfrak{S}(\mathcal{H})x\log^{-k}x$ where*

$$\mathfrak{S}(\mathcal{H}) = \prod_p\left(1-\frac{\upsilon_{\mathcal{H}(p)}}{p}\right)\left(1-\frac{1}{p}\right)^{-k}.$$

$\mathfrak{S}(\mathcal{H})$ *is called the 'singular series'. Recalling the fact that* $d_{\ell,r}(\ell) = \frac{\ell r}{\ell!}$*, we note that* Theorem 1.5.2 *is somewhat similar to the prime* $\ell-$*tuple conjecture except for an extra* $\frac{1}{\ell!}$*, which comes from the permutation of a* $\ell-$*tuple.*

In *Theorem 1.5.2* and *Theorem 1.5.3*, the parameter γ_1 is introduced to express the smaller order terms with precise constants. Further, in *Theorem 1.5.3*, the implied constant in the last error term is independent of γ_2.

In *Chapter 2*, we first give a proof of *Theorem 1.3.1* and *Theorem 1.4.1.* We shall see that *Theorem 1.4.1* is a straightforward application of *Theorem 1.3.1.* The proof of *Theorem 1.4.2* is somewhat more technical. We first show that the average $\hat{K}(N)$ equals to an average of a 'nice'function of the type that is defined in *Theorem 1.3.1* and hence just average that 'nice'function using *Theorem 1.3.1.*

While in *Chapter 3*, we produce a brief survey of the machinery that has been used in problems similar to the one discussed in *Section 1.5.* We give a brief sketch of the proof of Theorem A as done in [DS13]. In the last part of that chapter, we shall show how one can modify this method to get *Theorem 1.5.1.* We also complete the proof of *Theorem 1.5.2* and *Theorem 1.5.3* is the same chapter.

Since the final topic of our thesis, which is on the monotonicity of additive representation function, is somewhat different from what has been explained above, we leave the full discussion on that for *Chapter 4.*

Chapter 2

Shifted multiplication functions

One of the classical way of approaching the sums of the type $\sum\limits_{n\le x} f(n)$, where f is an arithmetic function, is to replace $f(n)$ by $\sum\limits_{d|n} g(d)$. In that case the expression becomes

$$\begin{aligned}\sum_{n\le x} f(n) &= \sum_{n\le x}\sum_{d|n} g(d)\\ &= \sum_{d\le x} g(d)\left(\frac{x}{d}+O(1)\right)\\ &= x\sum_{d\le x}\frac{g(d)}{d}+O\left(\sum_{d\le x}|g(d)|\right)\\ &= x\sum_{d=1}^{\infty}\frac{g(d)}{d}+O\left(x\sum_{d>x}\frac{g(d)}{d}\right)+O\left(\sum_{d\le x}|g(d)|\right)\end{aligned}$$

If one can assume that the last two terms are indeed error terms, then it is all about computing $\sum\limits_{d\ge 1}\frac{g(d)}{d}$.

We know by Möbius inversion formula,

$$f(n)=\sum_{d|n} g(d) \Longleftrightarrow g(d)=\sum_{d_1|d}\mu(d_1)f\left(\frac{d}{d_1}\right),$$

where μ is the Möbius function defined by

$$\mu(d) = \begin{cases} (-1)^m, & \text{where } d = p_1 p_2 \cdots p_m,\ p_i\text{'s are distinct primes.} \\ 0, & \text{else.} \end{cases}$$

Further, if f is multiplicative, then g is also multiplicative and vice versa. In that case

$$\sum_{d=1}^{\infty} \frac{g(d)}{d} = \prod_p \left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\right).$$

Here note that, we are assuming convergence of the sums in many occasions. Also, it is not clear what happens if f is not exactly multiplicative and slightly different from that.

In [Luc79], Lucht showed the existence of mean values $M(F) = \lim\limits_{x\to\infty} \frac{1}{x} \sum\limits_{n \le x} F(n)$ for arithmetical function $F : N \to \mathbb{C}$ defined by $F(n) = \prod\limits_{t=1}^{k} f_t(L_t(n))$, where the f_t's under consideration are multiplicative and satisfies

$$|f_t| \le 1 \quad \text{and} \quad \sum_p \left| \frac{f_t(p) - 1}{p} \right| < \infty. \tag{2.0.1}$$

$L_t : n \to \frac{1}{\gamma_t}(\beta_t n + \alpha_t)$ are linear form with $\alpha_t \in \mathbb{Z}$, $(\beta_t, \gamma_t) \in \mathbb{N}^2$. This convergence condition is the main reason why many of the results, as discussed in *Section 1.2*, assume the condition of f_t's being close to 1.

In [Mir49], Mirsky discussed a simpler version of the above problem. To be more precise, he considered the sums of the type

$$\sum_{n \le x} f_1(n - h_1) f_2(n - h_2) \cdots f_k(n - h_k), \tag{2.0.2}$$

where each f_i are multiplicative and satisfy certain general conditions, whose underlining ideas are somewhat similar to ours. He was able to show that the (2.0.2) can be asymptotically estimated with small enough error term. Note that the functions f_i are need not be close to 1 in his case.

In this thesis, we consider functions F and G which are close to some 'smooth' functions A and B such that $\frac{F}{A}$ and $\frac{G}{B}$ are close to 1 and $A(n-h)B(n)$ should be nicely summable on every arithmetic progression. To make this more precise, we shall first recall the conditions (1.4.2), (1.4.3), (1.4.4), (1.4.5) as stated in *Chapter 1* and see how such conditions can be useful. We restate the conditions as follows.

$$F(n) = A(n)\sum_{d|n} f(d) \quad \text{and} \quad G(n) = B(n)\sum_{d|n} g(d), \tag{2.0.3}$$

$$\sum_{d=1}^{\infty} \frac{|f(d)|}{d} < +\infty, \quad \text{and} \quad \sum_{d=1}^{\infty} \frac{|g(d)|}{d} < +\infty. \tag{2.0.4}$$

$$\sum_{d\leq x} |f(d)| = O(E_2(x)), \quad \text{and} \quad \sum_{d\leq x} |g(d)| = O(E_3(x)). \tag{2.0.5}$$

$$\sum_{\substack{n\leq x \\ n\equiv a(\text{mod } m)}} A(n-h)B(n) = \frac{1}{m}M(x) + O_h(E_1(x)), \tag{2.0.6}$$

Now if $\frac{F(n)}{A(n)} = \sum_{d|n} f(d)$ and $\frac{G(n)}{B(n)} = \sum_{d|n} g(d)$, then changing order of summation, we shall arrive to the equality,

$$F(n-h)G(n) = \sum_{d\leq x-h} f(d) \sum_{\substack{d_1\leq x \\ (d,d_1)|h}} g(d_1) \sum_{\substack{n\leq x \\ n\equiv 0 \,(\text{mod } d_1) \\ n\equiv(0 \text{ mod } d)}} A(n-h)B(n).$$

So to proceed further, we assume (2.0.6), i.e. the existence of a good estimate of the sums of the type $\sum\limits_{\substack{n\leq x \\ n\equiv a \text{ mod } [d,d_1]}} A(n-h)B(n)$, where the main term is independent of a.

With these conditions, we compute the main term of $\sum_{n\leq x} F(n-h)G(n)$ explicitly. The additional condition of f and g being multiplicative in *Theorem 1.4.1* is only required to get an Euler product form of the constant C_h. Also, note that if $\frac{F}{A}$ is multiplicative, then by möbius inversion formula, f is uniquely determined. Further, the convergence conditions, such as (2.0.4) are automatically satisfied.

In the next part we structure the above discussion to a proof of the *Theorem 1.4.1*.

2.1 Proof of *Theorem 1.4.1*

Using (2.0.3), we have

$$\begin{aligned}
\sum_{n\leq x} F(n-h)G(n) &= \sum_{n\leq x} G(n)A(n-h)\sum_{d\mid n-h} f(d)\\
&= \sum_{d\leq x-h} f(d) \sum_{\substack{n\leq x\\ n\equiv h (\bmod\ d)}} G(n)A(n-h)\\
&= \sum_{d\leq x-h} f(d) \sum_{\substack{n\leq x\\ n\equiv h (\bmod\ d)}} A(n-h)B(n)\sum_{d_1\mid n} g(d_1)\\
&= \sum_{d\leq x-h} f(d) \sum_{\substack{d_1\leq x\\ (d,d_1)\mid h}} g(d_1) \sum_{\substack{n\leq x\\ n\equiv 0 (\bmod\ d_1)\\ n\equiv h (\bmod\ d)}} A(n-h)B(n)
\end{aligned}$$

If $(d,d_1)\mid h$, then using the Chinese remainder theorem ,

$$\left.\begin{aligned} n &\equiv 0(\bmod\ d_1)\\ n &\equiv h(\bmod\ d)\end{aligned}\right\} \Longleftrightarrow n\equiv a(\bmod\ [d,d_1]) \text{ for some } a.$$

By (2.0.6), this equals to

$$\begin{aligned}
&= \sum_{d\leq x-h} f(d) \sum_{\substack{d_1\leq x\\(d,d_1)|h}} g(d_1)\left(\frac{M(x)}{[d,d_1]} + O_h(E_1(x))\right), \\
&= M(x)\sum_{d\leq x-h} \frac{f(d)}{d} \sum_{\substack{d_1\leq x\\(d,d_1)|h}} \frac{g(d_1)(d,d_1)}{d_1} + O_h(E_1(x)E_2(x)E_3(x)). \qquad (2.1.1)
\end{aligned}$$

Now, using the fact $(d,d_1)\leq h$, the d-sum and d_1-sum can be extended to ∞ to get

$$M(x)\sum_{d=1}^{\infty} \frac{f(d)}{d} \sum_{\substack{d_1=1\\(d,d_1)|h}}^{\infty} \frac{g(d_1)(d,d_1)}{d_1}$$

with an error term,

$$O(hM(x)\sum_{1\leq d<+\infty} \frac{|f(d)|}{d} \sum_{d_1>x} \frac{|g(d_1)|}{d_1}) + O(hM(x)\sum_{d>x-h} \frac{|f(d)|}{d} \sum_{d_1\leq x} \frac{|g(d_1)|}{d_1}).$$

Now note that

$$\begin{aligned}
\sum_{d>x} \frac{|f(d)|}{d} &= \sum_{x<d\leq 2x} \frac{|f(d)|}{d} + \sum_{2x<d\leq 4x} \frac{|f(d)|}{d} + \sum_{4x<d\leq 8x} \frac{|f(d)|}{d} + \cdots \\
&\ll \frac{E_2(2x)}{x} + \frac{E_2(4x)}{2x} + \frac{E_2(8x)}{4x} + \cdots \\
&\leq \frac{E_2(x)}{x}(c + c^2/2 + c^3/4 + c^4/8 + \cdots) \\
&\leq \frac{2c}{2-c}\frac{E_2(x)}{x}.
\end{aligned}$$

Similarly $\sum_{d_1>x} \frac{|g(d_1)|}{d_1} \ll \frac{2c}{2-c}\frac{E_3(x)}{x}$.

Then by (2.1.1),

$$\sum_{n\le x} F(n-h)G(n) = M(x) \sum_{\substack{d,d_1\\(d,d_1)|h}} \frac{f(d)g(d_1)(d,d_1)}{dd_1} + O_h\left(|E_1(x)E_2(x)E_3(x)|\right)$$
$$+ O\left(\frac{ch}{2-c}\frac{|M(x)|}{x}(|E_2(x)|+|E_3(x)|)\right). \quad (2.1.2)$$

We now express $\sum\limits_{\substack{d,d_1\\(d,d_1)|h}} \frac{f(d)g(d_1)(d,d_1)}{dd_1}$ as an Euler product.

Let T be a multiplicative function, defined on prime powers by

$$T(p^k) := \frac{S_p(p^k)}{S_p(1)} = \frac{\sum\limits_{\min\{e_1,e_2\}=k} \frac{f(p^{e_1})g(p^{e_2})}{p^{e_1+e_2}}}{\sum\limits_{\min\{e_1,e_2\}=0} \frac{f(p^{e_1})g(p^{e_2})}{p^{e_1+e_2}}}.$$

Then, we claim that

$$\sum_{(d,d_1)=\ell} \frac{f(d)g(d_1)}{dd_1} = T(\ell) \sum_{(d,d_1)=1} \frac{f(d)g(d_1)}{dd_1}. \quad (2.1.3)$$

To prove this, note that

$$\sum_{(d,d_1)=\ell} \frac{f(d)g(d_1)}{dd_1} = \prod_{p|\ell} S_p(p^{\nu_p(\ell)}) \prod_{p\nmid\ell} S_p(1)$$

where $S_p(p^i) := \sum\limits_{\min\{e_1,e_2\}=i} \frac{f(p^{e_1})g(p^{e_2})}{p^{e_1+e_2}}$, for $i \ge 0$. This follows from expanding the product from the right hand side.

Similarly,

$$\sum_{(d,d_1)=1} \frac{f(d)g(d_1)}{dd_1} = \prod_{p} S_p(1).$$

Hence, dividing the two quantities, (2.1.3) follows.

Now

$$\sum_{\substack{d,d_1\\(d,d_1)|h}} \frac{f(d)g(d_1)(d,d_1)}{dd_1} = \sum_{\ell|h} \ell \sum_{(d,d_1)=\ell} \frac{f(d)g(d_1)}{dd_1}$$
$$= \sum_{\ell|h} \ell T(\ell) \sum_{(d,d_1)=1} \frac{f(d)g(d_1)}{dd_1}.$$

Since T is multiplicative, the right hand side equals to

$$= \left(\sum_{(d,d_1)=1} \frac{f(d)g(d_1)}{dd_1} \right) \prod_{p|h} (1 + pT(p) + \cdots + p^{\nu_p(h)} T(p^{\nu_p(h)}))$$
$$= \prod_{p} \left(1 + \frac{f(p)+g(p)}{p} + \frac{f(p^2)+g(p^2)}{p^2} + \cdots \right) \times$$
$$\prod_{p|h} \left(1 + pT(p) + \cdots + p^{\nu_p(h)} T(p^{\nu_p(h)})\right),$$

which proves the result. □

Before going in the proof of *Theorem 1.3.1*, we try to see how the above result can be used in practice. For that we recall *Corollary 1.4.1* from *Section 1.4*.

