On the Theory of Integer Sequences

A Dissertation

presented to

the Faculty of the Graduate School

at the University of Missouri-Columbia

In Partial Fulfillment

of the Requirements for the Degree

Doctors of Philosophy

---

by

C. Wesley Nevans

Dr. William Banks, Dissertation Supervisor

December 2010

The undersigned, appointed by the dean of the Graduate School, have examined the dissertation entitled

On the Theory of Integer Sequences

presented by Wesley Nevans, a candidate for the degree of doctor of philosophy, and hereby certify that, in their opinion, it is worthy of acceptance.

Professor William Banks

Professor Steven Hofman

Professor Konstantin Makeover

Professor Stephen Montgomery-Smith

Professor Youssef Saab

I would most importantly like to thank my advisor Dr. William Banks for all of his help and understanding over the years.

Many thanks to all those gentlemen whom I coauthored papers, William Banks, Ahmet Güloğlu, Derrick Hart, Pieter Moree, Carl Pomerance and Fillip Saidak.

Contents

Abstract

We explore certain sequences of integers which appear in the number theory. We start by exploring properties of Beatty sequences. We concentrate on looking at the sum of primes from a Beatty sequence and properties of certain multiplicative functions on a Beatty sequence. We move on to the Robin and Nicolas inequalities and consider sequences with certain properties which must satisfy these. Next is we explore certain sequences of composite integers which are similar to those of the primes, mainly Carmichael, Guiga, and Lucas numbers. Finally we discuss Descartes numbers, and determine all such numbers with certain other properties.

Part 1

Introduction

Number theory is the study of the integers and those problems which may be stated in terms of them. Being problem based, this distinguishes number theory from other areas of mathematics such as algebra and analysis. Moreover, number theory is one of the oldest subjects in mathematics since the positive integers arise in a "natural" way. In what follows we will be considering several different sequences and (possibly empty) sets of integers.

This work described in this dissertation is the amalgamation of several different published on which the author has worked in collaboration on by the author with William Banks, Ahmet Güloğlu, Derrick Hart, Pieter Moree, Carl Pomerance and Fillip Saidak.

To start, we define some fairly ubiquitous concepts and notations from number theory that are used in this dissertation. The variables p, n and x are always used to denote a prime, a positive integer and a real number, respectively, unless otherwise noted. The notation $p^\alpha \| n$ means $p^\alpha | n$ but $p^{\alpha+1} \nmid n$. We denote the set of positive (rational) primes by $\mathbb{P} = \{2, 3, 5, 7, 11 \ldots\}$. Related to $\mathbb{P}$ is the *prime counting function*, $\pi(x) = \#|\mathbb{P} \cap [1, x]\,|$. Next is the *Euler φ function* which is defined on the positive integers by

$$\varphi(n) = \prod_{p^\alpha \| n} p^{\alpha-1}(p-1) = n \prod_{p|n} (1 - p^{-1}).$$

The number $\varphi(n)$ is the cardinality of the group $(\mathbb{Z}/n\mathbb{Z})^*$ and is also the number of Dirichlet characters to the modulus n. The *sum of divisors function σ* is defined on the positive integers by

$$\sigma(n) = \sum_{d|n} d = \prod_{p^\alpha \| n} \frac{p^{\alpha+1} - 1}{p - 1},$$

the product form being first introduced by Réne Descartes in 1638. The *Möbius μ function* defined by

$$\mu(n) = \begin{cases} 0 & \text{if } p^2 | n \text{ for some p} \\ (-1)^m & n \text{ is square free and has exactly } m \text{ prime divisors.} \end{cases}$$

We denote by $\lfloor x \rfloor$, $\lceil x \rceil$ and $\{x\}$ the greatest integer $\leqslant x$, the least integer $\geqslant x$, and the fractional part of x, respectively. The *Euler-Mascheroni constant* is defined to be

$$\gamma = \lim_{n\to\infty} \left(\sum_{m=1}^{n} \frac{1}{m} - \log n \right) = 0.5772156649 \cdots .$$

We also put $\mathbf{e}(x) = e^{2\pi i x}$. The *Riemann ζ function* is the analytic continuation of

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1} \qquad (\Re(s) > 1)$$

to $\mathbb{C} \setminus \{1\}$. The *Riemann Hypothesis* (RH) is the conjecture that for all $s \in \mathbb{C}$ such that $\Re(s) > 0$ and $\zeta(s) = 0$, $\Re(s) = \frac{1}{2}$. We recall that for functions $F(x)$ and $G(x) > 0$ the notations $F(x) \ll G(x)$, $G(x) \gg F(x)$ and $F(x) = O(G(x))$ are all equivalent to the statement that the inequality $|F(x)| \leqslant cG(x)$ holds for some constant $c > 0$ and all x sufficiently large possibly dependent on other stated parameters. The notation $F(x) \asymp G(x)$ means both $F(x) \ll G(x)$ and $G(x) \ll F(x)$. If we write $F(x) = o(G(x))$ we mean $F(x)/G(x) \to 0$ as $x \to \infty$.

The first two chapters start off by exploring properties of *(non-homogenous) Beatty sequences*

$$\mathcal{B}_{\alpha,\beta} = \{n \in \mathbb{N} \ : \ n = \lfloor \alpha m + \beta \rfloor \text{ for some } m \in \mathbb{Z}\}.$$

where $\alpha, \beta \in \mathbb{R}$. Such sequences are shown to have certain properties that similar to those enjoyed by the sequence of all natural numbers.

Chapter 2 concerns integers N that can expressed as the sum of a fixed number κ of primes from a fixed Beatty sequence $\mathcal{B}_{\alpha,\beta}$, the main result being Theorem 2.1. This problem was inspired by the famous conjecture of Goldbach and by the well known theorems of I. M. Vinogradov. Our results were limited by a few factors, the first being that α^{-1} is required to be of *finite type* (see Subchapter 2.2.2). The second limitation the density of $\mathcal{B}_{\alpha,\beta}$ when α is large. The third limitation is minor and arises from the nature of primes: $N \equiv \kappa \pmod 2$. This is due purely to a parity argument and would be required for any sequence of odd numbers. It is important to note, however, that when these conditions are met, our methods yields results comparable to what is known in the classical theory.

In Chapter 3 we once again are looking at Beatty sequences, but this time we are summing the values of a multiplicative function over the positive elements of a Beatty sequence. The original goal was to determine how many of the elements $n \leqslant N$ in a Beatty sequence $\mathcal{B}_{\alpha,\beta}$ can be expressed as the sum of two squares. This was accomplished in Corollary 3.2. From this study Theorem 3.1 naturally grew. Similar to Chapter 2, the result requires only a multiplication of α^{-1} to the main term. The α^{-1} comes from the number of positive integers in a Beatty sequence less than N approaches asymptoticly $\alpha^{-1}N$. It is easy to check well known results and see the hypothesis of Theorem 3.1 hold for several different multiplicative functions, including the characteristic function for numbers which may be expressed as a sum of squares.

Next comes some of the most interesting material, as it relates to the Riemann Hypothesis. Nicolas [43] proved that the inequality

$$\frac{n}{\varphi(n)} > e^{\gamma} \log\log n$$

holds for infinitely many natural numbers n. Moreover, if N_k denotes the product of the first k primes, he proved the last inequality holds for every $k \geqslant 1$ on the RH. Assuming RH is false, he also showed there are both infinitely many k for which this inequality holds and infinitely many k for which it does not hold. We denote by $\mathcal{N}$ the set of numbers $n \in \mathbb{N}$ that satisfy the *Nicolas inequality*:

$$\frac{n}{\varphi(n)} < e^{\gamma} \log\log n.$$

Later Robin [51] showed that if RH is true, then *Robin's inequality*:

$$\frac{\sigma(n)}{n} < e^{\gamma} \log\log n$$

holds for every integer $n > 5040$, whereas if RH is false, then this inequality fails for infinitely many n. We denote by $\mathcal{R}$ the set of numbers $n \in \mathbb{N}$ that satisfy the *Robin inequality*. The Nicolas and Robin inequalities are related by the inequality

$$\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} \qquad (n > 1)$$

and hence we have $\mathcal{N} \subset \mathcal{R}$.

Chapter 4 investigates certain subset of integers, defined by properties of their prime divisors, and we show that all but finitely many must satisfy both the Nicolas and Robin inequalities. The original question was once again related to those number which can be expressed as a sum of two squares. Many generalizations followed the original conjecture. To be specific, we partition $\mathbb{P}$ into two sets $\mathcal{P}$ and $\mathcal{Q}$ so that

$$0 < \overline{\lim} \frac{|\{p \in \mathcal{P} : p \leqslant x\}|}{\pi(x)} < 1 \qquad \text{and} \qquad 0 < \underline{\lim} \frac{|\{p \in \mathcal{P} : p \leqslant x\}|}{\pi(x)} < 1.$$

Obviously these inequalities must then hold when $\mathcal{P}$ is replaced by $\mathcal{Q}$. If we then define $\mathcal{S} = \mathcal{S}(\mathcal{P})$ by

$$\mathcal{S} = \left\{ n \in \mathbb{N} \ : \ \text{if } p \in \mathcal{Q} \text{ and } p \mid n, \text{ then } p^2 \mid n \right\}$$

then all but finitely many elements of $\mathcal{S}$ are in $\mathcal{N}$ as stated in Theorem 4.1. The structure of those integers which can be expressed as the sum of two squares allows one to apply this theorem. Moreover, using effective bounds for the prime number

theorem for arithmetic sequences from [50], we were able to state there are exactly 246 such integers which do not satisfy the Nicolas inequality and fifteen such integers which do not satisfy the Robin inequality.