In the first case of the Corollary, we need to estimate $\sum\limits_{n \le x} \phi(n)\phi(n-h)$ where $\phi(n) = n \prod\limits_{p|n} \left(1 - \frac{1}{p}\right)$. In this case we choose $A(n) = B(n) = n$ and hence $F(n) = G(n) = \prod\limits_{p|n} \left(1 - \frac{1}{p}\right)$. So we have

$$f(p^k) = g(p^k) = \begin{cases} 1, & \text{if } k = 0; \\ -\frac{1}{p} & \text{if } k = 1; \\ 0, & \text{else.} \end{cases}$$

Now,

$$\sum_{\substack{n\le x\\ n\equiv a(\bmod m)}} A(n-h)B(n) = \sum_{\substack{n\le x\\ n\equiv a(\bmod m)}} n^2 - h \sum_{\substack{n\le x\\ n\equiv a(\bmod m)}} n$$
$$= \frac{1}{m}x^3 + O(mx + hx^2).$$

Also, the convergence conditions such as $\sum_d \frac{|f(d)|}{d} < +\infty$ and $\sum_d \frac{|g(d)|}{d} < +\infty$ are satisfied.

While for the Jordan totient function $J_k(n) = n^k \prod_{p|n}\left(1 - \frac{1}{p^k}\right)$, one takes $A(n) = B(n) = n^k$. The remaining computations are similar to the ϕ function case discussed above. As another application of the above theorem, we shall give a proof of *Theorem 1.3.1* in the next section.

2.2 Proof of *Theorem 1.3.1*

Recall that, $K^*(N) = C_2^* F^*(N-1)G^*(N)$ where C_2^*, F^* and G^* are given as

$$C_2^* = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)$$
$$F^*(N) = \prod_{\substack{p|N\\ p>2}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p|N}\left(1 - \frac{1}{(p-1)^2(p+1)}\right)$$
$$G^*(N) = \frac{N}{\varphi(N)} \prod_{\substack{p|N\\ p>2}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p|N}\left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right).$$

Now following the notations of *Theorem 1.4.1*, $A(n) = B(n) = 1$, and hence $M(x) = x$ in this case.

Also, if we set

$$f^*(m) = \sum_{d|m} \mu(d) F^*(m/d) \tag{2.2.1}$$

and

$$g^*(m) = \sum_{d|m} \mu(d) G^*(m/d), \tag{2.2.2}$$

then f^*, g^* are multiplicative functions. So it is enough to compute the values on prime powers. It is straightforward to check that

$$f^*(p^k) = \begin{cases} 1, & \text{if } k = 0 \\ 1/(p+1)(p-2), & \text{if } k = 1 \\ 0, & \text{else.} \end{cases}$$

$$g^*(p^k) = \begin{cases} 1, & \text{if } k = 0 \\ (p-1)/p^k(p-2), & \text{if } k \geq 1 \end{cases}$$

for an odd prime p. Also

$$f^*(2^k) = \begin{cases} -1/3, & \text{if } k = 1 \\ 0, & \text{if } k \geq 2 \end{cases}$$

$$g^*(2^k) = \begin{cases} 0, & \text{for } k = 1 \\ 1/2^{k-1}, & \text{if } k \geq 2. \end{cases}$$

First, we shall compute the error terms $E_1(x)$, $E_2(x)$ and $E_3(x)$ as defined in *Theorem 1.4.1.*

It is easy to see that $E_1(x) = O(1)$.

Now,

$$\begin{aligned}
E_2(x) &= \sum_{d\le x} |f^*(d)| \\
&\ll \prod_{p\le x}(1+f^*(p)+f^*(p^2)+\cdots) \\
&\ll \prod_{2<p\le x}(1+\frac{1}{(p+1)(p-2)}) \\
&= O(1).
\end{aligned}$$

Also

$$\begin{aligned}
E_3(x) &= \sum_{d_1\le x} |g^*(d_1)| \\
&\le \prod_{p\le x}(1+g^*(p)+g^*(p^2)+\cdots) \\
&\le \prod_{2<p\le x}(1+\frac{1}{p-2}) \\
&\ll \log x.
\end{aligned}$$

If p is an odd prime,

$$\begin{aligned}
1+\sum_{i=1}^{+\infty}\frac{f^*(p^i)+g^*(p^i)}{p^i} &= 1+\frac{1/(p+1)(p-2)+(p-1)/p(p-2)}{p}+\frac{p-1}{p-2}\sum_{i\ge 2}\frac{1}{p^{2i}} \\
&= 1+\frac{1}{p(p+1)(p-2)}+\frac{p-1}{p-2}\frac{1}{p^2-1} \\
&= \frac{(p-1)^2}{p(p-2)} \\
&= \left(1-\frac{1}{(p-1)^2}\right)^{-1}. \qquad (2.2.3)
\end{aligned}$$

Also

$$1+\sum_{i=1}^{\infty}\frac{f^*(2^i)+g^*(2^i)}{2^i}=1+\frac{(-1/3)}{2}+\sum_{j\geq 2}\frac{1}{2^{2j-1}}=1. \qquad (2.2.4)$$

Since $C_2^*=\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)$ this completes the proof of part *(a)*.

To prove part *(b)* of the theorem, we may assume that G is supported on odd integers only. Hence $G(2^k)=0$ for all $k\geq 1$. In this case

$$g^*(2^k)=\begin{cases}-1, & \text{if } k=1\\ 0, & \text{if } k\geq 2.\end{cases} \qquad (2.2.5)$$

This gives

$$\begin{aligned}1+\sum_{i=1}^{\infty}\frac{f^*(2^i)+g^*(2^i)}{2^i}&=1+\frac{(-1/3)+(-1)}{2}\\&=\frac{1}{3}.\end{aligned}$$

This proves *(b)*. □

2.3 Proof of *Theorem 1.4.2*

Next, we focus on the proof of *Theorem 1.4.2*. In *Theorem 1.4.2*, the function $\hat{K}(N)$ under consideration is not a product of two shifted multiplicative functions. Hence the proof of the theorem is not as straight forward as the last one. Our main idea is to replace the function $\hat{K}(N)$ by a simpler function while averaging.

Recall that

$$\hat{K}(N) = C_2^* F^*(N-1) G_1^*(N), \tag{2.3.1}$$

where $F^*(N)$ is defined as in (1.3.7) and

$$G_1^*(N) = \frac{N}{\phi(N)} \prod_{\substack{p|N \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{\substack{p^\alpha \| N \\ 2\nmid\alpha}} \left(1 - \frac{1}{p^\alpha(p-1)}\right) \prod_{\substack{p^\alpha \| N \\ 2|\alpha}} \left(1 - \frac{p - \left(\frac{-N_p}{p}\right)}{p^{\alpha+1}(p-1)}\right). \tag{2.3.2}$$

We write $G_1^*(N) = G_2^*(N) G_3^*(N)$, where

$$G_2^*(N) = \frac{N}{\phi(N)} \prod_{\substack{p|N \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{\substack{p^\alpha \| N \\ 2\nmid\alpha}} \left(1 - \frac{1}{p^\alpha(p-1)}\right)$$

and

$$G_3^*(N) = \prod_{p^{2\alpha} \| N} \left(1 - \frac{p - \left(\frac{-N_p}{p}\right)}{p^{2\alpha+1}(p-1)}\right). \tag{2.3.3}$$

Then G_2^* is multiplicative, but G_3^* is not. Write

$$G_2^*(N) = \sum_{l|N} \hat{g}(l).$$

Then, if $p \neq 2$,

$$\hat{g}(p^k) = \begin{cases} 1, \text{ if } k = 0 \\ \frac{(p-1)}{p(p-2)}, \text{ if } k = 1 \\ \frac{1}{p^{2s-1}(p-2)}, \text{ if } k = 2s, \ s \geq 1 \\ -\frac{1}{p^{2s+1}(p-2)}, \text{ if } k = 2s+1, \ s \geq 1 \end{cases}$$

and

$$\hat{g}(2^k) = \begin{cases} 1, \text{ if } k = 0 \\ 0, \text{ if } k = 1 \\ \frac{1}{2^{k-2}}, \text{ if } k = 2s, s \geq 1 \\ -\frac{1}{2^{k-1}}, \text{ if } k = 2s+1, s \geq 1. \end{cases}$$

Our claim, which is motivated from a similar idea in [MPS14], is that the whole computation of $\sum\limits_{N \leq x} F^*(N-1)G_1^*(N)$ remains the same even if we replace $\left(\frac{-N_p}{p}\right)$ in $G_3^*(N)$ by its expected value 0 for every prime. To make this rigorous, define

$$G_4^*(N) = \prod_{p^{2\alpha} \| N} \left(1 - \frac{1}{p^{2\alpha}(p-1)}\right).$$

For any d, l with $(d,l) = 1$, we claim that

$$\sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d) \\ N \equiv 0 (\text{mod } l)}} G_3^*(N) = \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d) \\ N \equiv 0 (\text{mod } l)}} G_4^*(N) + O(1). \tag{2.3.4}$$

In fact,

$$\begin{aligned} \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d) \\ N \equiv 0 (\text{mod } l)}} G_3^*(N) &= \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d) \\ N \equiv 0 (\text{mod } l)}} \prod_{p^{2\alpha} \| N} \left(1 - \frac{p - \left(\frac{-N_p}{p}\right)}{p^{2\alpha+1}(p-1)}\right) \\ &= \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d) \\ N \equiv 0 (\text{mod } l)}} \prod_{p^{2\alpha} \| N} \left(1 - \frac{1}{p^{2\alpha}(p-1)} + \frac{\left(\frac{-N_p}{p}\right)/p}{p^{2\alpha}(p-1)}\right). \end{aligned} \tag{2.3.5}$$

From now on l_1, l_2, l_3 are mutually co-prime positive integers. we define the following notations

$$\psi(l_i) = \prod_{p^\beta \| l_i} p^\beta (p-1),$$

$$A(m, l_i) = \prod_{p|l_i} \frac{\left(\frac{-m_p}{p}\right)}{p},$$

and

$$l_3' = \prod_{p|l_3} p.$$

Now if $\omega(m)$ denote the number of distinct prime divisors of m, then with these notations, (2.3.5) is equal to

$$\sum_{\substack{l_1 l_2^2 l_3^2 \leq x \\ l_1 l_2^2 l_3^2 \equiv 1 (\bmod d) \\ l_1 l_2^2 l_3^2 \equiv 0 (\bmod l)}} \frac{(-1)^{\omega(l_2)} A(l_1 l_2^2 l_3^2, l_3)}{\psi(l_2^2 l_3^2)} = \sum_{l_2^2 l_3^2 \leq x} \frac{(-1)^{\omega(l_2)}}{l_3' \psi(l_2^2 l_3^2)} \sum_{\substack{l_1 \\ l_1 l_2^2 l_3^2 \leq x \\ l_1 l_2^2 l_3^2 \equiv 1 (\bmod d) \\ l_1 l_2^2 l_3^2 \equiv 0 (\bmod l)}} \left(\frac{-l_1}{l_3'}\right). \qquad (2.3.6)$$

We replace $\left(\frac{-l_1}{l_3'}\right)$ by 1, for $l_3' = 1$, in the last summation. Also in case of $l_3' \geq 2$, the condition $(l_1, l_3) = 1$ is taken care of by $\left(\frac{-l_1}{l_3'}\right)$

Hence (2.3.6) can be broken into two parts, namely $S(x, l, d)$ and $E_5(x)$, where

$$S(x, l, d) = \sum_{l_2^2 \leq x} \frac{(-1)^{\omega(l_2)}}{\psi(l_2^2)} \sum_{\substack{l_1 \\ l_1 l_2^2 \leq x \\ l_1 l_2^2 \equiv 1 (\bmod d) \\ l_1 l_2^2 \equiv 0 (\bmod l)}} 1$$

and

$$E_5(x) = \sum_{\substack{l_2^2 l_3^2 \leq x \\ (l_2, l_3) = 1 \\ l_3' \geq 2}} \frac{(-1)^{\omega(l_2)}}{l_3' \psi(l_2^2 l_3^2)} \sum_{\substack{l_1 \\ l_1 l_2^2 l_3^2 \leq x \\ l_1 l_2^2 l_3^2 \equiv 1 (\bmod d) \\ l_1 l_2^2 l_3^2 \equiv 0 (\bmod l)}} \left(\frac{-l_1}{l_3'}\right).$$

If we rewrite G_4^* as

$$G_4^*(n) = \prod_{p^{2\alpha} \| N} \left(1 - \frac{1}{p^{2\alpha}(p-1)}\right),$$

then it is easy to check that

$$\sum_{\substack{N\leq x\\ N\equiv 1(\text{mod } d)\\ N\equiv 0(\text{mod } l)}} G_4^*(N) = S(x,l,d).$$

For $E_5(x)$, note that the congruence relations in the last summation of $E_5(x)$ have no solution unless $(l_2l_3,d)=1$. So if l_2 and l_3 are fixed with $(l_2l_3,d)=1$, then the congruence condition on the last summation of $E_5(x)$ is equivalent to $l_1\equiv b(\text{ mod } dl_0)$, for some b, where $l_0=\frac{l}{(l,l_2^2l_3^2)}$. Also the condition $(l_1,l_2)=1$ gives rise to $\phi(l_2)$ residue classes module l_2. While if $(l_1,l_3)>1$, then $\left(\frac{-l_1}{l_3'}\right)=0$.

Combining all of them together gives the following residue classes

$$l_1\equiv a_i(\text{ mod } M_{d,l,l_2,l_3}),\quad i=1,2,\cdots,\phi(l_2)$$

for some a_1, a_2,$\cdots$,$a_{\phi(l_2)}$, with $M_{d,l,l_2,l_3}=dl_0l_2$. Note that $(M_{d,l,l_2,l_3},l_3')=1$ in this case.

Then for each fixed a_i, the set $\{a_i,\ a_i+M_{d,l,l_2,l_3},\ a_i+2M_{d,l,l_2,l_3},\cdots,\ a_i+(l_3'-1)M_{d,l,l_2,l_3}\}$ runs over all possible residue class module l_3' exactly once. Now, if $l_3'\geq 3$ is odd, then we know that

$$\sum_{a=1}^{l_3'}\left(\frac{a}{l_3'}\right)=0.$$

Also, if l_3' is even, then $(M_{d,l,l_2,l_3},4l_3')=1$. In this case $\{a_i,\ a_i+M_{d,l,l_2,l_3},\ a_i+2M_{d,l,l_2,l_3},\cdots,\ a_i+(4l_3'-1)M_{d,l,l_2,l_3}\}$ covers every residue class modulo $4l_3'$. Since $\left(\frac{\cdot}{2}\right)$ is a character modulo 8, we know for even l_3',

$$\sum_{a=1}^{4l_3'-1}\left(\frac{a}{l_3'}\right)=0.$$

So, in any case,

$$\sum_{\substack{l_1 \\ l_1 l_2^2 l_3^2 \leq x \\ l_1 l_2^2 l_3^2 \equiv 1 (\text{mod } d) \\ l_1 l_2^2 l_3^2 \equiv 0 (\text{mod } l)}} \left(\frac{-l_1}{l_3'} \right) = O(l_2 l_3').$$

Hence,

$$\begin{aligned}
E_5(x) &= O(\sum_{\substack{l_2^2 l_3^2 \leq x \\ (l_2, l_3)=1}} \frac{1}{l_3' \psi(l_2^2 l_3^2)} l_2 l_3') \\
&= O(\sum_{l_2 \leq \sqrt{x}} \frac{l_2}{\psi(l_2^2)} \sum_{l_3 \leq \sqrt{x}} \frac{1}{\psi(l_3^2)}) \\
&= O(\sum_{l_2 \leq \sqrt{x}} \frac{l_2}{\psi(l_2^2)}) \\
&= O(\sum_{l_2 \leq \sqrt{x}} \frac{1}{\psi(l_2)}) \\
&= O(1),
\end{aligned}$$

which proves the claim.

Now with these notations, where $f^*(d)$ is as in (2.2.1), we have

$$\begin{aligned}
\sum_{N \leq x} F^*(N-1) G_1^*(N) &= \sum_{N \leq x} G_1^*(N) \sum_{d | N-1} f^*(d) \\
&= \sum_{d \leq x-1} f^*(d) \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d)}} G_1^*(N) \\
&= \sum_{d \leq x-1} f^*(d) \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d)}} G_2^*(N) G_3^*(N) \\
&= \sum_{d \leq x-1} f^*(d) \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d)}} G_3^*(N) \sum_{l | N} \hat{g}(l) \\
&= \sum_{d \leq x-1} f^*(d) \sum_{\substack{l \leq x \\ (l,d)=1}} \hat{g}(l) \sum_{\substack{N \leq x \\ N \equiv 1 (\text{mod } d) \\ N \equiv 0 (\text{mod } l)}} G_3^*(N).
\end{aligned}$$

Now, using (2.3.4) we get

$$\begin{aligned}\sum_{N\le x} F^*(N-1)G_1^*(N) &= \sum_{d\le x-1} f^*(d) \sum_{\substack{l\le x\\(l,d)=1}} \hat{g}(l) \sum_{\substack{N\le x\\ N\equiv 1(\text{mod } d)\\ N\equiv 0(\text{mod } l)}} G_4^*(N) + O(\sum_{d\le x-1} |f^*(d)| \sum_{\substack{l\le x\\(l,d)=1}} |\hat{g}(l)|)\\ &= \sum_{d\le x-1} f^*(d) \sum_{\substack{N\le x\\ N\equiv 1(\text{mod } d)}} G_2^*(N)G_4^*(N) + O(\log x)\\ &= \sum_{N\le x} F^*(N-1)G_2^*(N)G_4^*(N) + O(\log x). \qquad (2.3.7)\end{aligned}$$

But $G_2^*(N)G_4^*(N)$ is nothing but the $G^*(N)$, which has been defined in (1.3.8). Hence the $\sum\limits_{N\le x} \hat{K}(N)\frac{N}{\phi(N)}$ equals to $\sum\limits_{N\le x} K^*(N)$ up to an error $O(\log x)$. Then *Theorem 1.4.2* follows from *Theorem 1.3.1.* □

Chapter 3

Poisson distribution of $M_E(N)$

The primary goal of this chapter is to present the proofs of the theorems stated in *Section 1.5.* But before going into the proofs, first we are going to understand the approach for these types of problems and the machinery that are needed. To do that, we first introduce the required notations and definitions.

3.1 Notations and preliminaries

Let

$$E = E_{a,b} : y^2 = x^3 + ax + b \quad \text{and} \quad E' = E_{a',b'} : y^2 = x^3 + a'x + b'$$

be elliptic curves defined over a field k. An isomorphism $\psi : E \to E'$ is defined by an element $u \in k^*$ such that $a' = u^4 a$ and $b' = u^6 b$. An automorphism of E is defined to be an isomorphism from E to E. We denote the isomorphism class of E by $\tilde{E}$. Also $E \overset{u}{\cong} E'$ implies that E and E' are isomorphic by an element $u \in k^*$.

Now, if $k = \mathbb{F}_p$, be the finite field with p elements, then it is not difficult to check that

$$\left|Aut_{\mathbb{F}_p}(E_{a,b})\right| = \begin{cases} 6, & \text{if } a = 0 \text{ and } p \equiv 1 \pmod 4 \\ 4, & \text{if } b = 0 \text{ and } p \equiv 1 \pmod 4 \\ 2, & \text{else} \end{cases}$$

For a negative discriminant d, the *Kronecker symbol* χ_d is defined by $\chi_d(n) = \left(\frac{d}{n}\right)$. Note that χ_d is a multiplicative character modulo d. Let $L(s, \chi_d)$ be the $L-$function corresponding to χ_d define as

$$L(s, \chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s} \quad \text{for } s \geq 1.$$

Since d is not a perfect square, χ_d is not a principal character and hence $L(s, \chi_d)$ converges at $s = 1$.

Let D be a negative discriminant. The *Hurwitz-Kronecker class number* of discriminant D is defined by

$$H(D) = \sum_{\substack{f^2 | D \\ D/f^2 \equiv 0,1(\mod 4)}} \frac{h(D/f^2)}{\omega(D/f^2)}$$

where $h(d)$ denotes the usual class number of the unique imaginary quadratic order of discriminant $d < 0$ and $\omega(d)$ is the size of the unit group.

Also by class number formula [p. 515, [IK04]],

$$\frac{h(d)}{\omega(d)} = \frac{\sqrt{d}}{2\pi} L(1, \chi_d).$$

This in turns gives,

$$H(D) := \sum_{\substack{f^2 \mid D \\ D/f^2 \equiv 0,1 \pmod 4}} \frac{\sqrt{|D|}}{2\pi f} L(1, \chi_{D/f^2}) \tag{3.1.1}$$

First we shall see how the class number is related to our problem. The answer is the following well known theorem due to Deuring[Deu41].

Theorem C. *Let $p > 3$ be a prime and t be an integer such that $t^2 - 4p < 0$. Then*

$$\sum_{\substack{\tilde{E}/\mathbb{F}_p \\ a_p(\tilde{E}) = t}} \frac{1}{|Aut_{\mathbb{F}_p}(\tilde{E})|} = H(t^2 - 4p),$$

where the sum runs over the $\mathbb{F}_p$-isomorphism classes of elliptic curves with fixed trace t.

Now, if $|\tilde{E}(\mathbb{F}_p)| = N$, then $a_p = p+1-N$. In that case $(t^2 - 4p) = (p+1-N)^2 - 4p = (N+1-p)^2 - 4N$. We denote it by

$$D_N(p) := (N + 1 - p)^2 - 4N, \tag{3.1.2}$$

Also, recall that $N^+ := (\sqrt{N} + 1)^2$ and $N^- := (\sqrt{N} - 1)^2$.

So, by Deuring's theorem we get

$$H(D_N(p)) = \sum_{\substack{\tilde{E}/\mathbb{F}_p \\ |\tilde{E}(\mathbb{F}_p)| = N}} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_p}(\tilde{E})|}, \tag{3.1.3}$$

where the sum is over the F_p-isomorphism classes of elliptic curves.

Next, we see how the right hand side of (3.1.3) relates to a sum of the type

$\sum\limits_{E \in \mathcal{C}(A,B)} M_E(N)$. Basically, one replaces $M_E(N)$ by $\sum\limits_{\substack{p \text{ prime} \\ E_p(\mathbb{F}_p)=N}} 1$. After a change in summation, this comes down to computing $\sum\limits_{p} \sum\limits_{\substack{E \in \mathcal{C}(A,B) \\ E_p(\mathbb{F}_p)=N}} 1$.

Now the counting in the last summation can also be done in two steps as follows

$$\sum_{\substack{\tilde{E}/\mathbb{F}_p \\ \tilde{E}(\mathbb{F}_p)=N}} \sum_{\substack{E \in \mathcal{C}(A,B) \\ E \cong_p \tilde{E}}} 1$$

where the first sum runs over the isomorphic class of curves over $\mathbb{F}_p$ with the group order is N.

The last sum is $\sim \frac{\#\mathcal{C}(A,B)}{|Aut_p(\tilde{E})|}$. Then from Deuring's theorem, the denominator gives rise to the class number $H(D_N(p))$. So finally it comes down to computing the average of the type $\sum\limits_{N^- < p < N^+} H(D_N(p))$.

In [DS13], this is the main idea behind the proof of *Theorem A*, as stated in *Section 1.2*. David and Smith were able to compute an asymptotic for $\sum_{N^- < p < N^+}$, under the assumption of *Conjecture 1*.

In the remaining part of this chapter, we are going to adopt the above approach to complete the proofs of the theorems stated in *Section 1.5*.

In the next section, we state some required results related to short interval averages of the function $H(D_N(p))$.

3.2 Estimation of class numbers

In our proofs, we are going to use various estimation of $H(D)$. Importantly, most of the required results related to $H(D)$ has already been proved in [DS13] and [CDKS14]. We state some of the results as follows.

Proposition 3.2.1. *Fix R to be a positive integer. Then for $x \geq 1$,*

$$\frac{1}{x}\sum_{1\leq N\leq x} |\sum_{N^-<p<N^+} H(D_N(p)) - \frac{K(N)N^2}{\phi(N)\log N}| \ll_R \frac{x}{(\log x)^R}.$$

The above proposition has been proved in (Theorem 1.8, [CDKS14]).

Note that, on the left hand side of *Proposition 3.2.1*, $p \approx N$ and $|D_N(p)| \leq 4N$.

We also prove the following lemma

Lemma 3.2.1. *Let N be a positive integers and N^-, N^+ and $H(D_N(p))$ are defined as before. Then*

(a)

$$\sum_{N^-<p<N^+} H(D_N(p)) \ll \frac{N^2}{\phi(N)\log N}.$$

(b) Also for $k \geq 2$,

$$\sum_{N^-<p<N^+} H(D_N(p))^k \ll N^{\frac{k+1}{2}}(\log N)^{k-2}(\log\log N)^k.$$

Proof. Part (a) essentially follows from [Theorem 1.7, [CDKS14]]. Also see [DS13].

To prove part (b), we recall that

$$H(D_N(p)) = \sum_{\substack{f^2|D_N(p)\\ \frac{D_N(p)}{f^2}\equiv 0,1(\bmod 4)}} \frac{\sqrt{|D_N(p)|}}{2\pi f} L(1,\chi_{d_{N,f}(p)})$$

where $d_{N,f}(p) := \frac{D_N(p)}{f^2}$.

Now $|D_N(p)| \leq 4N$ in the above range of p. Also $L(1,\chi_{d_{N,f}(p)}) \ll \log N$ using convexity bound. Further, using the fact that $\sum_{d|n} \frac{1}{d} \ll \log\log n$, we get

$$\begin{aligned} H(D_N(p)) &\ll \sum_{\substack{f^2|D_N(p) \\ \frac{D_N(p)}{f^2} \equiv 0,1 (\bmod 4)}} \frac{\sqrt{N}\log N}{f} \\ &\ll \sqrt{N}\log N \log\log N. \qquad (3.2.1) \end{aligned}$$

Then, (3.2.1) along with part (a) completes the proof. □

Probably a stronger bound for the second part of the previous lemma could be proved. But for the purpose of this paper, this result is sufficient.

3.3 Curves with fixed order modulo primes

We first recall the following lemma [Corollary 2F, [Sch76]]:

Lemma 3.3.1. *Suppose p is a prime. Suppose $g(x) = a_n x^n + \cdots + a_0$ is a polynomial with integer coefficients having $0 < n < p$ and $p \nmid a_n$. Then*

$$|\sum_{x=0}^{p-1} e\left(\frac{g(x)}{p}\right)| \leq (n-1)p^{\frac{1}{2}}.$$

From now on $E_{s,t}$ will denote the elliptic curve given by a Weierstrass equation of the form $y^2 = x^3 + sx + t$. Also note that, if the corresponding field is of characteristic different from 2 or 3, then any isomorphism class of curve can be represented by one such Weierstrass equation. By $\tilde{E}_{s,t}$, we denote the isomorphism class of $E_{s,t}$, over the field of definition. If p is a prime, then $E_p \cong_p \tilde{E}_{s,t}$ represents an isomorphism over the field $\mathbb{F}_p$ between the reduced curve E_p and the representative $E_{s,t}$ of the class $\tilde{E}_{s,t}$. With these notations, we state the following result

Proposition 3.3.1. *Let $\{p_i\}_{i=1}^{\ell}$ be a set of ℓ distinct primes in the range* $[N^-, N^+]$

and $\{\tilde{E}_{s_i,t_i}/\mathbb{F}_{p_i}\}_{i=1}^{\ell}$ *be a set of isomorphism class of elliptic curves over corresponding fields* $\mathbb{F}_{p_i}$*'s. Then for the class of rational curves* $\mathcal{C}(A,B)$ *as defined in (1.2.5),*

$$\#\{E \in \mathcal{C}(A,B) : \, E_{p_i} \cong_{p_i} \tilde{E}_{s_i,t_i} \text{ for } 1 \leq i \leq \ell\} = \frac{4AB}{p_1 \cdots p_\ell} \prod_{i=1}^{\ell} \left(\frac{1}{|Aut_{p_i}(E_{s_i,t_i})|} \right) + \mathcal{E}_\ell(A,B,N) \tag{3.3.1}$$

where

$$\mathcal{E}_\ell(A,B,N) \ll \frac{AB}{N^{2\ell}} + N^{\frac{\ell}{2}}(\log N)^2 + (A\prod_{t_i=0}\sqrt{N} + B\prod_{s_i=0}\sqrt{N})N^{-\frac{\ell}{2}}\log N.$$

Proof. We use a modified version of the character sum argument used by Fouvry and Murty (p. 94, [FM96]). First, subdivide the interval $[-A, A]$ into intervals of length $p_1 \cdots p_\ell$, starting from $[-A, -A + p_1 p_2 \ldots p_\ell]$. The last one is denoted by $\mathcal{A}$. Similarly for $[-B, B]$, with the last one as $\mathcal{B}$.