In Chapter 5, building upon the work of Nicolas, we derive an equivalent statement to the Riemann Hypothesis involving both the number of primitive Dirichlet characters for a modulus n and the twin prime constant. Our inspiration for studying the question was that the formula for the cardinality of $\mathcal{X}_n'$, the set of primitive Dirichlet characters modulo n, is given by

$$|\mathcal{X}_n'| = n \prod_{p \parallel n} \left(1 - \frac{2}{p}\right) \prod_{p^2 \mid n} \left(1 - \frac{1}{p}\right)^2 = \frac{\varphi(n)^2}{n} \prod_{p \parallel n} \frac{p(p-2)}{(p-1)^2},$$

and is therefore closely related to the formula for $\varphi(n)$.We follow the method of Nicolas [43] to prove Theorem 5.1. When considering extreme cases, namely integers of the form $2n_k = 2 * 2 * 3 * 5 * 7 * \cdots * p_k$, as $k \to \infty$ we have

$$\prod_{p \parallel 2n_k} \frac{p(p-2)}{(p-1)^2} \to C_2 = \prod_{p>2} \frac{p(p-2)}{(p-1)^2} = 0.6601618158\cdots$$

the twin prime constant and

$$\frac{\varphi(2n_k)^2}{2n_k} \to e^{-\gamma} \frac{\varphi(2n_k)}{\log\log(2n_k)}.$$

This is the first time an equivalent statement to RH has been phrased in terms of the number of primitive Dirichlet characters.

The question as to whether there are any composite numbers n for which $\varphi(n) \mid n-1$ was first posed by D. H. Lehmer [38] in 1932, and the answer. The conjecture that there are no such composite integers is known as *Lehmer's conjecture*. For any prime p we trivially have $\varphi(p) = p - 1 \mid p - 1$. Thus Lehmer's conjecture, if true provides a new characterization of prime numbers. To this end, we define $\mathcal{L}(x)$ to be the set of counterexamples to Lehmer's conjecture less than or equal to x. Chapter 6 is dedicated to finding a better upper bound for $\#\mathcal{L}(x)$ than had previously been demonstrated. Before this work, many bounds for $\mathcal{L}(x)$ had been given, but none could show $\#\mathcal{L}(x) \ll x^{1/2}$. This caused some concern, since the best known upper bound could not show the number of counterexamples to Lehmer's conjecture less than x were less prevalent than the number of squares. Theorem 6.1 goes beyond showing $\#\mathcal{L}(x) \ll x^{1/2}$ to $\#\mathcal{L}(x) = o(x^{1/2})$.

Chapter 7 studies three sets of composite integers. The interest in these will come from a desire to characterize primes by *Fermat's little theorem*, which asserts that the system of congruences

$$a^p \equiv a \pmod{p} \qquad \text{for all } a \in \mathbb{Z}$$

holds for all primes p. The first set we consider the set of *Carmichael numbers*, denoted by $\mathcal{C}$; these are composite integers n such that

$$a^n \equiv a \pmod{n} \qquad \text{for all } a \in \mathbb{Z}.$$

As a consequence of Fermat's little theorem we have

$$p \mid 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} + 1$$

for any prime p. The second set we consider is the set of *Giuga numbers*, denoted by $\mathcal{G}$, which are composite integers n for which

$$n \mid 1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} + 1.$$

The third set is the (presumably empty) $\mathcal{L}$ of counterexamples to Lehmer's conjecture, i.e. composite integers n for which $\varphi(n) \mid n-1$.

It has been shown $n \in \mathcal{C}$ if and only if

$$p(p-1) \mid n-p \qquad \text{for every prime } p \text{ dividing } n,$$

which is a variation of *Korselt's criterion*. Similarly it has been shown $n \in \mathcal{G}$ if and only if

$$p^2(p-1) \mid n-p \qquad \text{for every prime } p \text{ dividing } n.$$

Note that $\mathcal{G} \subset \mathcal{C}$. It is well known (see [1]) that there are infinitely many elements in $\mathcal{C}$, and it has been conjectured

$$|\mathcal{C} \cap [1, X]\,| = X^{1+o(1)}.$$

On the other hand it has been conjectured $|\mathcal{G}| = 0$, and upper bounds for $|\mathcal{G} \cap [1, X]\,|$ have been given. We explore

$$\#|\mathcal{C} \setminus \mathcal{G} \cap [1, X]\,|$$

and give a lower bound for this quantity. Similarly we find a lower bound for

$$\#|\mathcal{C} \setminus \mathcal{L} \cap [1, X]\,|.$$

We do this by constructing elements of $\mathcal{C}$ which can not be in $\mathcal{G}$ and $\mathcal{L}$, respectively.

Finally, Chapter 8 we consider a particular integer $\mathfrak{D} = 198585576189$, and show that it has a unique property. *Perfect numbers*, are integers n such that $\sigma(n) = 2n$, and have been studied since Euclid. Euler was able to classify all even perfect numbers as having the form $n = (2^p - 1)2^{p-1}$, where $2^p - 1$ is prime. On the other hand, there are no known examples of odd perfect numbers. Descartes noted that

$$\mathfrak{D} = 3^2\, 7^2\, 11^2\, 13^2\, 22021 = 198585576189$$

and if 22021 were prime then $\mathfrak{D}$ would be an example of an odd perfect number (however, $22021 = 19^2\,61$). We call n a *Descartes number* if n is *odd*, and if $n = km$ for two integers $k, m > 1$ such that

$$\sigma(k)(m+1) = 2n.$$

We show in Theorem 8.2 that $\mathfrak{D}$ is the only cube-free Descartes number with 7 or fewer distinct prime factors. We also show that if n is a cube-free Descartes number which is not divisible by 3, then n has more than one million distinct prime divisors.

Part 2

Primes from a Beatty sequence

2.1 Introduction

The celebrated 1937 theorem of Vinogradov states that every sufficiently large odd number is the sum of three prime numbers. However, the statement is no longer true if all three primes are required to lie in the Beatty sequence $\mathcal{B}_{\alpha,0} = \{\lfloor \alpha m \rfloor \ : \ m \in \mathbb{N}\}$ for a fixed irrational number $\alpha > 3$. Indeed, if N is odd and

$$N = \lfloor \alpha m_1 \rfloor + \lfloor \alpha m_2 \rfloor + \lfloor \alpha m_3 \rfloor \tag{1}$$

for some $m_1, m_2, m_3 \in \mathbb{N}$, it is easy to see that

$$N\alpha^{-1} \leqslant m_1 + m_2 + m_3 < N\alpha^{-1} + 3\alpha^{-1}.$$

Hence, the relation (1) cannot hold if the fractional part $\{N\alpha^{-1}\}$ of $N\alpha^{-1}$ lies in the open interval $(0, 1 - 3\alpha^{-1})$, which happens for about $\frac{1}{2}(1 - 3\alpha^{-1})X$ positive odd integers $N \leqslant X$. On the other hand, for an irrational number α of *finite type* (see Section 2.2.2) in the range $1 < \alpha < 3$, we show that every sufficiently large odd number is the sum of three prime numbers, each of which lies in the Beatty sequence $\mathcal{B}_\alpha$.

We prove the following:

Theorem 2.1. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. Then,*

(*i*) *Almost all even numbers N can be expressed as the sum of two primes from the Beatty sequence $\mathcal{B}_{\alpha,\beta}$ if and only if $\alpha < 2$.*

(*ii*) *For any integer $\kappa \geqslant 3$, every sufficiently large number $N \equiv \kappa \pmod 2$ can be expressed as the sum of κ primes from the Beatty sequence $\mathcal{B}_{\alpha,\beta}$ if and only if $\alpha < \kappa$.*

To state our results more explicitly, we define for every integer $\kappa \geqslant 2$ the function

$$\mathcal{G}_\kappa(N) = \mathcal{G}_\kappa(\alpha, \beta; N) = \sum_{\substack{n_1+\cdots+n_\kappa = N \\ n_1,\ldots,n_\kappa \in \mathcal{B}_{\alpha,\beta}}} \Lambda(n_1)\cdots\Lambda(n_\kappa) \qquad (N \geqslant 1),$$

where Λ is the *von Mangoldt function*:

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a positive power of the prime } p; \\ 0 & \text{otherwise.} \end{cases}$$

By partial summation, our estimates for $\mathcal{G}_\kappa(N)$ lead to estimates for the number of representations of an integer $N \equiv \kappa \pmod 2$ as the sum of κ primes from the Beatty sequence $\mathcal{B}_{\alpha,\beta}$.