Note that, for a isomorphism class $\tilde{E}_{s,t}$, the number of elliptic curves E_p over $\mathbb{F}_p$ such that $E_p \equiv_p E_{s,t}$ is $\frac{(p-1)}{|Aut_p(E_{s,t})|}$. This is due to the fact that the isomorphisms are given by $u \in \mathbb{F}_p^*$ by $(s,t) \mapsto (u^4 s, u^6 t)$. Out of $p - 1 = |\mathbb{F}_p^*|$ such u's, only $\frac{p-1}{|Aut(E_{s,t})|}$ of them gives rise to distinct pairs $(u^4 s, u^6 t)$ or distinct curves $E_{u^4 s, u^6 t}/\mathbb{F}_p$. Now, using the Chinese remainder theorem, we get

$$\begin{aligned}
&\#\{E \in \mathcal{C}(A,B) : \, E \cong_{p_i} \tilde{E}_{s_i,t_i} \text{ for } 1 \leq i \leq \ell\} \\
&= \left[\frac{2A}{p_1 \cdots p_\ell}\right] \left[\frac{2B}{p_1 \cdots p_\ell}\right] \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{|Aut_{p_i}(E_{s_i,t_i})}| \right) \\
&+ \left[\frac{2A}{p_1 \cdots p_\ell}\right] \frac{\#\{(u_1, \cdots u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : t_i u_i^6 \in \mathcal{B}(\text{mod } p_i), \, \forall 1 \leq i \leq \ell\}}{\prod_{i=1}^{\ell} |Aut_{p_i}(E_{s_i,t_i})|} \\
&+ \left[\frac{2B}{p_1 \cdots p_\ell}\right] \frac{\#\{(u_1, \cdots u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : s_i u_i^4 \in \mathcal{A}(\text{mod } p_i), \, \forall 1 \leq i \leq \ell\}}{\prod_{i=1}^{\ell} |Aut_{p_i}(E_{s_i,t_i})|} \\
&+ \frac{\#\{(u_1, \cdots, u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : s_i u_i^4 \in \mathcal{A}(\text{mod } p_i), \, t_i u_i^6 \in \mathcal{B}(\text{mod } p_i), \, \forall 1 \leq i \leq \ell\}}{\prod_{i=1}^{\ell} |Aut_{p_i}(E_{s_i,t_i})|} \\
&+ O\Big(\frac{AB}{p_1 \cdots p_\ell}\Big(\sum_{i=1}^{\ell} \frac{1}{p_i^9}\Big)\Big),
\end{aligned} \tag{3.3.2}$$

where the last error term comes from the rational curves of the form $E_{s_i u_i^4 p_i^4, t_i u_i^6 p_i^6}$.

Now from the fourth term on the right hand side of (3.3.2),

$$\begin{aligned}
&\#\left\{(u_1, \cdots u_\ell) \in \mathbb{F}_{p_1} \times \cdots \mathbb{F}_{p_\ell} : s_i u_i^4 \in \mathcal{A}(\text{mod } p_i),\, t_i u_i^6 \in \mathcal{B}(\text{mod } p_i),\, \forall 1 \le i \le \ell\right\} \\
&\quad = \frac{1}{(p_1 \cdots p_\ell)^2} \sum_{\substack{(h_1,\cdots,h_\ell) \\ 0 \le h_i \le p_i \\ 1 \le i \le \ell}} \sum_{\substack{(g_1,\cdots,g_\ell) \\ 0 \le g_i \le p_i \\ 1 \le i \le \ell}} \sum_{\substack{(u_1,\cdots,u_\ell) \\ 1 \le u_i \le p_i - 1 \\ 1 \le i \le \ell}} \sum_{(a,b) \in \mathcal{A} \times \mathcal{B}} e\left(\sum_{i=1}^{\ell} \frac{h_i(s_i u_i^4 - a) + g_i(t_i u_i^6 - b)}{p_i}\right),
\end{aligned} \tag{3.3.3}$$

where $e(x) = e^{2\pi i x}$.

When $(h_1, \cdots, h_\ell) = (0, \cdots, 0)$ and $(g_1, \cdots, g_\ell) = (0, \cdots, 0)$, the R.H.S of (3.3.3) gives a contribution equal to $|\mathcal{A}||\mathcal{B}| \prod_{i=1}^{\ell} (\frac{p_i - 1}{p_i^2})$. If $\| \alpha \|$ denotes the distance between α and its nearest integer, then using the fact that $\mathcal{A}$ and $\mathcal{B}$ are intervals, the contributions corresponding to $(h_1, \cdots, h_\ell) \neq (0, \cdots, 0)$, $(g_1, \cdots, g_\ell) \neq (0, \cdots, 0)$ are bounded by

$$\begin{aligned}
&\frac{1}{(p_1 \cdots p_\ell)^2} \sum_{\substack{(h_1,\cdots,h_\ell) \neq (0,\cdots,0) \\ 0 \le h_i \le p_i - i \\ 1 \le i \le \ell}} \sum_{\substack{(g_1,\cdots,g_\ell) \neq (0,\cdots,0) \\ 0 \le g_i \le p_i - 1 \\ 1 \le i \le \ell}} \left\| \frac{h_1}{p_1} + \cdots + \frac{h_\ell}{p_\ell} \right\|^{-1} \left\| \frac{g_1}{p_1} + \cdots + \frac{g_\ell}{p_\ell} \right\|^{-1} \\
&\qquad\qquad \times \prod_{i=1}^{\ell} \left(\sum_{u_i=1}^{p_i - 1} e\left(\frac{h_i s_i u_i^4 + g_i t_i u_i^6}{p_i} \right) \right).
\end{aligned} \tag{3.3.4}$$

This follows from the fact that $\sum_{n \in I} e(\alpha n) \ll \| \alpha \|^{-1}$, where I is an interval.

Now, if $h_i g_i$ is different from 0 for all i, then using *Lemma 3.3.1*,

$$\sum_{u_i=1}^{p_i - 1} e\left(\frac{h_i s_i u_i^4 + g_i t_i u_i^6}{p_i} \right) \le 5\sqrt{p}_i.$$

If $h_{i_1}, h_{i_2}, \cdots, h_{i_r}$ are zero and other h_i are non zero, then

$$\frac{1}{(p_1\cdots p_\ell)} \sum_{\substack{(h_1,\cdots,h_\ell)\neq(0,\cdots,0)\\ 0\le h_i\le p_i-i\\ 1\le i\le \ell\\ h_{i_1}=h_{i_2}=\cdots=h_{i_r}=0}} \left\|\frac{h_1}{p_1}+\cdots+\frac{h_\ell}{p_\ell}\right\|^{-1} = O\left(\frac{\log\left(\frac{p_1\cdots p_\ell}{p_{i_1}\cdots p_{i_r}}\right)}{p_{i_1}\cdots p_{i_r}}\right).$$

A similar result holds for g_i's. Without loss of generality, we may assume that $p_i \gg 2^{2\ell}$. In that case (3.3.4) is

$$O(\sqrt{p_1\cdots p_\ell}\log(p_1\cdots p_\ell)^2).$$

Similarly, considering contributions corresponding to $(h_1,\cdots,h_\ell)=(0,\cdots,0)$, $(g_1,\cdots,g_\ell)\neq(0,\cdots,0)$, as well as $(h_1,\cdots,h_\ell)\neq(0,\cdots,0)$, $(g_1,\cdots,g_\ell)=(0,\cdots,0)$, (3.3.3) equals

$$\begin{aligned}|\mathcal{A}||\mathcal{B}|\prod_{i=1}^{\ell}(\frac{p_i-1}{p_i^2}) + O(\frac{|\mathcal{A}|}{(p_1\cdots p_\ell)}\log(p_1\cdots p_\ell)\prod_{t_i=0}(p_i)\prod_{t_i\neq 0}\sqrt{(}p_i))\\ + O(\frac{|\mathcal{B}|}{(p_1\cdots p_\ell)}\log(p_1\cdots p_\ell)\prod_{s_i=0}(p_i)\prod_{s_i\neq 0}\sqrt{(}p_i)) + O(\sqrt{p_1\cdots p_\ell}\log(p_1\cdots p_\ell)^2)\end{aligned} \tag{3.3.5}$$

Proceeding in a similar way for the second and third term in the right hand side of

(3.3.2), we get the following

$$
\begin{aligned}
\#\{E \in \mathcal{C}(A,B) :\ E \cong_{p_i} \tilde{E}_{s_i,t_i} \text{ for } 1 \le i \le \ell\} &= \left[\frac{2A}{p_1\cdots p_\ell}\right]\left[\frac{2B}{p_1\cdots p_\ell}\right]\prod_{i=1}^{\ell}\left(\frac{p-1}{|Aut_{p_i}(E_{s_i,t_i})}\right) \\
&+ \left[\frac{2A}{p_1\cdots p_\ell}\right]\prod_{i=1}^{\ell}\frac{1}{|Aut_{p_i}(E_{s_i,t_i})|}\left[|\mathcal{B}|\prod_{i=1}^{\ell}\frac{p_i-1}{p_i} + O\left(\left(\prod_{s_i=0}p_i\right)\left(\prod_{s_i\neq 0}\sqrt{p_i}\right)\log(p_1\cdots p_\ell)\right)\right] \\
&+ \left[\frac{2B}{p_1\cdots p_\ell}\right]\prod_{i=1}^{\ell}\frac{1}{|Aut_{p_i}(E_{s_i,t_i})|}\left[|\mathcal{A}|\prod_{i=1}^{\ell}\frac{p_i-1}{p_i} + O\left(\left(\prod_{t_i=0}p_i\right)\left(\prod_{t_i\neq 0}\sqrt{p_i}\right)\log(p_1\cdots p_\ell)\right)\right] \\
&+ |\mathcal{A}||\mathcal{B}|\prod_{i=1}^{\ell}(\frac{p_i-1}{p_i^2}) + O(\frac{|\mathcal{A}|}{(p_1\cdots p_\ell)}\log(p_1\cdots p_\ell)\prod_{t_i=0}(p_i)\prod_{t_i\neq 0}\sqrt{(}p_i)) \\
&+ O(\frac{|\mathcal{B}|}{(p_1\cdots p_\ell)}\log(p_1\cdots p_\ell)\prod_{s_i=0}(p_i)\prod_{s_i\neq 0}\sqrt{(}p_i)) + O(\sqrt{p_1\cdots p_\ell}\log(p_1\cdots p_\ell)^2).
\end{aligned}
$$

By combining the terms together, we get

$$
\begin{aligned}
\#\{E \in \mathcal{C}(A,B) :\ E \cong_{p_i} \tilde{E}_{s_i,t_i} \text{ for } 1 \le i \le \ell\} &= \frac{4AB}{(p_1\cdots p_\ell)^2}\prod_{i=1}^{\ell}\left(\frac{p_i-1}{|Aut_{p_i}(E_{s_i,t_i})|}\right) \\
&+ O(\sqrt{p_1\cdots p_\ell}\log(p_1\cdots p_\ell)^2) + O\left(\frac{A}{(p_1\cdots p_\ell)}\log(p_1\cdots p_\ell)\left(\prod_{t_i=0}p_i\right)\left(\prod_{t_i\neq 0}\sqrt{p}_i\right)\right) \\
&+ O\left(\frac{B}{(p_1\cdots p_\ell)}\log(p_1\cdots p_\ell)\left(\prod_{s_i=0}p_i\right)\left(\prod_{s_i\neq 0}\sqrt{p}_i\right)\right), \qquad (3.3.6)
\end{aligned}
$$

and this proves *Proposition 3.3.1.* □

Lemma 3.3.2. *Let $\mathcal{C}(A,B)$ be as above. Now, for positive a integer ℓ and a positive constant γ_2,*

(a) If $A, B > N^{\frac{\ell}{2}}(\log N)^{1+\ell+\gamma_2}$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{2+\ell+\gamma_2}$, then

$$
\frac{1}{\#\mathcal{C}(A,B)}\sum_{N^- < p_1 \neq \cdots \neq p_\ell < N^+} \#\{E \in \mathcal{C}(A,B) : \#E_{p_1}(\mathbb{F}_{p_1}) = \cdots = \#E_{p_\ell}(\mathbb{F}_{p_\ell}) = N\} = \left(\sum_{N^- < p < N^+}\frac{H(D_N(p))}{p}\right)^{\ell} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right).
$$

(b) For $r \leq \ell$,

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{N^- < p_1, \cdots, p_r < N^+} \sum_{\substack{E \in \mathcal{C}(A,B),\, M_E(N) \geq \ell+1 \\ E_{p_1}(\mathbb{F}_{p_1}) = \cdots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1 \ll_\ell \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+1} + \frac{1}{(\log N)^{\ell+\gamma_2}}$$

Proof. Note that

$$\begin{aligned} &\#\{E \in \mathcal{C}(A,B) : \#E_{p_1}(\mathbb{F}_{p_1}) = \cdots = \#E_{p_\ell}(\mathbb{F}_{p_\ell}) = N\} \\ &\qquad = \sum_{\substack{\tilde{E}_1/\mathbb{F}_{p_1} \\ \tilde{E}_1(\mathbb{F}_{p_1}) = N}} \cdots \sum_{\substack{\tilde{E}_\ell/\mathbb{F}_{p_\ell} \\ \tilde{E}_\ell(\mathbb{F}_{p_\ell}) = N}} \#\{E \in \mathcal{C} : E_{p_i} \cong_{p_i} \tilde{E}_i \text{ for } 1 \leq i \leq \ell\}. \end{aligned} \tag{3.3.7}$$

If $N > 7$, then p is different from 2 and 3. Hence every isomorphism class of curve can be represented in a minimal Weierstrass equation, say $E_{s,t} : y^2 = x^3 + sx + t$ with $s, t \in \mathbb{F}_p$. Let each of the E_i are given as E_{s_i,t_i}. so we can use *Proposition 3.3.1* to estimate the summand in the right hand side of (3.3.7).

Now for a fixed prime p_i, the number of isomorphism class of curves E_{s_i,t_i} with $s_i t_i = 0$ is at most 10. Also recall that $\#\mathcal{C}(A,B) = 4AB + O(A+B)$ and $H(D_N(p_i)) = \sum_{E_{s_i,t_i}/\mathbb{F}_{p_i}} \frac{1}{|Aut_{p_i}(E_{s_i,t_i})|}$. Thus dividing (3.3.7) by $\mathcal{C}(A,B)$, the sum in the first part of the lemma equals to

$$\begin{aligned} \Sigma_1 &= \sum_{N^- < p_1 \neq p_2 \neq \cdots \neq p_\ell < N^+} \sum_{\substack{\tilde{E}_1/\mathbb{F}_{p_1} \\ \tilde{E}_1(\mathbb{F}_{p_1}) = N}} \cdots \sum_{\substack{\tilde{E}_\ell/\mathbb{F}_{p_\ell} \\ \tilde{E}_\ell(\mathbb{F}_{p_\ell}) = N}} \prod_{i=1}^{\ell} \frac{1}{p_i |Aut_{p_i}(E_{s_i,t_i})|} + \hat{\mathcal{E}}_\ell(A,B,N) \\ &= \sum_{N^- < p_1 \neq p_2 \neq \cdots \neq p_\ell < N^+} \left(\prod_{i=1}^{\ell} \frac{H(D_N(p_i))}{p_i} \right) + \hat{\mathcal{E}}_\ell(A,B,N) \end{aligned} \tag{3.3.8}$$

with

$$\hat{\mathcal{E}}_\ell(A,B,N) \ll \left\{ \frac{1}{N^{2\ell}} + \frac{\log N}{N^{\frac{\ell}{2}}} \left(\frac{1}{A} + \frac{1}{B} \right) + \frac{N^{\frac{\ell}{2}} (\log N)^2}{AB} \right\} \left(\frac{N \log\log N}{\log N} \right)^\ell$$

where the implied constant depends on ℓ only. Also, since $A, B > N^{\frac{\ell}{2}}(\log N)^{1+\ell+\gamma_2}$, and $AB > N^{\frac{3\ell}{2}}(\log N)^{2+\ell+\gamma_2}$ it follows that

$$\hat{\mathcal{E}}_\ell(A, B, N) \ll \frac{1}{(\log N)^{\ell+\gamma_2}}.$$

Further, if we relax the condition $p_1 \neq p_2 \neq \cdots \neq p_\ell$ from the right hand side of (3.3.8), then one gets

$$\begin{aligned}\Sigma_1 &= \sum_{\substack{(p_1,p_2,\cdots,p_\ell)\\ N^-<p_i<N^+ \ \forall i}} \prod_i \frac{H(D_N(p_i))}{p_i} + \sum_{\substack{(p_1,p_2,\cdots,p_\ell)\\ p_i=p_j \text{ for some } i\neq j\\ N^-<p_i<N^+ \ \forall i}} \prod_i \frac{H(D_N(p_i))}{p_i} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right)\\ &= \left(\sum_{N^<-p<N^+} \frac{H(D_N(p))}{p}\right)^\ell + O\left(\sum_{r=2}^{\ell}\left(\sum_{N^-<p<N^+}\frac{H(D_N(p))}{p}\right)^{\ell-r}\sum_{N^-<p<N^+}\frac{H(D_N(p))^r}{p^r}\right)\\ &\qquad + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right)\end{aligned} \tag{3.3.9}$$

Using *Lemma 3.2.1* it is easy to see that

$$\sum_{r=2}^{\ell}\left(\sum_{N^-<p<N^+}\frac{H(D_N(p))^r}{p^r}\right)\left(\sum_{N^-<p<N^+}\frac{H(D_N(p))}{p}\right)^{\ell-r} \ll O(N^{-\frac{1}{2}+\epsilon})$$

for any small $\epsilon > 0$. Hence

$$\Sigma_1 = \left(\sum_{N^-<p<N^+}\frac{H(D_N(p))}{p}\right)^\ell + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right). \tag{3.3.10}$$

This proves the result part (a) of the Lemma.

Now, if for a curve E, $M_E(N) = L \geq \ell + 1$, then E is counted L^r times in part (b).

While the same E will be counted $\frac{L!}{(\ell+1)!}$ times if we consider the expression

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{N^-<p_1\neq\cdots\neq p_{\ell+1}<N^+} \#\{E\in\mathcal{C}(A,B) : \#E_{p_1}(\mathbb{F}_{p_1}) = \cdots = \#E_{p_{\ell+1}}(\mathbb{F}_{p_{\ell+1}}) = N\}$$

Using Stirling's approximation, is easy to see that $\frac{L^r(\ell+1)!}{L!} \ll (\ell+1)^\ell$ for $r \leq \ell$. Hence part (b) follows from part (a). □

3.4 Some combinatorial arguments

Proposition 3.4.1. *Let $M_E(N)$ and $\mathcal{C}(A,B)$ be defined as before. Let ℓ is a positive integer and γ_1, γ_2 are nonnegative integers. If $A, B > x^{\frac{\ell+\gamma_1}{2}}(\log x)^{1+\ell+\gamma_2}$ and $AB > x^{\frac{3(\ell+\gamma_1)}{2}}(\log x)^{2+\ell+\gamma_2}$, then for any positive integer $r \leq \ell$,*

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{\substack{E\in\mathcal{C}(A,B)\\ M_E(N)\geq\ell}} M_E(N)^r = \sum_{j=\ell}^{\ell+\gamma_1} d_{\ell,r}(j)\left(\sum_{N^-<p<N^+}\frac{H(D_N(p))}{p}\right)^j$$
$$+O\left(\sum_p \frac{H(D_N(p))}{p}\right)^{\ell+\gamma_1+1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right),$$

where $d_{\ell,r}(j) = \sum_{k=\ell}^{j} \frac{k^r}{k!}\frac{(-1)^{j-k}}{(j-k)!}$.

Proof.

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{\substack{E\in\mathcal{C}(A,B)\\ M_E(N)\geq\ell}} M_E(N)^r = \frac{1}{\#\mathcal{C}(A,B)} \sum_{\substack{E\in\mathcal{C}(A,B)\\ M_E(N)\geq\ell}} \left(\sum_{\substack{N^-<p<N^+\\ E_p(\mathbb{F}_p)=N}} 1\right)^r$$
$$= \frac{1}{\#\mathcal{C}(A,B)} \sum_{N^-<p_1,\cdots,p_r<N^+} \sum_{\substack{E\in\mathcal{C}(A,B),\, M_E(N)\geq\ell\\ E_{p_1}(\mathbb{F}_{p_1})=\cdots=E_{p_r}(\mathbb{F}_{p_r})=N}} 1.$$

By breaking the sum into two parts depending on the value of $M_E(N)$, we get the following

$$\frac{1}{\#\mathcal{C}(A,B)}\sum_{N^-<p_1,\cdots,p_r<N^+}\sum_{j=\ell}^{\ell+\gamma_1}\sum_{M_E(N)=j}1+\frac{1}{\#\mathcal{C}(A,B)}\sum_{N^-<p_1,\cdots,p_r<N^+}\sum_{M_E(N)\geq\ell+\gamma_1+1}1 \tag{3.4.1}$$

where the range of summation is over $E\in\mathcal{C}(A,B)$ with $E_{p_1}(\mathbb{F}_{p_1})=\cdots=E_{p_r}(\mathbb{F}_{p_r})=N$. Now, by *Lemma 3.3.2*(b), the last sum in the right hand side is bounded by

$$\left(\sum_{N^-<p<N^+}\frac{H(D_N(p)}{p}\right)^{\ell+\gamma_1+1}+O(\frac{1}{(\log N)^{\ell+\gamma_2}})$$

Now, we claim that for $r\leq\ell\leq j\leq\ell+\gamma_1$

$$\sum_{N^-<p_1\neq p_2\neq\cdots\neq p_r<N^+}\sum_{\substack{E\in\mathcal{C}(A,B),\,M_E(N)=j\\E_{p_1}(\mathbb{F}_{p_1})=\cdots=E_{p_r}(\mathbb{F}_{p_r})=N}}1=\frac{1}{(j-r)!}\sum_{N^-<p_1\neq p_2\neq\cdots\neq p_j<N^+}\sum_{\substack{E\in\mathcal{C}(A,B),\,M_E(N)=j\\E_{p_1}(\mathbb{F}_{p_1})=\cdots=E_{p_j}(\mathbb{F}_{p_j})=N}}1 \tag{3.4.2}$$

In fact, any curve $E\in\mathcal{C}(A,B)$ with $M_E(N)=j$ is counted $\frac{j!}{(j-r)!}$ times in the left hand side summation, while on the right hand side, the same curve is counted $j!$ times.

We now consider the first term of (3.4.1). Note that the primes in the range of summations in (3.4.1) are not distinct. Then, using (3.4.2) and recalling the definition of $S(n,m)$, the Stirling number of the second kind, which equals to the number of ways of partitioning a set of n elements into m nonempty sets, we get

$$\sum_{N^- < p_1, \cdots, p_r < N^+} \sum_{\substack{E \in \mathcal{C},\, M_E(N) = j \\ E(\mathbb{F}_{p_1}) = \cdots = E(\mathbb{F}_{p_r}) = N}} 1 = \left(\sum_{m=1}^{r} \frac{S(r,m)}{(j-m)!} \right) \sum_{N^- < p_1 \neq p_2 \neq \cdots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A,B),\, M_E(N) = j \\ E_{p_1}(\mathbb{F}_{p_1}) = \cdots = E_{p_r}(\mathbb{F}_{p_j}) = N}} 1. \tag{3.4.3}$$

To simplify the constant on the right hand side, we use the fact that $\sum_{m=1}^{r} \frac{S(r,m) j!}{(j-m)!} = j^r$. See [(4.1.3), p. 60 , [Rom84]].

With this

$$\begin{aligned} &\sum_{N^- < p_1 \neq p_2 \neq \cdots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A,B),\, M_E(N) = j \\ E_{p_1}(\mathbb{F}_{p_1}) = \cdots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1 \\ &= \sum_{N^- < p_1 \neq p_2 \neq \cdots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A,B),\, M_E(N) \geq j \\ E(\mathbb{F}_{p_1}) = \cdots = E(\mathbb{F}_{p_j}) = N}} 1 - \sum_{N^- < p_1 \neq p_2 \neq \cdots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A,B),\, M_E(N) \geq j+1 \\ E(\mathbb{F}_{p_1}) = \cdots = E(\mathbb{F}_{p_j}) = N}} 1 \end{aligned} \tag{3.4.4}$$

Now, we plan to write (3.4.1) as a polynomial in $\sum\limits_{N^- < p < N^+} \frac{H(D_N(p))}{p}$ with a suitable error term. To find the correct coefficients of the polynomial, we introduce the following invariants.

We denote the left hand side of (3.4.2) by $\omega(r,j)$ and the first term of the right hand side of (3.4.4) by $\Omega(j,j)$. Also, we call the left hand side of (3.4.3) by $\Upsilon(r,j)$. Then in view of (3.4.2) and (3.4.3), we get the following set of relations

$$\begin{cases} \Upsilon(r,j) = \frac{j^r}{j!} \omega(j,j), \\ \Omega(t,s) = \sum\limits_{n=s}^{\infty} \omega(t,n) \quad \text{for } t \leq s, \\ \omega(t,n) = \frac{1}{(n-t)!} \omega(n,n) \quad \text{for } t \leq n. \end{cases} \tag{3.4.5}$$

Now, by *Lemma 3.3.2*(a),

$$\frac{1}{\#\mathcal{C}(A,B)} \times \Omega(j,j) = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O(\frac{1}{(\log N)^{j+\gamma_2}}),$$

whenever $A, B > x^{\frac{j}{2}} (\log x)^{1+j+\gamma_2}$ and $AB > x^{\frac{3j}{2}} (\log x)^{2+j+\gamma_2}$.

From (3.4.5), it is clear that ω's can be written is terms of Υ's as well as Ω's. Hence the equation

$$\sum_{j=\ell}^{\ell+\gamma_1} \Upsilon(r,j) = \sum_{j=\ell}^{\ell+\gamma_1} z_{\ell,r}(j)\Omega(j,j) + O(\Omega(\ell+\gamma_1, \ell+\gamma_1+1))$$

has a unique solution in the variables $\{z_{\ell,r}(j)\}$. Also note that

$$\Omega(\ell+\gamma_1, \ell+\gamma_1+1) \ll AB \left[\left(\sum_p \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1} + \frac{1}{(\log N)^{\ell+\gamma_2}} \right].$$

Then (3.4.1) equals to

$$\sum_{j=\ell}^{\ell+\gamma_1} z_{\ell,r}(j) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}} \right).$$

The only thing that remains to be shown is that $\{z_{\ell,r}(j)\}_j$ equals to $\{d_{\ell,r}(j)\}_j$, as defined in the statement of the proposition. For that, we prove the following lemma.

□

Lemma 3.4.1. *Consider ω, Ω as variables satisfying the identities in (3.4.5). Then the solution of the equation*

$$\sum_{j=\ell}^{\infty} \frac{j^r}{j!} \omega(j,j) = \sum_{j=\ell}^{\infty} z_{\ell,r}(j)\Omega(j,j)$$

in $z_{\ell,r}(j)$ is given by

$$z_{\ell,r}(j) = \sum_{k=\ell}^{j} \frac{k^r}{k!} \frac{(-1)^{j-k}}{(j-k)!}.$$

Proof. Using the second equation in (3.4.5), we have

$$\begin{aligned} \sum_{j=\ell}^{\infty} \frac{j^r}{j!}\omega(j,j) &= \sum_{j=\ell}^{\infty} z_{\ell,r}(j)\Omega(j,j) \\ &= \sum_{j=\ell}^{\infty} z_{\ell,r}(j) \sum_{n=j}^{\infty} \omega(j,n). \end{aligned}$$

By changing the order of summation, the right hand side equals to

$$= \sum_{n=\ell}^{\infty} \sum_{\ell \le j \le n} z_{\ell,r}(j)\omega(j,n) = \sum_{j=\ell}^{\infty} \sum_{\ell \le n \le j} z_{\ell,r}(n)\omega(n,j)$$

But by the last relation in (3.4.5), this can be written as

$$\sum_{j=\ell}^{\infty} \left(\sum_{\ell \le n \le j} \frac{z_{\ell,r}(n)}{(j-n)!} \right) \omega(j,j)$$

Thus, comparing the coefficients of $\omega(j,j)$ from both sides, we get

$$\sum_{\ell \le n \le j} \frac{z_{\ell,r}(n)}{(j-n)!} = \frac{j^r}{j!} \qquad \text{for } j \ge \ell. \tag{3.4.6}$$

Since we are only interested in the values of $z_{\ell,r}(n)$ for $\ell \le n \le \ell + \gamma_1$, we consider the following matrix equation

$$AZ = J,$$

where A is the $(\gamma_1 + 1) \times \ (\gamma_1 + 1)$ matrix $(a_{mn})_{m,n}$, where

$$a_{mn} = \begin{cases} 0, & \text{if } m < n, \\ \frac{1}{(m-n)!} & \text{if } m \geq n; \end{cases}$$

Also Z and J are the column matrices

$$\begin{bmatrix} z_{\ell,r}(\ell) & z_{\ell,r}(\ell+1) & \cdots & z_{\ell,r}(\ell+\gamma_1) \end{bmatrix}^{\mathrm{T}}$$

and

$$\begin{bmatrix} \frac{\ell^r}{\ell!} & \frac{(\ell+1)^r}{(\ell+1)!} & \cdots & \frac{(\ell+\gamma_1)^r}{(\ell+\gamma_1)!} \end{bmatrix}^{\mathrm{T}}$$

respectively.