Let $\psi = \psi_\alpha$ be the periodic function with period one which is defined on the interval $(0, 1]$ as follows:

$$\psi(x) = \begin{cases} 1 & \text{if } 0 < x \leqslant \alpha^{-1}; \\ 0 & \text{if } \alpha^{-1} < x \leqslant 1. \end{cases} \tag{2}$$

The function ψ is closely related to the characteristic function of the set $\mathcal{B}_{\alpha,\beta}$. Let $\psi^{(1)} = \psi$, and for every $\kappa \geqslant 2$, let $\psi^{(\kappa)}$ denote the κ-fold convolution of ψ with itself, defined inductively by

$$\psi^{(\kappa)}(x) = \int_0^1 \psi^{(\kappa-1)}(x-y)\psi(y)\,dy \qquad (\kappa \geqslant 2).$$

Finally, for every $\kappa \geqslant 2$ we define the *singular series*

$$\mathfrak{S}_\kappa(N) = \prod_{p \,|\, N} \left(1 + \frac{(-1)^\kappa}{(p-1)^{\kappa-1}}\right) \prod_{p \nmid N} \left(1 + \frac{(-1)^{\kappa+1}}{(p-1)^\kappa}\right) \qquad (N \geqslant 1).$$

The numbers $\mathfrak{S}_\kappa(N)$ arise naturally in estimates for the number of representations of an integer as a sum of κ prime numbers. Note that $\mathfrak{S}_\kappa(N) = 0$ if and only if $N \not\equiv \kappa \pmod 2$.

Theorem 2.2. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. Then, for any constant $C > 0$, the estimate*

$$\mathcal{G}_2(N) = \psi^{(2)}(\eta N + 2\delta)\mathfrak{S}_2(N)N + O\left(\frac{N}{(\log N)^C}\right)$$

holds for all but $O\big(X(\log X)^{-C}\big)$ integers $N \leqslant X$, where $\eta = \alpha^{-1}$, $\delta = \alpha^{-1}(1-\beta)$, and the implied constants depend only on α and C.

Theorem 2.3. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. Then, for every integer $\kappa \geqslant 3$ and any constant $C > 0$, the estimate*

$$\mathcal{G}_\kappa(N) = \psi^{(\kappa)}(\eta N + \kappa\delta)\mathfrak{S}_\kappa(N)\frac{N^{\kappa-1}}{(\kappa-1)!} + O\left(\frac{N^{\kappa-1}}{(\log N)^C}\right)$$

holds, where $\eta = \alpha^{-1}$, $\delta = \alpha^{-1}(1-\beta)$, and the implied constant depends only on α, κ and C.

The proof of Theorem 2.2 is given in Section 2.3 (see the remark after the statement of Theorem 2.8) and that of Theorem 2.3 is given in Section 2.4 (see the remark after the statement of Proposition 2.11). In Section 2.5 we study properties of the convolutions $\psi^{(\kappa)}$ ($\kappa \geqslant 2$) and, in particular, derive a sharp lower bound for values of $\psi^{(\kappa)}$ in the special case that $\kappa = \lceil \alpha \rceil$. Our proof of Theorem 2.1, which is given in Section 2.6, follows immediately from the results of Section 2.5.

Our arguments have been strongly influenced by the treatment of the Goldbach problem that is given in the book [30] of Iwaniec and Kowalski, and we adopt a similar notation here. Our underlying approach relies heavily on ideas from a recent paper of Banks and Shparlinski [12] on primes in a Beatty sequence.

2.2 Preliminaries

2.2.1 Notation

The notation $[\![x]\!]$ is used to denote the distance from the real number x to the nearest integer; that is,

$$[\![x]\!] = \min_{n \in \mathbb{Z}} |x - n| \qquad (x \in \mathbb{R}).$$

Throughout the part, the implied constants in symbols O, $\ll$ and $\gg$ may depend (where obvious) on the parameters α, κ, C but are absolute otherwise.

2.2.2 Discrepancy of fractional parts

Recall that the *discrepancy* $D(M)$ of a sequence of (not necessarily distinct) real numbers $a_1, a_2, \ldots, a_M \in [0,1)$ is defined by

$$D(M) = \sup_{\mathcal{I} \subseteq [0,1)} \left| \frac{V(\mathcal{I}, M)}{M} - |\mathcal{I}| \right|, \tag{3}$$

where the supremum is taken over all subintervals $\mathcal{I} = (c,d)$ of the interval $[0,1)$, $V(\mathcal{I}, M)$ is the number of positive integers $m \leqslant M$ such that $a_m \in \mathcal{I}$, and $|\mathcal{I}| = d - c$ is the length of $\mathcal{I}$.

For any irrational number η we define its *type* τ by the relation

$$\tau = \sup\Big\{ t \in \mathbb{R} \ : \ \varliminf_{n \to \infty} \ n^t \, [\![\eta n]\!] = 0 \Big\}.$$

Using *Dirichlet's approximation theorem*, it is easily seen that $\tau \geqslant 1$ for every irrational number η. The well known theorems of Khinchin [31] and of Roth [53, 54] assert that $\tau = 1$ for *almost all* real numbers (in the sense of the Lebesgue measure) and *all* irrational algebraic numbers η, respectively; see also [13, 55].

For every irrational number η, it is known that the sequence of fractional parts $\{\eta\}, \{2\eta\}, \{3\eta\}, \ldots$, is *uniformly distributed modulo* 1 (for instance, see [33, Example 2.1, Chapter 1]). When η is of finite type, this statement can be made more precise. Let $D_{\eta,\delta}(M)$ denote the discrepancy of the sequence of fractional parts $(\{\eta m+\delta\})_{m=1}^{M}$. By [33, Theorem 3.2, Chapter 2] we have:

Lemma 2.4. *Let η be a fixed irrational number of finite type $\tau < \infty$. Then, for all $\delta \in \mathbb{R}$ the following bound holds:*

$$D_{\eta,\delta}(M) \leqslant M^{-1/\tau+o(1)} \qquad (M \to \infty),$$

where the function implied by $o(\cdot)$ depends only on η.

2.2.3 Numbers in a Beatty sequence

The following elementary result characterizes the set of numbers that occur in the Beatty sequence $\mathcal{B}_{\alpha,\beta}$:

Lemma 2.5. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and put $\eta = \alpha^{-1}$, $\delta = \alpha^{-1}(1-\beta)$. Then, $n = \lfloor \alpha m + \beta \rfloor$ for some integer m if and only if $0 < \{\eta n + \delta\} \leqslant \eta$.*

2.2.4 Estimates with the von Mangoldt function

The following estimate follows immediately from the *Siegel–Walfisz theorem* (see, for example, the book [29] by Huxley) using partial summation:

Lemma 2.6. *Let $\kappa \geqslant 1$ be fixed. For any fixed constant $A > 0$ and uniformly for integers $N \geqslant 3$ and $0 \leqslant c < d \leqslant (\log N)^A$ with $\gcd(c,d) = 1$, the estimate*

$$\sum_{\substack{n \leqslant N \\ n \equiv c \pmod d}} \Lambda(n)(N-n)^{\kappa-1} = \frac{N^\kappa}{\kappa\,\varphi(d)} + O\left(N^\kappa \exp\left(-B(\log N)^{1/2}\right)\right)$$

holds, where $B > 0$ is a constant that depends only on κ and A.

We also need the following:

Lemma 2.7. *Let $\kappa \geqslant 1$ be fixed. For an arbitrary real number θ and coprime integers c, d with $0 \leqslant c < d$, if $|\theta - a/b| \leqslant 1/N$ and $\gcd(a,b) = 1$, then*

$$\sum_{\substack{n \leqslant N \\ n \equiv c \pmod d}} \Lambda(n)\mathbf{e}(\theta n)(N-n)^{\kappa-1} \ll \left(b^{-1/2}N^\kappa + b^{1/2}N^{\kappa-1/2} + N^{\kappa-1/5}\right)(\log N)^3,$$

where the implied constant depends only on κ.

Proof. The special case $\kappa = 1$ is a simplified and weakened version of a theorem of Balog and Perelli [4] (see also [37]), and the general case follows by partial summation.

□

2.2.5 The singular series

For every integer $\kappa \geqslant 2$, it is easy to check that the singular series

$$\mathfrak{S}_\kappa(N) = \prod_{p \,|\, N} \left(1 + \frac{(-1)^\kappa}{(p-1)^{\kappa-1}}\right) \prod_{p \nmid N} \left(1 + \frac{(-1)^{\kappa+1}}{(p-1)^\kappa}\right)$$

satisfies the identity

$$\mathfrak{S}_\kappa(N) = \sum_{d \,|\, N} \sum_{\substack{c \geqslant 1 \\ \gcd(c,d)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa \varphi(d)^\kappa}, \tag{4}$$

and for every $\kappa \geqslant 3$ we also have

$$\mathfrak{S}_\kappa(N) = \sum_{\substack{c,d \geqslant 1 \\ \gcd(d,cN)=1}} \frac{\mu(c)^\kappa \mu(d)^{\kappa+1} d}{\varphi(c)^{\kappa-1}\varphi(d)^\kappa}. \tag{5}$$

We also have the bound

$$\mathfrak{S}_2(N) \ll \log\log N, \tag{6}$$

and for every $\kappa \geqslant 3$,

$$\mathfrak{S}_\kappa(N) \ll 1. \tag{7}$$

2.3 Two Beatty primes

Fix $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. In this section, we focus our attention on the function

$$\mathcal{G}_2(N) = \sum_{\substack{n_1+n_2=N \\ n_1,n_2 \in \mathcal{B}_{\alpha,\beta}}} \Lambda(n_1)\Lambda(n_2) \qquad (N \geqslant 1).$$

Put $\eta = \alpha^{-1}$ and $\delta = \alpha^{-1}(1-\beta)$, and let τ denote the (finite) type of η. We recall that ψ is the periodic function with period one which is defined by (2) on the interval $(0, 1]$, and $\psi^{(2)} = \psi * \psi$ is the convolution of ψ with itself.