Now it is not difficult to check that A is an invertible matrix with inverse $B = (b_{mn})$, where

$$b_{mn} = (-1)^{m-n} a_{mn}.$$

Finally, using $Z = A^{-1}J = BJ$, we get the desired value of $z_{\ell,r}(j)$'s. This completes the proof of the lemma.

□

3.5 Proof of *Theorem 1.5.1* and *Theorem 1.5.3*

Putting $\ell = 1$, $r = 1$ and $\gamma_1 = 0$, $\gamma_2 = \gamma$, in *Proposition 3.4.1* we get,

$$\frac{1}{\#\mathcal{C}(A,B)} \sum_{E \in \mathcal{C}(A,B)} M_E(N) = \sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} + O\left(\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}\right)^2\right) + O(\frac{1}{(\log N)^{1+\gamma}}) \tag{3.5.1}$$

for appropriate A, B. Then, using (3.5.1), we replace $\sum\limits_{N^- < p < N^+} \frac{H(D_N(p))}{p}$ in *Proposition 3.4.1* by $\frac{1}{\#\mathcal{C}(A,B)} \sum_{E \in \mathcal{C}(A,B)} M_E(N)$. We also recall that $d_{\ell,r}(\ell) = \frac{\ell^r}{\ell!}$. Now take $\gamma_1 = 0$, $r = 1$ and consider the sum $\frac{1}{\#\mathcal{C}(A,B)} \sum\limits_{\substack{E \in \mathcal{C}(A,B) \\ M_E(N) = \ell}} M_E(N) = \frac{1}{\#\mathcal{C}(A,B)} \sum\limits_{\substack{E \in \mathcal{C}(A,B) \\ M_E(N) = \ell}} \ell$. Then dividing the last equation by ℓ, *Theorem 1.5.1* follows immidiately from the above discussion.

Again, (3.5.1) together with *Proposition 3.4.1* and *Theorem A* completes the proof of *Theorem 1.5.3*. □

3.6 Proof of *Theorem 1.5.2*

First of all note that

$$\begin{aligned} \sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} &= \frac{1}{N} \sum_{N^- < p < N^+} H(D_N(p)) \left(1 + O\left(\frac{1}{\sqrt{N}}\right)\right) \\ &= \frac{1}{N} \sum_{N^- < p < N^+} H(D_N(p)) + \frac{1}{N^{\frac{3}{2}}} \sum_{N^- < p < N^+} |H(D_N(p))| \end{aligned}$$

Now, from Lemma 3.2.1(a), we get

$$\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} = \frac{1}{N} \sum_{N^- < p < N^+} H(D_N(p)) + O\left(\frac{\log\log N}{\sqrt{N}\log N}\right)$$

Also

$$\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}\right)^j = \frac{1}{N^j}\left(\sum_{N^- < p < N^+} H(D_N(p))\right)^j + O\left(\frac{1}{\sqrt{N}}\right)$$

Then,

$$\begin{aligned}\sum_{N \le x}\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}\right)^j &= \sum_{N \le x}\frac{1}{N^j}\left(\sum_{N^- < p < N^+} H(D_N(p))\right)^j + O(\sqrt{x}) \\ &= \sum_{N \le x}\left(\frac{K(N)N}{\phi(N)\log N}\right)^j + \tilde{\mathcal{E}}_1\end{aligned}$$

To bound the error $\tilde{\mathcal{E}}_1$, note that

$$\tilde{\mathcal{E}}_1 \ll \sum_{N \le x}\frac{1}{N^j}\left|\left(\sum_{N^- < p < N^+} H(D_N(p))\right)^j - \left(\frac{K(N)N^2}{\phi(N)\log N}\right)^j\right| + O(\sqrt{x})$$

Using Lemma 3.2.1(a), the right hand side is bounded by

$$\begin{aligned}&\sum_{N \le x}\frac{1}{N^j}\left|\sum_{N^- < p < N^+} H(D_N(p)) - \frac{K(N)N^2}{\phi(N)\log N}\right|\left(\frac{N^2}{\phi(N)\log N}\right)^{j-1} + O(\sqrt{x}) \\ \ll &\frac{1}{x}\sum_{N \le x}\left|\sum_{N^- < p < N^+} H(D_N(p)) - \frac{K(N)N^2}{\phi(N)\log N}\right| + \sqrt{x}\end{aligned}$$

Using *Proposition 3.2.1* with $R = 1 + \ell + \gamma_1$, the last summation is

$$\ll_{\ell,\gamma_1} \frac{x}{(\log x)^{1+\ell+\gamma_1}} + \sqrt{x}.$$

The only thing that remains is to estimate the main term, i.e.

$$\sum_{N\leq x}\left(\frac{K(N)N}{\phi(N)\log N}\right)^j$$

for every $\ell \leq j \leq \ell+\gamma_1$. To do this, we write

$$\left(\frac{K(N)N}{\phi(N)}\right)^j = \Theta F(N-1)G(N)$$

where

$$\begin{aligned}
\Theta &= \prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)^j \\
F(N) &= \prod_{\substack{p|N\\ p>2}}\left(1-\frac{1}{(p-1)^2}\right)^{-j}\prod_{p|N}\left(1-\frac{1}{(p-1)^2(p+1)}\right)^j \\
G(N) &= \left(\frac{N}{\phi(N)}\right)^j\prod_{\substack{p|N\\ p>2}}\left(1-\frac{1}{(p-1)^2}\right)^{-j}\prod_{p|N}\left(1-\frac{1}{p^{\nu_p(N)}(p-1)}\right)^j
\end{aligned}$$

Note that both F and G are multiplicative functions. We use *Theorem 1.4.1* with $A(n)=B(n)=1$, and hence $M(x)=x$. Also, if we set

$$f(m)=\sum_{d|m}\mu(d)F(m/d) \tag{3.6.1}$$

and

$$g(m)=\sum_{d|m}\mu(d)G(m/d), \tag{3.6.2}$$

then f,g are multiplicative functions. So it is enough to compute the values on prime powers. It is straightforward to check that

$$f(p^t) = \begin{cases} 1, \qquad \text{if } t = 0 \\ \left(1 - \frac{1}{(p-1)^2}\right)^{-j} \left(1 - \frac{1}{(p-1)^2(p+1)}\right)^{j} - 1, \quad \text{if } t = 1 \\ 0, \qquad \text{else,} \end{cases}$$

and

$$g(p^t) = \begin{cases} 1, \quad \text{if } t = 0 \\ (\frac{p}{p-1})^j (1 - \frac{1}{(p-1)^2})^{-j} (1 - \frac{1}{p(p-1)})^j - 1, \quad \text{if } t = 1 \\ (\frac{p}{p-1})^j (1 - \frac{1}{(p-1)^2})^{-j} [(1 - \frac{1}{p^t(p-1)})^j - (1 - \frac{1}{p^{t-1}(p-1)})^j], \qquad \text{if } t \geq 2, \end{cases}$$

for an odd prime p.

Also

$$f(2^t) = \begin{cases} (2/3)^j - 1, \qquad \text{if } t = 1 \\ 0, \qquad \text{if } t \geq 2, \end{cases}$$

and

$$g(2^t) = \begin{cases} 0, \quad \text{for } t = 1 \\ 2^j [(1 - \frac{1}{2^t})^j - (1 - \frac{1}{2^{t-1}})^j], \qquad \text{if } t \geq 2. \end{cases}$$

Then from *Theorem 1.4.1*, we know

$$\frac{1}{x} \sum_{N \leq x} \left(\frac{K(N)N}{\phi(N)} \right)^j = \mathit{\Theta} \sum_{N \leq x} F(N-1)G(N) = \mathit{\Theta} \prod_p \left(1 + \sum_{t \geq 1} \frac{f(p^t) + g(p^t)}{p^t} \right) + O\left(\frac{\log x}{x} \right).$$

But the constant in the main term is nothing but the $C(j)$, which has been defined in (1.5.4). Using partial summation, we get

$$\sum_{N\leq x}\left(\frac{K(N)N}{\phi(N)\log N}\right)^{j} = C(j)\int_{2}^{x}\frac{1}{(\log t)^{j}}\,dt + O\left(\frac{x}{(\log x)^{R_1}}\right)$$

for any $R_1 > 0$. By choosing $R_1 = 1 + \ell + \gamma_1$ we completes the proof of *Theorem 1.5.2.* □

It may be interesting to try to improve the error term in *Theorem 1.5.2.* This can be done by improving the *Proposition 3.2.1* or [Theorem 1.8, [CDKS14]], which is dependent on a result from [Kou14] on the distribution of primes in short arithmetic progressions. So again, one need to look at such problems related to distribution of primes.

We end the discussion on elliptic curve here. In the next chapter the questions are going to be independent of the earlier discussion.

Chapter 4

Additive Representation Function

In this chapter, we are going to focus on a problem in additive number theory. From the title of the chapter, it is evident that the problem is in some way related to the addition of subsets of integers.

Let $\mathcal{A} = \{a_1, a_2, \cdots\}(0 \leq a_1 < a_2 < \cdots)$ be an infinite sequence of non-negative integers. For $n \in \mathbb{N}_0$, define

$$R_1(n) = R_1(\mathcal{A}, n) = \sum_{a_i + a_j = n} 1, \tag{4.0.1}$$

$$R_2(n) = R_2(\mathcal{A}, n) = \sum_{\substack{a_i + a_j = n \\ i \leq j}} 1. \tag{4.0.2}$$

R_1 and R_2 are called additive representation functions. We are interested in monotonicity of these functions.

Now, it is easy to check that if $\mathcal{A}$ is a complement of a finite set inside the set of natural numbers, then both R_1 and R_2 are monotonically increasing for all large n. Here we are interested in the inverse problems, i.e., how the monotonicity of the representation functions affects the cardinality of the set $\mathcal{A}$.

The question of characterization of the set $\mathcal{A}$, under the condition that either $R_1(n)$

or $R_2(n)$ is monotonic, was raised by Erdős, Sárközy and Sós [ESS85]. Also see [Bal87], [CSST05], [TC09, ES85, ES86, ESS87] and [ESS86]. Erdős, Sárközy and Sós [ESS85] and Balasubramanian [Bal87] independently proved that $R_1(n)$ can be monotonically increasing from a certain point, only in a trivial way, i.e. if the set $\mathcal{A}$ is complement of a finite set of nonnegative integers.

Theorem D. *If $R_1(n+1) \geq R_1(n)$ for all large n, then $\mathbb{N} \setminus \mathcal{A}$ is a finite set.*

The analogous conclusion is not known to be true in the case of R_2. If, we define

$$\mathcal{A}(N) = |\mathcal{A} \cap [1, N]|, \tag{4.0.3}$$

then Balasubramanian [Bal87] proved the following theorem:

Theorem E. *If $R_2(n+1) \geq R_2(n)$ for all large n, then $\mathcal{A}(N) = N + O(\log N)$.*

In other words, if $R_2(n)$ is monotonic, then the complement set of $\mathcal{A}$ is at most of order $O(\log N)$.

In the first part of this chapter we shall focus on the function R_2 and quantities related to monotonicity of it. Also in *Section 4.5*, we shall make a remark concerning a question raised by Sárközy [Sar06], related to monotonicity of R_1.

In [ESS86], Erdős, Sárközy and Sós proved

Theorem F. *If*

$$\lim_{n \to +\infty} \frac{n - \mathcal{A}(n)}{\log n} = +\infty, \tag{4.0.4}$$

then we have,

$$\limsup_{N \to +\infty} \sum_{k=1}^{N} (R_2(2k) - R_2(2k+1)) = +\infty. \tag{4.0.5}$$

The assumption (4.0.4) in the above theorem cannot be relaxed. In fact Erdős, Sárközy and Sós [ESS86] constructed a sequence $\hat{\mathcal{A}}$ such that $(n - \hat{\mathcal{A}}(n)) > c \log n$ (for large n and fixed constant c) and

$$\limsup_{N \to +\infty} \sum_{k=1}^{N} (R_2(2k) - R_2(2k+1)) < +\infty.$$

In [TC05], Tang and Chen gave a quantitative version of *Theorem F*. We need the following definitions to state their theorem. Define S_n and $m(N)$ by

$$S_n = \sum_{k \le n} (R_2(2k) - R_2(2k+1)),$$
$$m(N) = N(\log N + \log \log N)$$

for any positive real number N.

Also the L^∞ norm of S_n, denoted by $T(N)$, is defined as follows:

$$T(N) = \max_{n \le m(N)} S_n = \max_{n \le m(N)} \sum_{k \le n} (R_2(2k) - R_2(2k+1)). \tag{4.0.6}$$

In [TC05], the authors proved that, when the ratio $\frac{T(N)}{\mathcal{A}(N)}$ is bounded above by a small enough fixed constant, then $T(N)$ and $\frac{N - \mathcal{A}(N)}{\log N}$ satisfies a simple inequality. More precisely,

Theorem G. *Let $T(N)$ be defined as in (4.0.6). If*

$$T(N) < \frac{1}{36} \mathcal{A}(N) \tag{4.0.7}$$

for all large enough N, then there exists a $C > 0$, depending only on $\mathcal{A}$, such that

$$T(N) > \frac{1}{80e} \frac{N - \mathcal{A}(N)}{\log N} - C \tag{4.0.8}$$

for all $N \geq 1$.

It is easy to see that, *Theorem G* implies *Theorem F*.

Now, set

$$S_n^+ = \max\{S_n, 0\}, \quad \text{and} \quad T^+(N) = \max_{n \leq m(N)} \{S_n^+\}.$$

Note: $T(N)$ and $T^+(N)$ are same unless all the elements of the set $\{S_n : n \leq m(N)\}$ are negative.

Here, we again assume that $\frac{T(N)}{\mathcal{A}(N)}$ is bounded above and prove an improved version of (4.0.8) where we replace the L^∞ norm of $S(n)$ by the L^1 norm of $\frac{S^+(n)}{n}$. More precisely, we prove the following theorem:

Theorem 4.0.1. *Let $\mathcal{A}$ be an infinite sequence of positive integers. Assume that there exists N_0 such that $T(N) < \frac{1}{36}\mathcal{A}(N)$ for $N \geq N_0$. Then there exists a constant $c_1 > 0$, depending on $\mathcal{A}$, such that*

$$\sum_{n=1}^{m(N)} \frac{S_n^+}{n} > \frac{1}{10e}(N - \mathcal{A}(N)) - \frac{1}{4}\log N - c_1, \tag{4.0.9}$$

for all $N \geq 1$.

Corollary 4.0.1. *If (4.0.7) in Theorem G holds, then for any $\epsilon > 0$,*

$$T^+(N) > \frac{1}{10e + \epsilon}\frac{N - \mathcal{A}(N)}{\log N} - \frac{1}{4}, \tag{4.0.10}$$

for any large enough N.

So, if at least one of $S(n)$ is non-negative, then $T^+(N)$ indeed equals $T(N)$. In that case, *Corollary 4.0.1* gives *Theorem G* with a better constant.

4.1 Generating Functions

It is more natural to consider the problem in terms of generating function.

Set

$$f(z) = \sum_{a \in \mathcal{A}} z^a, \quad \text{for } |z| < 1.$$

Then,

$$f(z)^2 = \sum_{n=1}^{+\infty} R_1(n) z^n.$$

For any positive real number Y, define

$$\psi(Y) = f(e^{-\frac{1}{Y}}) = \sum_{a \in \mathcal{A}} e^{-\frac{a}{Y}}, \tag{4.1.1}$$

and

$$g(Y) = 1 + 4(1 - e^{-\frac{2}{Y}}) \sum_{k=1}^{+\infty} S_k e^{-\frac{2k}{Y}}. \tag{4.1.2}$$

Theorem 4.1.1. *Let $g(Y)$ and $\psi(Y)$ be defined as above. Also assume*

$$g(Y) \leq \min\{\psi\left(\frac{Y}{2}\right), \frac{1}{9}Y\} \tag{4.1.3}$$

for all sufficiently large positive real numbers Y. Then

$$\psi(Y) \geq Y \exp\left(-\frac{2.3}{2Y}\left(\log_2 Y + \frac{16}{Y}\sum_{k=1}^{\infty} S_k^+ \frac{e^{-\frac{2k}{Y}}}{1 - e^{-\frac{2k}{Y}}}\right) - \frac{c}{Y}\right)$$

for some positive constant c depending only on first few elements of $\mathcal{A}$.

In *Section 4.3*, we will give a proof of *Theorem 4.1.1.* In *Section 4.4*, we will show how *Theorem 4.0.1* follows from *Theorem 4.1.1.*

4.2 Notations and preliminary lemmas

Consider a function $h : \mathbb{R} \mapsto [0, +\infty)$. For any real number Y and integer $\alpha \geq 0$, define $H(Y; \alpha)$ by the recurrences

$$\begin{aligned} H(Y;0) &= 0, \\ H(Y;\alpha) &= \frac{h(Y)}{2} + \frac{h(\frac{Y}{2})}{4} + \frac{h(\frac{Y}{4})}{8} + \cdots + \frac{h(\frac{Y}{2^{\alpha-1}})}{2^\alpha} \\ &= \sum_{j=0}^{\alpha-1} \frac{1}{2^{j+1}} h\left(\frac{Y}{2^j}\right), \quad \text{for integer } \alpha \geq 1. \end{aligned} \tag{4.2.1}$$

Also

$$H(Y) = \sum_{j=0}^{\infty} \frac{1}{2^{j+1}} h\left(\frac{Y}{2^j}\right). \tag{4.2.2}$$

Lemma 4.2.1. *If $h(Y)$ and $H(Y; \alpha)$ are defined as above and*

$$(\psi(Y))^2 \geq 2Y \exp(-h(Y)) \psi(\frac{Y}{2}) \tag{4.2.3}$$

for all real numbers $Y \geq \tilde{N}_0$, then for every integer $\alpha \geq 0$,

$$\psi(Y) \geq Y \exp(-H(Y;\alpha)) \left(\frac{\psi\left(\frac{Y}{2^\alpha}\right) 2^\alpha}{Y}\right)^{\frac{1}{2^\alpha}} \tag{4.2.4}$$

for any real number $Y \geq 2^\alpha \tilde{N}_0$.

Proof. We shall prove the result by induction.

For $\alpha = 0$, both sides of (4.2.4) are equal.

In the general case, suppose it is true for $\alpha = \alpha_0$. Then

$$\begin{aligned}(\psi(Y))^2 &\geq 2Y\exp(-h(Y))\psi\left(\frac{Y}{2}\right)\\ &\geq Y^2\exp\left(-h(Y) - H\left(\frac{Y}{2};\alpha_0\right)\right)\left(\frac{\psi\left(\frac{Y}{2^{\alpha_0+1}}\right)2^{\alpha_0+1}}{Y}\right)^{\frac{1}{2^{\alpha_0}}}, \quad \text{for } Y \geq 2^{\alpha+1}\tilde{N}_0\\ &= \left(Y\exp(-H(Y,\alpha_0+1))\left(\frac{\psi\left(\frac{Y}{2^{\alpha_0+1}}\right)2^{\alpha_0+1}}{Y}\right)^{\frac{1}{2^{\alpha_0+1}}}\right)^2.\end{aligned}$$

Hence the result is true for $\alpha = \alpha_0 + 1$. This concludes the proof. □

Lemma 4.2.2. *There exists a positive constant c such that, if Y is large enough, then we have*

$$\left(\frac{\psi\left(\frac{Y}{2^\alpha}\right)2^\alpha}{Y}\right)^{\frac{1}{2^\alpha}} \geq \exp(-\frac{c}{Y})$$

for some $\alpha \leq \log_2 Y$.

Proof. Now fix an interval $[a, 2a]$, with $a \geq 1$, so that $\psi(a) \geq 1$.

Then choose α suitably so that $\frac{Y}{2^\alpha} \in [a, 2a]$. In that case, we have

$$\left(\frac{\psi(\frac{Y}{2^\alpha})2^\alpha}{Y}\right)^{\frac{Y}{2^\alpha}} \geq \left(\frac{1}{2a}\right)^{2a} = \exp(-2a\log(2a)).$$

This proves the lemma. □

Lemma 4.2.3. *Let $0 < x < 1$ be a real number. Then* $\displaystyle\sum_{n=0}^{+\infty} 2^n x^{2^n} \leq \frac{2x}{1-x}$.

Proof. Note that

$$2^n x^{2^n} \leq 2\sum_{2^{n-1}<j\leq 2^n} x^j.$$

Summing over $n = 1$ to $+\infty$,

$$\sum_{n=1}^{+\infty} 2^n x^{2^n} \leq 2 \sum_{j=2}^{+\infty} x^j = \frac{2x^2}{1-x}.$$

Adding x corresponding to $n = 0$, on both sides, we get

$$\sum_{n=0}^{+\infty} 2^n x^{2^n} \leq \frac{2x^2}{1-x} + x = \frac{x(1+x)}{(1-x)}.$$

But since $x < 1$, this proves the result. □

Lemma 4.2.4. *In the notation of* Lemma 4.2.1, *let* $h(Y) = d\frac{g(Y)}{Y}$ *for some fixed positive constant d, to be chosen later. Then*

$$H(Y, \alpha) \leq \frac{d}{2Y}\left(\alpha + \frac{16}{Y}\sum_{k=1}^{\infty} S_k^+ \frac{e^{-\frac{2k}{Y}}}{1 - e^{-\frac{2k}{Y}}}\right).$$

Proof. Set $x = e^{-\frac{2}{Y}}$. Then

$$\begin{aligned} g(Y) &= 1 + 4(1 - e^{-\frac{2}{Y}}) \sum_{k=1}^{\infty} S_k x^k. \\ &\leq 1 + \frac{8}{Y} \sum_{k=1}^{\infty} S_k^+ x^k. \end{aligned}$$

Now,

$$\begin{aligned}
H(Y;\alpha) &= \sum_{j=0}^{\alpha-1} \frac{1}{2^{j+1}} h\left(\frac{Y}{2^j}\right) \\
&= \sum_{j=0}^{\alpha-1} \frac{d}{2^{j+1}} \frac{2^j}{Y} g(\frac{Y}{2^j}) \\
&\leq \sum_{j=0}^{\alpha-1} \frac{d}{2Y} \left(1 + \frac{8}{Y} \sum_{k=1}^{\infty} S_k^+ 2^j x^{k2^j}\right) \\
&\leq \frac{d}{2Y} \left(\alpha + \frac{8}{Y} \sum_{k=1}^{\infty} S_k^+ \sum_{j=0}^{\infty} 2^j x^{k2^j}\right) \\
&\leq \frac{d}{2Y} \left(\alpha + \frac{8}{Y} \sum_{k=1}^{\infty} S_k^+ \frac{2x^k}{1-x^k}\right).
\end{aligned}$$

□

4.3 Proof of *Theorem 4.1.1*

It is easy to verify the following equality by comparing the coefficients of z^n from both sides.

$$f(z^2) = \frac{1-z}{2z}(f(z))^2 + 2\sum_{k=1}^{+\infty}(R_2(2k) - R_2(2k+1))z^{2k} - \frac{(1+z)}{2z} f(-z)^2. \quad (4.3.1)$$

Choose z to be a positive real number. This gives

$$f(z^2) \leq \frac{1-z}{2z} f(z)^2 + 2\sum_{k=1}^{+\infty}(R_2(2k) - R_2(2k+1))z^{2k}. \quad (4.3.2)$$

Now, considering the right hand side of the summation, we get

$$\begin{aligned}\sum_{k=1}^{+\infty}(R_2(2k)-R_2(2k+1))z^{2k} &= \sum_{k=1}^{+\infty}(S_k-S_{k-1})z^{2k}\\ &= \sum_{k=1}^{+\infty}S_k(z^{2k}-z^{2k+2})-S_0z^2\\ &\leq (1-z^2)\sum_{k=1}^{+\infty}S_kz^{2k}.\end{aligned}$$

Thus, from (4.3.2) we get

$$f(z^2)\leq \frac{1-z}{2z}f(z)^2+2(1-z^2)\sum_{k=1}^{+\infty}S_kz^{2k}.$$

Now putting $z=e^{-\frac{1}{Y}}$, we get

$$\psi\left(\frac{Y}{2}\right)\leq \frac{1}{2}\left(\frac{1}{Y}+\frac{1}{Y^2}\right)(\psi(Y))^2+2(1-e^{-\frac{2}{Y}})\sum_{k=1}^{+\infty}S_ke^{-\frac{2k}{Y}}.$$

Since $\psi(Y)\leq Y$, this gives

$$2Y\psi\left(\frac{Y}{2}\right)\leq (\psi(Y))^2+Yg(Y).$$

Thus,

$$(\psi(Y))^2\geq 2Y\psi\left(\frac{Y}{2}\right)-Yg(Y). \tag{4.3.3}$$

Lemma 4.3.1. *If $g(Y)\leq\psi\left(\frac{Y}{2}\right)$, then for all large enough real numbers Y,*

$$\psi(Y)\geq 0.49Y.$$

Proof. Since $g(Y) \leq \psi\left(\frac{Y}{2}\right)$, using (4.3.3) we get

$$(\psi(Y))^2 \geq Y\psi\left(\frac{Y}{2}\right).$$

Then (4.2.3) in *Lemma 4.2.1* holds with $h(Y) = \log 2$.

In that case

$$H(Y) = \sum_{0 \leq j < +\infty} \frac{1}{2^{j+1}} h\left(\frac{Y}{2^j}\right) = \log 2.$$

This gives, by *Lemma 4.2.1* and *Lemma 4.2.2*,

$$\psi(Y) \geq 0.49Y$$

if Y is large enough. □

Thus, combining (4.3.3) and *Lemma 4.3.1* we get

$$\psi(Y)^2 \geq 2Y\psi\left(\frac{Y}{2}\right)\left(1 - \frac{g(Y)}{0.49Y}\right) \tag{4.3.4}$$

for sufficiently large Y.

Since $\frac{g(Y)}{Y} < \frac{1}{9}$, equation (4.2.3) in *Lemma 4.2.1* is satisfied with $h(Y) = 2.3\frac{g(Y)}{Y}$.

Hence *Lemma 4.2.4* and *Lemma 4.2.1* together give the following inequality

$$\psi(Y) \geq Y\exp\left(-\frac{2.3}{2Y}\left(\alpha + \frac{16}{Y}\sum_{k=1}^{+\infty} S_k^+\left(\frac{e^{-\frac{2k}{Y}}}{1 - e^{-\frac{2k}{Y}}}\right)\right)\right)\left(\frac{\psi\left(\frac{Y}{2^\alpha}\right)2^\alpha}{Y}\right)^{\frac{1}{2^\alpha}}. \tag{4.3.5}$$

Hence *Theorem 4.1.1* follows from (4.3.5) and *Lemma 4.2.2*.

4.4 Proof of *Theorem 4.0.1*

Lemma 4.4.1. *Let $g(Y)$ and $T(N)$ be as in (4.1.2) and (4.0.6). Then*

(a)

$$g(N) < 4T(N) + 40$$

for any real number $N \geq 40$.

(b) Further, if $(\mathbb{N} \setminus \mathcal{A})$ is infinite and $T(N) \leq \frac{1}{36}\mathcal{A}(N)$ for any real number $N \geq N_0$, then there exists $N_2 \geq N_0$ such that

$$g(N) \leq \min\{\psi\left(\frac{N}{2}\right), \frac{1}{9}N\}$$

for any real number $N \geq N_2$.