Theorem 2.8. *For any complex numbers c_N and any constant $C > 0$, we have*

$$\sum_{N \leqslant X} c_N \mathcal{G}_2(N) = \sum_{N \leqslant X} c_N \psi^{(2)}(\eta N + 2\delta)\mathfrak{S}_2(N)N + O\left(\|c\|_2 \frac{X^{3/2}}{(\log X)^C}\right),$$

where $\|c\|_2 = \left(\sum_{N \leqslant X} |c_N|^2\right)^{1/2}$.

Remark. This result immediately yields a proof of Theorem 2.2. Indeed, taking $c_N = \mathcal{G}_2(N) - \psi^{(2)}(\eta N + 2\delta)\mathfrak{S}_2(N)N$, we derive the bound

$$\sum_{N \leqslant X} \big(\mathcal{G}_2(N) - \psi^{(2)}(\eta N + 2\delta)\mathfrak{S}_2(N)N\big)^2 \ll \frac{X^3}{(\log X)^{2C}},$$

and Theorem 2.2 follows at once.

Proof of Theorem 2.8. By Lemma 2.5 and the definition (2), it follows that

$$\mathcal{G}_2(N) = \sum_{n_1+n_2=N} \Lambda(n_1)\Lambda(n_2)\psi(\eta n_1 + \delta)\psi(\eta n_2 + \delta). \tag{8}$$

According to a classical result of Vinogradov (see [61, Chapter I, Lemma 12]), for any Δ such that

$$0 < \Delta < \frac{1}{8} \qquad \text{and} \qquad \Delta \leqslant \frac{1}{2}\min\{\eta, 1-\eta\}$$

there is a real-valued function Ψ with the following properties:

(*i*) Ψ is periodic with period one;

(*ii*) $0 \leqslant \Psi(x) \leqslant 1$ for all $x \in \mathbb{R}$;

(*iii*) $\Psi(x) = \psi(x)$ if $\Delta \leqslant \{x\} \leqslant \eta - \Delta$ or if $\eta + \Delta \leqslant \{x\} \leqslant 1 - \Delta$;

(*iv*) Ψ can be represented as a Fourier series:

$$\Psi(x) = \sum_{k\in\mathbb{Z}} g(k)\mathbf{e}(kx),$$

where $g(0) = \eta$, and the Fourier coefficients satisfy the uniform bound

$$|g(k)| \ll \min\big\{|k|^{-1}, |k|^{-2}\Delta^{-1}\big\} \qquad (k \neq 0). \tag{9}$$

From the properties (*i*)–(*iii*) above, it follows that the estimate

$$\Psi^{(2)}(x) = \psi^{(2)}(x) + O(\Delta) \tag{10}$$

holds uniformly for all $x \in \mathbb{R}$, where $\Psi^{(2)}$ is the convolution $\Psi * \Psi$.

From (8) we see that

$$\begin{aligned}\mathcal{G}_2(N) = \sum_{n_1+n_2=N} &\Lambda(n_1)\Lambda(n_2)\Psi(\eta n_1 + \delta)\Psi(\eta n_2 + \delta) \\ &+ O\big(V(\mathcal{I}, N)(\log N)^2\big),\end{aligned} \tag{11}$$

where $V(\mathcal{I}, N)$ is the number of positive integers $n \leqslant N$ such that

$$\{\eta n + \delta\} \in \mathcal{I} = [0, \Delta) \cup (\eta - \Delta, \eta + \Delta) \cup (1 - \Delta, 1).$$

Since $|\mathcal{I}| = 4\Delta$, it follows from the definition (3) and Lemma 2.4 that

$$V(\mathcal{I}, N) \ll \Delta N + N^{1-1/(2\tau)}. \tag{12}$$

Now let $K \geqslant \Delta^{-1}$ be a large real number (to be specified later), and let Ψ_K be the trigonometric polynomial given by

$$\Psi_K(x) = \sum_{|k| \leqslant K} g(k)\mathbf{e}(kx). \tag{13}$$

Using (9), we see that the estimate

$$\Psi_K(x) = \Psi(x) + O(K^{-1}\Delta^{-1}) \tag{14}$$

holds uniformly for all $x \in \mathbb{R}$, and therefore

$$\Psi_K^{(2)}(x) = \Psi^{(2)}(x) + O(K^{-1}\Delta^{-1}) = \psi^{(2)}(x) + O(\Delta + K^{-1}\Delta^{-1}), \tag{15}$$

where we have used (10) in the second step. From the definition (13) we also have

$$\Psi_K^{(2)}(x) = \sum_{|k| \leqslant K} g(k)^2\mathbf{e}(kx). \tag{16}$$

Inserting the estimate (14) into (11) and taking into account (12), we derive that

$$\begin{aligned}\mathcal{G}_2(N) = \sum_{n_1+n_2=N} \Lambda(n_1)\Lambda(n_2)\Psi_K(\eta n_1 + \delta)\Psi_K(\eta n_2 + \delta)\\ + O\big(\big(\Delta + K^{-1}\Delta^{-1} + N^{-1/(2\tau)}\big)N(\log N)^2\big).\end{aligned}$$

For a given real number $Z \geqslant 2$, we now split $\Lambda(n)$ as follows:

$$\Lambda(n) = -\sum_{d\,|\,n} \mu(d)\log d = \Lambda^\sharp(n) + \Lambda^\flat(n),$$

where

$$\Lambda^\sharp(n) = -\sum_{\substack{d\,|\,n\\ d\leqslant Z}} \mu(d)\log d \qquad \text{and} \qquad \Lambda^\flat(n) = -\sum_{\substack{d\,|\,n\\ d> Z}} \mu(d)\log d.$$

Then,

$$\begin{aligned}\mathcal{G}_2(N) = \mathcal{G}_2^{\sharp\sharp}(N) + 2\mathcal{G}_2^{\sharp\flat}(N) + \mathcal{G}_2^{\flat\flat}(N)\\ + O\big(\big(\Delta + K^{-1}\Delta^{-1} + N^{-1/(2\tau)}\big)N(\log N)^2\big),\end{aligned} \tag{17}$$

where

$$\mathcal{G}_2^{\sharp\sharp}(N) = \sum_{n_1+n_2=N} \Lambda^\sharp(n_1)\Lambda^\sharp(n_2)\Psi_K(\eta n_1+\delta)\Psi_K(\eta n_2+\delta),$$
$$\mathcal{G}_2^{\sharp\flat}(N) = \sum_{n_1+n_2=N} \Lambda^\sharp(n_1)\Lambda^\flat(n_2)\Psi_K(\eta n_1+\delta)\Psi_K(\eta n_2+\delta),$$
$$\mathcal{G}_2^{\flat\flat}(N) = \sum_{n_1+n_2=N} \Lambda^\flat(n_1)\Lambda^\flat(n_2)\Psi_K(\eta n_1+\delta)\Psi_K(\eta n_2+\delta).$$

From now on, let X be a large integer, and put

$$\Delta = X^{-1/(8\tau)} \qquad \text{and} \qquad K = X^{1/(4\tau)}. \tag{18}$$

Then, for all $N \leqslant X$ the estimate (17) implies

$$\mathcal{G}_2(N) = \mathcal{G}_2^{\sharp\sharp}(N) + 2\mathcal{G}_2^{\sharp\flat}(N) + \mathcal{G}_2^{\flat\flat}(N) + O\big(X^{1-1/(10\tau)}\big).$$

Therefore, for any complex numbers c_N, it follows that

$$\sum_{N\leqslant X} c_N\mathcal{G}_2(N) = \sum_{N\leqslant X} c_N\big(\mathcal{G}_2^{\sharp\sharp}(N) + 2\mathcal{G}_2^{\sharp\flat}(N) + \mathcal{G}_2^{\flat\flat}(N)\big) + O\big(\|c\|_2\, X^{3/2-1/(10\tau)}\big). \tag{19}$$

Next, we need the following result, the proof of which is given below:

Lemma 2.9. *For any complex numbers u_ℓ and v_m, the bound*

$$\sum_{\ell+m+n=X} u_\ell\, v_m\, \Lambda^\flat(n)\Psi_K(\eta n+\delta) \ll \|u\|_2\, \|v\|_2\, \frac{X(\log X)^2}{(\log Z)^A}$$

holds with any $A > 0$, where $\|u\|_2 = \big(\sum_{\ell\leqslant X} |u_\ell|^2\big)^{1/2}$, $\|v\|_2 = \big(\sum_{m\leqslant X} |v_m|^2\big)^{1/2}$, and the implied constant depends only on α and A.