Proof. We have

$$\begin{aligned} g(N) &= 1 + 4(1 - e^{-\frac{2}{N}})\{\sum_{k \leq m(N)} S_k e^{-\frac{2k}{N}} + \sum_{k > m(N)} S_k e^{-\frac{2k}{N}}\} \\ &= 1 + 4(1 - e^{-\frac{2}{N}})\{\Sigma_3 + \Sigma_4\}, \quad \text{say.} \end{aligned}$$

For the first summation, we use the fact $S_k \leq T(N)$, for $k \leq m(N)$, while for the second we use the trivial estimate $S_k \leq \frac{k^2}{2}$.

In that case

$$\Sigma_3 \leq \sum_{k=0}^{+\infty} T(N) e^{-\frac{2k}{N}} = T(N) \frac{1}{1 - e^{-\frac{2}{N}}}$$

and

$$\Sigma_4 \le \sum_{k>m(N)} \frac{k^2}{2} e^{-\frac{2k}{N}} \le \int_{m(N)-1}^{+\infty} \frac{x^2}{2} e^{-\frac{2x}{N}}\, dx \le 4N,$$

using integration by parts and the fact that $m(N) = N(\log N + \log\log N)$. This proves *(a)*.

To prove *(b)* note that,

$$\mathcal{A}(N) = \sum_{\substack{a\in\mathcal{A} \\ a\le N}} 1 \le \sum_{\substack{a\in\mathcal{A} \\ a\le N}} e^{2-\frac{2a}{N}} \le e^2\psi(\frac{N}{2}). \tag{4.4.1}$$

Also, using $T(N) < \frac{1}{36}\mathcal{A}(N)$, from (a) we get

$$g(N) < \frac{1}{9}\mathcal{A}(N) + 40. \tag{4.4.2}$$

Then from (4.4.1) and (4.4.2), we get $g(N) < \frac{e^2}{9}\psi(\frac{N}{2}) + 40$.
Since $e^2 < 9$ and $\mathcal{A}$ is infinite, it follows $g(N) < \psi(\frac{N}{2})$, for sufficiently large N.

Also (4.4.2) can be written as $g(N) < \frac{1}{9}N - \frac{1}{9}(N - \mathcal{A}(N)) + 40$. As $\mathbb{N}\setminus\mathcal{A}$ are infinite, so we get (b) for sufficiently large N.

□

Notice that if $\mathbb{N}\setminus\mathcal{A}$ is finite set, then *Theorem 4.0.1* is satisfied trivially. So without loss of generality, we may assume that both $\mathcal{A}$ and $\mathbb{N}\setminus\mathcal{A}$ are infinite sets.

Then in view of *Lemma 4.4.1*, condition (4.1.3) of *Theorem 4.1.1* is satisfied. Hence

$$\frac{\psi(N)}{N} \geq \exp\left(-\frac{2.3}{2N}\left(\log_2 N + \frac{16}{N}\sum_{k=1}^{\infty} S_k^+ \frac{e^{-\frac{2k}{N}}}{1-e^{-\frac{2k}{N}}}\right) - \frac{c}{N}\right) \tag{4.4.3}$$

where c is the constant, as defined in *Lemma 4.2.2*.

Taking logarithm on both sides,

$$\begin{aligned}\frac{2.3}{2N}\left(\log_2 N + \frac{16}{N}\sum_{k=1}^{\infty} S_k^+ \frac{e^{-\frac{2k}{N}}}{1-e^{-\frac{2k}{N}}}\right) + \frac{c}{N} &\geq -\log\left(1-\left(1-\frac{\psi(N)}{N}\right)\right)\\ &> \left(1-\frac{\psi(N)}{N}\right).\end{aligned}$$

Now, following the calculation of Σ_4,

$$\frac{2.3}{2N}\left(\log_2 N + \frac{16}{N}\sum_{k=1}^{m(N)} S_k^+ \left(\frac{e^{-\frac{2k}{N}}}{1-e^{-\frac{2k}{N}}}\right) + 100\right) + \frac{c}{N} > \left(1-\frac{\psi(N)}{N}\right).$$

Now, $\frac{e^{-x}}{1-e^{-x}} \leq \frac{1}{x}$ and hence we can replace $\frac{e^{-\frac{2k}{N}}}{1-e^{-\frac{2k}{N}}}$ by $\frac{N}{2k}$, for $k \leq m(N)$. Hence

$$\frac{2.3}{2N}\left(\log_2 N + 8\sum_{k=1}^{m(N)} \frac{S_k^+}{k} + 100\right) + \frac{c}{N} > \frac{N-\psi(N)}{N}.$$

Also note that

$$\begin{aligned}
N-\psi(N) &= (\sum_{n=1}^{+\infty} e^{-n/N} + O(1)) - \sum_{a\in\mathcal{A}} e^{-a/N} \\
&= \sum_{\substack{n\notin\mathcal{A} \\ n\geq 1}} e^{-n/N} + O(1) \\
&\geq \sum_{\substack{n\notin\mathcal{A} \\ 1\leq n\leq N}} e^{-1} + O(1) \\
&= \frac{N-\mathcal{A}(N)}{e} + O(1).
\end{aligned}$$

It implies that

$$\sum_{k=1}^{m(N)} \frac{S_k^+}{k} > \frac{1}{10e}(N-\mathcal{A}(N)) - \frac{1}{8}\log_2 N - c_1 \tag{4.4.4}$$

for positive integer N and fixed constant c_1 depending on $\mathcal{A}$. This proves *Theorem 4.0.1.* □

4.5 Monotonicity of $R_1(n)$ on dense set of integers

In this section, we solve a question raised by Sárközy (see [Sar06])[Problem 5, Page 337]. His question was the following:
Does there exist an infinite set $\mathcal{A} \subset \mathbb{N}$ such that $\mathbb{N}\setminus\mathcal{A}$ is also infinite and $R_1(n+1) \geq R_1(n)$ holds on a sequence of integers n whose density is 1?

Here we show that the answer to this question is positive by giving a simple example.

A Sidon set is a set of positive integers such that the sums of any two terms are all different. i.e., $R_2(n) \leq 1$ for the corresponding R_2 function. By [AKS81], it is possible to construct Sidon sequence of order $(n\log n)^{\frac{1}{3}}$.

Now, let $\mathcal{B}$ be an infinite Sidon set of even integers and $\mathcal{A} = \mathbb{N}\setminus\mathcal{B}$;

Put

$$Y = (\mathcal{B} + \mathcal{B}) \cup \mathcal{B} \quad \text{and } X = \mathbb{N} \setminus Y;$$

Then,

$$R_1(n+1) \geq R_1(n) \quad \text{for all } n \in X.$$

To see this, let

$$f(z) = \sum_{a \in \mathcal{A}} z^a \quad \text{and } g(z) = \sum_{b \in \mathcal{B}} z^b.$$

Then,

$$\begin{aligned}
\sum_{n=1}^{+\infty} (R_1(n) - R_1(n-1)) z^n &= (1-z) f(z)^2 \\
&= (1-z)(\frac{z}{(1-z)} - g(z))^2 \\
&= \frac{z^2}{(1-z)} + (1-z)(g(z))^2 - 2zg(z).
\end{aligned}$$

Again, let

$$r_1(n) = \sum_{\substack{b_i + b_j = n \\ b_i \in \mathcal{B}, b_j \in \mathcal{B}}} 1,$$

So, $R_1(n+1) \geq R_1(n)$ iff coefficient of z^{n+1} in $(1-z)(f(z))^2$ is non negative.

$$\begin{aligned}
\text{Now coefficient of } z^{2k} \text{ is } &= 1 + r_1(2k) - r_1(2k-1) - 2\chi_{\mathcal{B}}(2k-1) \\
\text{and coefficient of } z^{2k+1} \text{ is } &= 1 + r_1(2k+1) - r_1(2k) - 2\chi_{\mathcal{B}}(2k).
\end{aligned}$$

Then, it is clear from the above choice of X and $\mathcal{A}$ that $R_1(n+1) \geq R_1(n)$ for all

n in X.

For example, we can take $\mathcal{B} = \{2, 4, 8, 16, 32, ..., 2^m, ...\}$. Then $\mathcal{B}$ is infinite and X is of density 1. □

Bibliography

[AKS81] M. Ajtai, J. Komlós and E. Szemerédi, A dense infinite Sidon sequence, *European J. Combin.* **2** (1981), 1-11.

[AS90] S.D. Adhikari,A. Sankaranarayanan, On an error term related to the Jordan totient function $J_k(n)$, J. Number Theory **34** (1990), 178-188.

[Bal87] R. Balasubramanian, A note on a result of Erdős, Sárközy and Sós, *Acta Arith.* **49** (1987), 45-53.

[BCD11] A. Balog, A.-C. Cojocaru, and C. David, Average twin prime conjecture for elliptic curves, Amer. J. Math. **133** (2011), 1179-1229.

[BPS12] W.D. Banks, F. Pappalardi, I.E. Shparlinski, On group structures realized by elliptic curves over arbitrary finite fields, Exp. Math. **21** (2012), 11-25.

[BS09] W.D. Banks, I.E. Shparlinski, Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height, Israel J. Math. **173** (2009), 253-277.

[CDKS14] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith, The frequency of elliptic curve groups over prime finite fields , arXiv:1405.6923 [math.NT].

[CS01] E.-H. Choi, W. Schwarz, Mean-values of products of shifted arithmetical functions. Analytic and probabilistic methods in number theory (Palanga, 2001), 32-41, TEV, Vilnius, 2002.

[CSST05] Y.G. Chen, A. Sárközy, V.T. Sós and M Tang, On The Monotonicity Properties of Additive Representations Functions, *Bull. Austral. Math. Soc.* **72** (2005), 129-138.

[Deu41] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkorpr. Abh. Math. Sem. Univ. Humbury, 14 (1941, no. 1), 197-272.

[DS13] C. David and E. Smith, Elliptic curves with a given number of points over finite fields, *Compositio Math.* **149** (2013), 175-203.

[DS14] C. David and E. Smith, Corrigendum to Elliptic curves with a given number of points over finite fields, *Compositio Math.* 150 (2014), no. 8, 1347-1348.

[EI90] P. Erdos and A. Ivic, The distribution of values of a certain class of arithmetic functions at consecutive integers. Number theory, Vol. I (Budapest, 1987), 45-91, Colloq. Math. Soc. Jnos Bolyai, **51**, North-Holland, Amsterdam, 1990.

[ES51] P. Erdős, H.N. Shapiro, On the changes of sign of a certain error function, Canadian J. Math. **3**, (1951), 375-385.

[ES85] P. Erdős and A. Sárközy, Problems and results on additive properties of general sequences. I, *Pacific J. Math.* **118** (1985), 347-357.

[ES86] P. Erdős and A. Sárközy, Problems and results on additive properties of general sequences. II, *Acta Math. Hungar.* **48** (1986), 201-211.

[ESS87] P. Erdős, A. Sárközy and V.T. Sós, Problems and results on additive properties of general sequences. III, *Studia Sci. Math. Hungar.* **22** (1987), 53-63.

[ESS85] P. Erdős, A. Sárközy and V.T. Sós, Problems and results on additive properties of general sequences. IV, *Number Theory (Ootacamund, 1984)*, Lecture Notes in Mathematics 1122. (Springer-Verlag, Berlin, 1985), 85-104.

[ESS86] P. Erdős, Sárközy and V.T. Sós, Problems and results on additive properties of general sequences. V, *Monatsh. Math.* **102** (1986), 183-197.

[FM96] E. Fouvry and M. Ram Murty, On the distribution of supersingular primes, Canad. J. Math. **48** (1996), 81-104.

[Ing27] A. E. Ingham, Some asymptotic formulae in the theory of numbers, J. London Math. Soc., **S1-2**, no. 3 (1927), 202-208.

[IK04] H. Iwaniec and E. Kowalski, Analytic number theory, colloquium publications, vol. 53, American Mathematical Society.

[Kat69] I. Katai, On the distribution of arithmetical functions. Acta Math. Acad. Sci. Hungar. **20**, 1969, 69-87.

[Kou14] D. Koukoulopoulos, Prime numbers in short arithmetic progressions. arXiv:1405.6592 [math.NT].

[Kow06] E. Kowalski, Analytic problems for elliptic curves, J. Ramanujan Math. Soc. **21** (2006), 19-114.

[Luc79] L. Lucht, Mittelwerte multiplikativer Funktionen auf Linearformen. Arch. Math. (Basel) 32 (1979), no. 4, 349-355.

[LPZ10] A. Languasco, A. Perelli, and A. Zaccagnini, On the MontgomeryHooley Theorem in short intervals, Mathematika **56** (2010), 231-243.

[Mir49] L. Mirsky, Summation formulae involving arithmetic functions, Duke Math. J. **16**, (1949), 261-272.

[MPS14] G. Martin, P. Pollack and E. Smith, Averages of the number of points on elliptic curves. Algebra Number Theory **8** (2014), no. 4, 813-836.

[Rom84] S. Roman, The Umbral Calculus. New York: Academic Press, pp. 59-63, 1984.

[Sar06] A. Sárközy, On the Number of Additive Representations of Integers, *Bolyai Society Mathematical Studies,* **15** (2006), 329-339.

[Ste97a] G. Stepanauskas, The mean values of multiplicative functions. II, Lithuanian Math. J. **37** (1997), 162-170.

[Ste97b] G. Stepanauskas, The Mean Values of Multiplicative Functions on Shifted Primes, Lithuanian Math. J. **37** (1997), 443-451.

[Ste01] G. Stepanauskas, The mean values of multiplicative functions. V. Analytic and probabilistic methods in number theory (Palanga, 2001), 272-281, TEV, Vilnius, 2002.

[Sch76] W. M. Schimidt, Equations over finite fields. An elementary approach, Lecture notes in Math. **536**, Springer Verlag, 1976.

[SS07] J. Šiaulys and G. Stepanauskas, On the Mean Value of the Product of Multiplicative Functions with Shifted Argument, Monatsh. Math. **150**, (2007), 343-351 .

[TC05] M. Tang and Y.G. Chen, On Additive Properties of General Sequences, *Bull. Austral. Math. Soc.* **71** (2005), 479-485.

[TC09] M. Tang and Y.G. Chen, On the monotonicity properties of additive representation functions. II, *Discrete Math.* **309** (2009), 1368-1373.