For any complex numbers c_N, we have

$$\sum_{N\leqslant X} c_N\mathcal{G}_2^{\sharp\flat}(N) = \sum_{\ell+m+n=X} c_{X-\ell}\,\Lambda^\sharp(m)\Psi_K(\eta m+\delta)\cdot\Lambda^\flat(n)\Psi_K(\eta n+\delta).$$

We now apply Lemma 2.9 with

$$u_\ell = \begin{cases} c_{X-\ell} & \text{if } 1\leqslant \ell\leqslant X;\\ 0 & \text{otherwise,}\end{cases}$$

and

$$v_m = \begin{cases} \Lambda^\sharp(m)\Psi_K(\eta m+\delta) & \text{if } 1\leqslant m\leqslant X;\\ 0 & \text{otherwise.}\end{cases}$$

Using the trivial bound

$$|\Lambda^\sharp(m)\Psi_K(\eta m+\delta)| \leqslant d(m)\log(m),$$

where $d(m)$ is the number of positive integer divisors of m, it follows that

$$\|v\|_2^2 \ll X(\log X)^5,$$

where we have used the well known bound $\sum_{m\leqslant X} d(m)^2 \ll X(\log X)^3$ (see, for example, the proof given by Hua [28, Theorem 5.3]; see also [44, 62, 63]). Hence, using Lemma 2.9 with $A = C + 9/2$ we derive the bound

$$\sum_{N\leqslant X} c_N \mathcal{G}_2^{\sharp\flat}(N) \ll \|c\|_2 \frac{X^{3/2}(\log X)^{9/2}}{(\log Z)^{C+9/2}} \tag{20}$$

for any constant $C > 0$. Similarly,

$$\sum_{N\leqslant X} c_N \mathcal{G}_2^{\flat\flat}(N) \ll \|c\|_2 \frac{X^{3/2}(\log X)^{9/2}}{(\log Z)^{C+9/2}}. \tag{21}$$

Turning to the sum $\mathcal{G}_2^{\sharp\sharp}(N)$, we begin by inserting the Fourier expansion of $\Psi_K(x)$ and then changing the order of summation, obtaining

$$\begin{aligned}\mathcal{G}_2^{\sharp\sharp}(N) &= \sum_{n_1+n_2=N} \Lambda^\sharp(n_1)\Lambda^\sharp(n_2)\Psi_K(\eta n_1+\delta)\Psi_K(\eta n_2+\delta)\\ &= \sum_{n\leqslant N} \Lambda^\sharp(n)\Lambda^\sharp(N-n)\Psi_K(\eta n+\delta)\Psi_K(\eta(N-n)+\delta)\\ &= \sum_{\substack{|k|\leqslant K\\ |\ell|\leqslant K}} g(k)g(\ell)\mathbf{e}(k\delta)\mathbf{e}(\ell(\eta N+\delta))\sum_{n\leqslant N}\Lambda^\sharp(n)\Lambda^\sharp(N-n)\mathbf{e}((k-\ell)\eta n).\end{aligned}$$

We now collect terms in double sum according to whether $k = \ell$ or not. Writing

$$G_2^{\sharp\sharp}(N) = \sum_{n\leqslant N}\Lambda^\sharp(n)\Lambda^\sharp(N-n),$$

the contribution to $\mathcal{G}_2^{\sharp\sharp}(N)$ coming from terms with $k = \ell$ is

$$G_2^{\sharp\sharp}(N)\sum_{|k|\leqslant K} g(k)^2\mathbf{e}(k(\eta N+2\delta)) = \Psi_K^{(2)}(\eta N+2\delta)G_2^{\sharp\sharp}(N),$$

where we have used (16) in the second step. To bound the remainder

$$R = \sum_{\substack{|k|,|\ell|\leqslant K\\ (k\neq\ell)}} g(k)g(\ell)\mathbf{e}(k\delta)\mathbf{e}(\ell(\eta N+\delta))\sum_{n\leqslant N}\Lambda^\sharp(n)\Lambda^\sharp(N-n)\mathbf{e}((k-\ell)\eta n),$$

we use the following result, the proof of which is given below:

Lemma 2.10. *For every integer $k_0 \neq 0$ with $|k_0| \leqslant 2K = 2X^{1/(4\tau)}$, we have*

$$\sum_{n \leqslant N} \Lambda^\sharp(n)\Lambda^\sharp(N-n)\mathbf{e}(k_0\eta n) \ll X^{1/2}Z^{3+4\tau},$$

where the implied constant depends only on α.

Using Lemma 2.10, it follows that

$$R \ll X^{1/2}Z^{3+4\tau} \sum_{|k| \leqslant K} \big|g(k)\big| \sum_{|\ell| \leqslant K} \big|g(\ell)\big| \ll X^{1/2}Z^{3+4\tau}(\log X)^2,$$

where we have used (9) together with our choice of K.

We have therefore shown that

$$\mathcal{G}_2^{\sharp\sharp}(N) = \Psi_K^{(2)}(\eta N + 2\delta)\, G_2^{\sharp\sharp}(N) + O\big(X^{1/2}Z^{3+4\tau}(\log X)^2\big).$$

For any complex numbers c_N, it follows that

$$\sum_{N \leqslant X} c_N \mathcal{G}_2^{\sharp\sharp}(N) = \sum_{N \leqslant X} c_N \Psi_K^{(2)}(\eta N + 2\delta)\, G_2^{\sharp\sharp}(N) + O\big(\|c\|_2\, XZ^{3+4\tau}(\log X)^2\big).$$

Now put $Z = X^{1/(9+12\tau)}$. Using the previous estimate together with the bounds (20) and (21), we derive from (19) the estimate

$$\sum_{N \leqslant X} c_N \mathcal{G}_2(N) = \sum_{N \leqslant X} c_N \Psi_K^{(2)}(\eta N + 2\delta)\, G_2^{\sharp\sharp}(N) + O\left(\|c\|_2 \frac{X^{3/2}}{(\log X)^C}\right).$$

Examining the proof of [30, Lemma 19.3] (which is stated only for even numbers N but holds for odd numbers as well) and taking into account the identity (4) with $\kappa = 2$, we deduce that

$$G_2^{\sharp\sharp}(N) = \mathfrak{S}_2(N)N + O\left(\frac{N}{(\log N)^C}\right).$$

Using the trivial estimate

$$\sum_{N \leqslant X} c_N \Psi_K^{(2)}(\eta N + 2\delta) \ll \|c\|_2\, X^{1/2},$$

it follows that

$$\sum_{N \leqslant X} c_N \mathcal{G}_2(N) = \sum_{N \leqslant X} c_N \Psi_K^{(2)}(\eta N + 2\delta)\, \mathfrak{S}_2(N)N + O\left(\|c\|_2 \frac{X^{3/2}}{(\log X)^C}\right).$$

Finally, by (15) and our choices of Δ and K, we have

$$\Psi_K^{(2)}(x) = \psi^{(2)}(x) + O(X^{-1/(8\tau)}).$$

In view of the trivial bound (6), it follows that

$$X^{-1/(8\tau)} \sum_{N \leqslant X} c_N \, \mathfrak{S}_2(N) N \ll \|c\|_2 \, X^{3/2-1/(8\tau)} \log\log X;$$

therefore,

$$\sum_{N \leqslant X} c_N \mathcal{G}_2(N) = \sum_{N \leqslant X} c_N \psi^{(2)}(\eta N + 2\delta) \, \mathfrak{S}_2(N) N + O\left(\|c\|_2 \, \frac{X^{3/2}}{(\log X)^C} \right)$$

as required. □

Proof of Lemma 2.9. We argue as in [30, Section 19.3] and begin with a bound for the exponential sum

$$S^\flat_{\Psi_K}(\xi) = \sum_{n \leqslant X} \Lambda^\flat(n) \Psi_K(\eta n + \beta) \mathbf{e}(\xi n).$$

From the definition (13), it follows that

$$|S^\flat_{\Psi_K}(\xi)| \leqslant \sum_{|k| \leqslant K} \big| g(k) S^\flat(\xi + k\eta) \big|,$$

where

$$S^\flat(\xi) = \sum_{n \leqslant X} \Lambda^\flat(n) \mathbf{e}(\xi n).$$

Using the bound (19.17) from [30] together with (9), we immediately deduce that the uniform bound

$$|S^\flat_{\Psi_K}(\xi)| \ll \frac{X \log X \log K}{(\log Z)^A} \qquad (\xi \in \mathbb{R}) \tag{22}$$

holds with any fixed constant $A > 0$.

To complete the proof, we observe that

$$\sum_{\ell+m+n=X} u_\ell \, v_m \, \Lambda^\flat(n) \Psi_K(\eta n + \delta)$$
$$= \int_0^1 \Big(\sum_{\ell \leqslant X} u_\ell \, \mathbf{e}(\xi \ell) \Big) \Big(\sum_{m \leqslant X} v_m \, \mathbf{e}(\xi m) \Big) S^\flat_{\Psi_K}(\xi) \mathbf{e}(-\xi X) \, d\xi.$$

Applying the Cauchy-Schwarz inequality and using (22) (with $K = X^{1/(4\tau)}$) together with the equalities

$$\int_0^1 \left| \sum_{\ell \leqslant X} u_\ell \, \mathbf{e}(\xi \ell) \right|^2 d\xi = \sum_{\ell \leqslant X} |u_\ell|^2$$

and

$$\int_0^1 \left| \sum_{m \leqslant X} v_m \, \mathbf{e}(\xi m) \right|^2 d\xi = \sum_{m \leqslant X} |v_m|^2,$$

we obtain the stated bound. □

Proof of Lemma 2.10. We have:

$$\begin{aligned}\sum_{n\leqslant N}&\Lambda^\sharp(n)\Lambda^\sharp(N-n)\mathbf{e}(k_0\eta n)\\ &=\sum_{n\leqslant N}\Bigg(\sum_{\substack{d_1\mid n\\ d_1\leqslant Z}}\mu(d_1)\log d_1\Bigg)\Bigg(\sum_{\substack{d_2\mid N-n\\ d_2\leqslant Z}}\mu(d_2)\log d_2\Bigg)\mathbf{e}(k_0\eta n)\\ &=\sum_{d_1,d_2\leqslant Z}\mu(d_1)\mu(d_2)\log d_1\log d_2\sum_{\substack{\ell_1,\ell_2\geqslant 1\\ \ell_1d_1+\ell_2d_2=N}}\mathbf{e}(k_0\eta\ell_1d_1).\end{aligned}\tag{23}$$

If $\ell_1\geqslant 1$, then $\ell_1d_1+\ell_2d_2=N$ for some $\ell_2\geqslant 1$ if and only if $\ell_1<N/d_1$, $f=\gcd(d_1,d_2)$ is a divisor of N, and

$$\ell_1(d_1/f)\equiv(N/f)\pmod{d_2/f}.$$

Let a be the least positive integer such that

$$a\equiv(d_1/f)^{-1}(N/f)\pmod{d_2/f}$$

Therefore, ℓ_1 varies over the set $\{a,a+d_2/f,\dots,a+(L-1)d_2/f\}$, where

$$L=\left\lfloor\frac{N/d_1-a}{d_2/f}\right\rfloor=\frac{N}{[d_1,d_2]}+O(1),$$

and it follows that

$$\begin{aligned}\sum_{\substack{\ell_1,\ell_2\geqslant 1\\ \ell_1d_1+\ell_2d_2=N}}\mathbf{e}(k_0\eta\ell_1d_1)&=\mathbf{e}(k_0\eta ad_1)\sum_{j=0}^{L-1}\mathbf{e}(k_0\eta j\,[d_1,d_2])\\ &\ll\frac{1}{\llbracket k_0\eta\,[d_1,d_2]\rrbracket},\end{aligned}\tag{24}$$

where we have used a standard estimate in the second step (see, for example, [32, Chapter 1, Lemma 1]). Since η is of type τ, we have

$$\llbracket\eta n\rrbracket\gg n^{-2\tau}\qquad(n\geqslant 1),$$

where the implied constant depends on α; thus,

$$\frac{1}{\llbracket k_0\eta\,[d_1,d_2]\rrbracket}\ll k_0^{2\tau}\,[d_1,d_2]^{2\tau}\leqslant(2X^{1/(4\tau)})^{2\tau}Z^{4\tau}\ll X^{1/2}Z^{4\tau}.$$

Combining this bound with (23) and (24), and using the trivial bound

$$\sum_{d_1,d_2\leqslant Z}\log d_1\log d_2\leqslant Z^2(\log Z)^2\ll Z^3,$$

we obtain the desired result. □

2.4 Three or more Beatty primes

In what follows, we use the same notation as in the proof of Theorem 2.8, except that we now define

$$\Delta = N^{-1/(8\tau)} \qquad \text{and} \qquad K = N^{1/(4\tau)}$$

instead of (18). With these choices, we have the following analog of (15) for every $\kappa \geqslant 2$:

$$\Psi_K^{(\kappa)}(x) = \psi^{(\kappa)}(x) + O(N^{-1/(8\tau)}) \qquad (x \in \mathbb{R}). \tag{25}$$

Also,

$$\Psi_K^{(\kappa)}(x) = \sum_{|\ell| \leqslant K} g(\ell)^\kappa \mathbf{e}(\ell x). \tag{26}$$

Proposition 2.11. *Let $\kappa \geqslant 2$ be fixed. If, for any constant $C > 0$, the estimate*

$$\mathcal{G}_\kappa(n) = \Psi_K^{(\kappa)}(\eta n + \kappa\delta)\mathfrak{S}_\kappa(n)\frac{n^{\kappa-1}}{(\kappa-1)!} + O\left(\frac{n^{\kappa-1}}{(\log n)^C}\right) \tag{27}$$

holds for all but $O\big(N(\log N)^{-C}\big)$ integers $n \leqslant N$, then the estimate

$$\mathcal{G}_{\kappa+1}(N) = \Psi_K^{(\kappa+1)}(\eta N + (\kappa+1)\delta)\mathfrak{S}_{\kappa+1}(N)\frac{N^\kappa}{\kappa!} + O\left(\frac{N^\kappa}{(\log N)^C}\right) \tag{28}$$

holds with any constant $C > 0$.

Remark. This result immediately yields a proof of Theorem 2.3. Indeed, using (6) and (25) we obtain (27) with $\kappa = 2$. By induction, Proposition 2.11 implies that (28) holds for every fixed $\kappa \geqslant 2$. Replacing κ by $\kappa - 1$ in (28) and then using the estimate (25) again, we obtain the statement of Theorem 2.3.

Proof of Proposition 2.11. To simplify our exposition in what follows, for any functions $F = F(N)$ and $G = G(N)$ we use notation

$$F = \widetilde{O}(G)$$

to mean that for any choice of the constant $C > 0$ the inequality

$$|F| \leqslant c\,\frac{|G|}{(\log N)^C}$$

holds for all $N \geqslant 2$ with a constant $c > 0$ that depends only on α, κ and C.

By Lemma 2.5 and the definition (2), we have

$$\begin{aligned}
\mathcal{G}_{\kappa+1}(N) &= \sum_{n_1+\dots+n_{\kappa+1}=N} \Lambda(n_1)\cdots\Lambda(n_{\kappa+1})\psi(\eta n_1+\delta)\cdots\psi(\eta n_{\kappa+1}+\delta) \\
&= \sum_{n\leqslant N} \Lambda(N-n)\psi(\eta(N-n)+\delta)\mathcal{G}_\kappa(n) \\
&= \sum_{n\leqslant N}{}^{*} \Lambda(N-n)\psi(\eta(N-n)+\delta)\mathcal{G}_\kappa(n) + \widetilde{O}(N^\kappa),
\end{aligned}$$

where $\sum^*$ indicates that the sum is restricted to integers n satisfying (27); note that we have used the trivial bound

$$\Lambda(N-n)\psi(\eta(N-n)+\delta)\mathcal{G}_\kappa(n) \ll N^{\kappa-1}(\log N)^\kappa$$

to estimate the contribution from exceptional integers. By (27), the previous sum is equal to

$$\sum_{n\leqslant N}^{*}\Lambda(N-n)\psi(\eta(N-n)+\delta)\Psi_K^{(\kappa)}(\eta n+\kappa\delta)\mathfrak{S}_\kappa(n)\frac{n^{\kappa-1}}{(\kappa-1)!}+\widetilde{O}(N^\kappa).$$

We now extend the sum to all integers $n \leqslant N$, using (6) or (7) to bound $\mathfrak{S}_\kappa(n)$ for each exceptional n, then we replace ψ with Ψ_K using (25) to control the error term. Finally, replacing n by $N-n$, we see that $\mathcal{G}_{\kappa+1}(N)$ is equal to

$$\sum_{n\leqslant N}\Lambda(n)\Psi_K(\eta n+\delta)\Psi_K^{(\kappa)}(\eta(N-n)+\kappa\delta)\mathfrak{S}_\kappa(N-n)\frac{(N-n)^{\kappa-1}}{(\kappa-1)!}+\widetilde{O}(N^\kappa).$$

In this sum, we substitute the Fourier expansions (13) and (26) for Ψ_K and $\Psi_K^{(\kappa)}$, respectively, then change the order of summation, obtaining

$$\mathcal{G}_{\kappa+1}(N)=\sum_{\substack{|k|\leqslant K\\|\ell|\leqslant K}}g(k)g(\ell)^\kappa\mathbf{e}(k\delta+\ell\eta N+\ell\kappa\delta)\frac{S_{k,\ell}(N)}{(\kappa-1)!}+\widetilde{O}(N^\kappa), \tag{29}$$

where

$$S_{k,\ell}(N)=\sum_{n\leqslant N}\Lambda(n)\mathbf{e}((k-\ell)\eta n)\mathfrak{S}_\kappa(N-n)(N-n)^{\kappa-1}.$$

We now show that the main contribution to $\mathcal{G}_{\kappa+1}(N)$ comes from the sums $S_{k,\ell}(N)$ with $k=\ell$. To this end, we use (4) to write

$$\begin{aligned}S_{k,\ell}(N)&=\sum_{n\leqslant N}\Lambda(n)\mathbf{e}((k-\ell)\eta n)(N-n)^{\kappa-1}\sum_{d\,|\,N-n}\sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}}\frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^\kappa}\\&=\sum_{d\leqslant N}\sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}}\frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^\kappa}\,T_{k,\ell,d}(N),\end{aligned}$$

where

$$T_{k,\ell,d}(N)=\sum_{\substack{n\leqslant N\\ n\equiv N\pmod d}}\Lambda(n)\mathbf{e}((k-\ell)\eta n)(N-n)^{\kappa-1}.$$

Using the trivial uniform bound

$$T_{k,\ell,d}(N)\ll\frac{N^\kappa\log N}{d}$$

and the well known lower bound $\varphi(d) \gg d/\log\log d$, we have for any $y > 3$ (since $\kappa \geqslant 2$):

$$\sum_{d>y} \sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^\kappa}\, T_{k,\ell,d}(N) \ll \sum_{d>y} \frac{d(\log\log d)^\kappa}{d^\kappa}\, \frac{N^\kappa \log N}{d}$$

$$\ll N^\kappa \log N \sum_{d>y} \frac{1}{d^{3/2}} \ll \frac{N^\kappa \log N}{y^{1/2}}.$$

Taking $y = (\log N)^A$ with $A = 2C + 2$ and $C > 0$ arbitrary, we derive that

$$S_{k,\ell}(N) = \sum_{d\leqslant (\log N)^A} \sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^\kappa}\, T_{k,\ell,d}(N) + O\left(\frac{N^\kappa}{(\log N)^C}\right).$$

Next, we observe that if $d \leqslant (\log N)^A$ and $\gcd(d, N) \neq 1$, then the number $\omega(d)$ of distinct prime divisors of d satisfies the bound $\omega(d) \ll \log\log N$, and it is easy to see that the bound

$$T_{k,\ell,d}(N) \ll N^{\kappa-1} \log N \log\log N$$

holds for all such d. Using this estimate in the preceding expression for $S_{k,\ell}(N)$, it follows that

$$S_{k,\ell}(N) = \sum_{\substack{d\leqslant (\log N)^A\\ \gcd(d,N)=1}} \sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^\kappa}\, T_{k,\ell,d}(N) + O\left(\frac{N^\kappa}{(\log N)^C}\right).$$

In the case that $k = \ell$, Lemma 2.6 immediately implies that

$$T_{k,k,d}(N) = \sum_{\substack{n\leqslant N\\ n\equiv N \pmod d}} \Lambda(n)(N-n)^{\kappa-1} = \frac{N^\kappa}{\kappa\,\varphi(d)} + \widetilde{O}(N^\kappa),$$

and therefore,

$$S_{k,k}(N) = \frac{N^\kappa}{\kappa} \sum_{\substack{d\leqslant (\log N)^A\\ \gcd(d,N)=1}} \sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^{\kappa+1}} + O\left(\frac{N^\kappa}{(\log N)^C}\right).$$

Since

$$\sum_{\substack{d>(\log N)^A\\ \gcd(d,N)=1}} \sum_{\substack{c\geqslant 1\\ \gcd(c,d)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^{\kappa+1}} \ll \sum_{d>(\log N)^A} \frac{(\log\log d)^{\kappa+1}}{d^\kappa} \ll \frac{1}{(\log N)^{C+1}},$$

and C is arbitrary, it follows that

$$S_{k,k}(N) = \frac{N^\kappa}{\kappa} \sum_{\substack{c,d\geqslant 1\\ \gcd(d,cN)=1}} \frac{\mu(c)^{\kappa+1}\mu(d)^\kappa d}{\varphi(c)^\kappa\varphi(d)^{\kappa+1}} + \widetilde{O}(N^\kappa).$$

Finally, using (5) (with κ replaced by $\kappa+1$) we deduce that

$$S_{k,k}(N) = \mathfrak{S}_{\kappa+1}(N)\frac{N^\kappa}{\kappa} + \widetilde{O}(N^\kappa) \qquad (|k| \leqslant K). \tag{30}$$

To treat the case $k \neq \ell$, we use the following result, the proof of which is given below:

Lemma 2.12. *There exists a constant $\nu > 0$ that depends only on α with the following property. For any positive integer d coprime to N, and any nonzero integer k_0 such that $|k_0| \leqslant 2N^{1/(4\tau)}$, the bound*

$$\sum_{\substack{n\leqslant N\\ n\equiv N \pmod d}} \Lambda(n)\mathbf{e}(k_0\eta n)(N-n)^{\kappa-1} \ll N^{\kappa-\nu}$$

holds, where the implied constant depends only on κ.

By Lemma 2.12 we have for all $|k|, |\ell| \leqslant K$ with $k \neq \ell$:

$$T_{k,\ell,d}(N) = \sum_{\substack{n\leqslant N\\ n\equiv N \pmod d}} \Lambda(n)\mathbf{e}((k-\ell)\eta n)(N-n)^{\kappa-1} = \widetilde{O}(N^\kappa),$$

and therefore,

$$S_{k,\ell}(N) = \widetilde{O}(N^\kappa) \qquad (|k|, |\ell| \leqslant K,\ k \neq \ell). \tag{31}$$

Inserting the estimates (30) and (31) into (29), and taking into account (9), it follows that

$$\begin{aligned}\mathcal{G}_{\kappa+1}(N) &= \mathfrak{S}_{\kappa+1}(N)\frac{N^\kappa}{\kappa!}\sum_{|k|\leqslant K} g(k)^{\kappa+1}\mathbf{e}(k\eta N + (\kappa+1)k\delta) + \widetilde{O}(N^\kappa)\\ &= \Psi_K^{(\kappa+1)}(\eta N + (\kappa+1)\delta)\mathfrak{S}_{\kappa+1}(N)\frac{N^\kappa}{\kappa!} + \widetilde{O}(N^\kappa),\end{aligned}$$

and this completes the proof. □

Proof of Lemma 2.12. Fix a constant ϱ such that

$$1 \leqslant \tau < \varrho < 2\tau.$$

Since η is of type τ, for some constant $c_0 > 0$ we have

$$[\![\eta m]\!] > c_0 m^{-\varrho} \qquad (m \geqslant 1). \tag{32}$$

Taking c_0 smaller if necessary, we can assume that $c_0 < 2^\varrho$. Put

$$c_1 = 2^\varrho/c_0 \qquad \text{and} \qquad \varepsilon = 1/(4\tau+2).$$

Let d and k_0 be integers with the properties stated in the lemma; without loss of generality, we can assume that k_0 is positive. Let a/b be the convergent in the continued fraction expansion of $k_0\eta$ that has the largest denominator b not exceeding $c_1 N^{1-\varepsilon}$; then,

$$\left|k_0\eta - \frac{a}{b}\right| \leqslant \frac{1}{bc_1N^{1-\varepsilon}} = \frac{c_0}{b2^\varrho N^{1-\varepsilon}}. \tag{33}$$

Multiplying by b and taking (32) into account, we have

$$\frac{c_0}{2^\varrho N^{1-\varepsilon}} \geqslant |bk_0\eta - a| \geqslant [\![bk_0\eta]\!] > c_0(bk_0)^{-\varrho}.$$

Thus, since $k_0 \leqslant 2N^{1/(4\tau)}$ and $\varrho < 2\tau$, it follows that

$$b \geqslant N^{(1-\varepsilon)/(2\tau)-1/(4\tau)} = N^\varepsilon. \tag{34}$$

Inserting (34) into (33) and recalling that $c_0 < 2^\varrho$, we conclude that

$$\left|k_0\eta - \frac{a}{b}\right| \leqslant \frac{1}{N}.$$

We are therefore in a position to apply Lemma 2.7 with $\theta = k_0\eta$, and this yields the stated result immediately since $N^\varepsilon \leqslant b \leqslant c_1 N^{1-\varepsilon}$. □

2.5 Convolutions with ψ

In this section, we focus on properties of the κ-fold convolutions of ψ. We recall that ψ is the periodic function with period one defined by

$$\psi(x) = \begin{cases} 1 & \text{if } 0 < \{x\} \leqslant \eta; \\ 0 & \text{if } \eta < \{x\} < 1 \text{ or } x \in \mathbb{Z}. \end{cases}$$

We assume that $\eta = \alpha^{-1} < 1$. As before, we put $\psi^{(1)} = \psi$, and for every $\kappa \geqslant 2$, we denote by $\psi^{(\kappa)}$ the κ-fold convolution of ψ with itself:

$$\psi^{(\kappa)}(x) = \int_0^1 \psi^{(\kappa-1)}(x-y)\psi(y)\,dy = \int_{x-\eta}^{x} \psi^{(\kappa-1)}(y)\,dy.$$

Since $0 \leqslant \psi(x) \leqslant \eta$ for all $x \in \mathbb{R}$, it is easy to see that

$$0 \leqslant \psi^{(\kappa)}(x) \leqslant \eta^{\kappa-1} \qquad (\kappa \geqslant 1,\ x \in \mathbb{R}).$$

Note that $\psi^{(\kappa)}$ is continuous for $\kappa \geqslant 2$ and differentiable for $\kappa \geqslant 3$.

Proposition 2.13. *If $\kappa \geqslant \lceil\alpha\rceil$, then there exists a constant $c > 0$ which depends only on α and κ such that $\psi^{(\kappa)}(x) \geqslant c$ for all $x \in \mathbb{R}$.*

Proof. By periodicity, it suffices to prove this for all x in $[\varepsilon, 1+\varepsilon]$ for some $\varepsilon > 0$. Since $\kappa\eta \geqslant \lceil\alpha\rceil / \alpha > 1$, there exists $\varepsilon > 0$ such that $1 + 2\varepsilon \leqslant \kappa\eta$. Fixing ε, it is easy to see that for every $x \in [\varepsilon, 1+\varepsilon]$ the closed intervals

$$\mathcal{I}_x = \left[\frac{x}{\kappa} - \frac{\varepsilon}{\kappa}, \frac{x}{\kappa} + \frac{\varepsilon}{\kappa}\right] \qquad \text{and} \qquad \mathcal{J}_x = \left[\frac{x}{\kappa} - \frac{\varepsilon}{\kappa(\kappa-1)}, \frac{x}{\kappa} + \frac{\varepsilon}{\kappa(\kappa-1)}\right]$$

are contained in $[0, \eta]$. Also, if $y_j \in \mathcal{J}_x$ for $j = 1, \dots, \kappa - 1$, then the number $x - y_1 - \cdots - y_{\kappa-1}$ lies in $\mathcal{I}_x$. Therefore,

$$\begin{aligned}\psi^{(\kappa)}(x) &= \int_0^1 \cdots \int_0^1 \psi(y_1) \cdots \psi(y_{\kappa-1}) \psi(x - y_1 - \cdots - y_{\kappa-1})\, dy_1 \cdots dy_{\kappa-1} \\ &\geqslant \int_{\mathcal{J}_x} \cdots \int_{\mathcal{J}_x} dy_1 \cdots dy_{\kappa-1} = \left(\frac{2\varepsilon}{\kappa(\kappa-1)}\right)^{\kappa-1}\end{aligned}$$

for all $x \in [\varepsilon, 1+\varepsilon]$. □

The remainder of this section is devoted to the problem of finding a sharp lower bound for $\psi^{(\kappa)}(x)$ in the special case that $\kappa = \lceil\alpha\rceil$, which is given in Theorem 2.19 below.

Lemma 2.14. *If $\kappa \geqslant 2$, then $\psi^{(\kappa)}(x) = \psi^{(\kappa)}(\kappa\eta - x)$ for all $x \in \mathbb{R}$.*

Proof. Let ψ_0 be the characteristic function of the set of real numbers x such that $[\![x]\!] \leqslant \eta/2$. Clearly, $\psi(x) = \psi_0(x - \eta/2)$ for all $x \in \mathbb{R} \setminus \mathbb{Z}$, and by induction on κ, we have $\psi^{(\kappa)}(x) = \psi_0^{(\kappa)}(x - \kappa\eta/2)$ for all $\kappa \geqslant 2$ and $x \in \mathbb{R}$. Since ψ_0 is an even function, so is $\psi_0^{(\kappa)}$ for all $\kappa \geqslant 2$; therefore,

$$\psi^{(\kappa)}(x) = \psi_0^{(\kappa)}(x - \kappa\eta/2) = \psi_0^{(\kappa)}(\kappa\eta/2 - x) = \psi^{(\kappa)}(\kappa\eta - x)$$

for all $\kappa \geqslant 2$ and $x \in \mathbb{R}$. □

Lemma 2.15. *If $1 \leqslant \kappa < \lceil\alpha\rceil$ and $x \in (\kappa\eta, 1]$, then $\psi^{(\kappa)}(x) = 0$.*

Proof. When $\kappa = 1$, this follows from the definition of ψ. Now suppose that $\psi^{(\kappa-1)}(x) = 0$ for all $x \in ((\kappa-1)\eta, 1]$, where $\kappa \geqslant 2$. Then, for each $x \in (\kappa\eta, 1]$ the interval $[x-\eta, x]$ is contained in $((\kappa-1)\eta, 1]$; therefore,

$$\psi^{(\kappa)}(x) = \int_{x-\eta}^{x} \psi^{(\kappa-1)}(y)\, dy = 0,$$

and the result follows by induction. □

The next result is an easy consequence of Lemma 2.15:

Lemma 2.16. *If $2 \leqslant \kappa < \lceil \alpha \rceil$ and $x \in [0, \eta]$, then*

$$\psi^{(\kappa)}(x) = \int_0^x \psi^{(\kappa-1)}(y)\, dy.$$

The same result holds for $\kappa = \lceil \alpha \rceil$ and $x \in [\kappa\eta - 1, \eta]$.

Lemma 2.17. *For $1 \leqslant \kappa < \lceil \alpha \rceil$ and $x \in (0, \eta]$, we have*

$$\psi^{(\kappa)}(x) = \frac{x^{\kappa-1}}{(\kappa-1)!}.$$

Proof. This is immediate for $\kappa = 1$. Suppose that $\psi^{(\kappa-1)}(x) = x^{\kappa-2}/(\kappa-2)!$ for $x \in (0, \eta]$, where $2 \leqslant \kappa < \lceil \alpha \rceil$. Then, by Lemma 2.16 we have

$$\psi^{(\kappa)}(x) = \int_0^x \psi^{(\kappa-1)}(y)\, dy = \int_0^x \frac{y^{\kappa-2}}{(\kappa-2)!}\, dy = \frac{x^{\kappa-1}}{(\kappa-1)!},$$

and the result follows by induction. □

Lemma 2.18. *If $1 \leqslant \kappa < \lceil \alpha \rceil$, then $\psi^{(\kappa)}$ is increasing on $[0, \kappa\eta/2]$.*

Proof. For $\kappa = 1$ this is immediate, and for $\kappa = 2$, it follows from the fact that $\psi^{(2)}(x) = x$ for $x \in [0, \eta]$ by Lemma 2.17 and the continuity of $\psi^{(2)}$. Now suppose that $\psi^{(\kappa-1)}$ is increasing on $[0, (\kappa-1)\eta/2]$, where $\kappa \geqslant 3$. Since $\psi^{(\kappa)}$ is differentiable, we have for $x \in [\eta, (\kappa-1)\eta/2]$:

$$\left.\frac{d\psi^{(\kappa)}(t)}{dt}\right|_{t=x} = \psi^{(\kappa-1)}(x) - \psi^{(\kappa-1)}(x-\eta) \geqslant 0.$$

If $x \in [0, \eta]$, then by Lemma 2.16 it follows that

$$\left.\frac{d\psi^{(\kappa)}(t)}{dt}\right|_{t=x} = \psi^{(\kappa-1)}(x) - \psi^{(\kappa-1)}(0) \geqslant 0.$$

Finally, suppose that $x \in [(\kappa-1)\eta/2, \kappa\eta/2]$. Since $\psi^{(\kappa-1)}$ is increasing on $[0, (\kappa-1)\eta/2]$, it is decreasing on $[(\kappa-1)\eta/2, (\kappa-1)\eta]$ by Lemma 2.14; therefore, using the same lemma we have

$$\begin{aligned}\left.\frac{d\psi^{(\kappa)}(t)}{dt}\right|_{t=x} &= \psi^{(\kappa-1)}(x) - \psi^{(\kappa-1)}(x-\eta) \\ &\geqslant \psi^{(\kappa-1)}(\kappa\eta/2) - \psi^{(\kappa-1)}((\kappa-2)\eta/2) = 0,\end{aligned}$$

and the proof is completed by induction. □

Theorem 2.19. *For $\kappa = \lceil \alpha \rceil$, the sharp lower bound*

$$\psi^{(\kappa)}(x) \geqslant \frac{(\kappa\eta - 1)^{\kappa-1}}{2^{\kappa-2}(\kappa-1)!}$$

holds uniformly for all $x \in \mathbb{R}$.

Proof. Since $\psi^{(\kappa)}$ has period one, we can assume that $x \in [0,1]$.

Using Lemmas 2.14 and 2.16 and arguing as in the proof of Lemma 2.18, one sees that $\psi^{(\kappa)}$ is increasing on the interval $[\kappa\eta - 1, \kappa\eta/2]$ and decreasing on the interval $[\kappa\eta/2, 1]$. Therefore,

$$\psi^{(\kappa)}(x) \geqslant \psi^{(\kappa)}(1) = \psi^{(\kappa)}(0)$$

for all $x \in [\kappa\eta - 1, 1]$. On the other hand, for $x \in [0, \kappa\eta - 1]$ we have by Lemmas 2.14, 2.15 and 2.17:

$$\begin{aligned}
\psi^{(\kappa)}(x) &= \int_{x+1-\eta}^{1} \psi^{(\kappa-1)}(y)\,dy + \int_0^x \psi^{(\kappa-1)}(y)\,dy \\
&= \int_{(\kappa-1)\eta-1}^{\kappa\eta-1-x} \psi^{(\kappa-1)}(y)\,dy + \int_0^x \psi^{(\kappa-1)}(y)\,dy \\
&= \int_0^{\kappa\eta-1-x} \psi^{(\kappa-1)}(y)\,dy + \int_0^x \psi^{(\kappa-1)}(y)\,dy = f(x),
\end{aligned}$$

where

$$f(x) = \frac{(\kappa\eta - 1 - x)^{\kappa-1} + x^{\kappa-1}}{(\kappa-1)!}.$$

Since the function $f(x)$ attains its minimum on $[0, \kappa\eta - 1]$ at $x = (\kappa\eta - 1)/2$, we obtain the stated result. □

2.6 Proof of Theorem 2.1

Suppose that $\kappa < \alpha$. If $N \equiv \kappa \pmod 2$, and

$$N = \lfloor \alpha m_1 + \beta \rfloor + \lfloor \alpha m_2 + \beta \rfloor + \cdots + \lfloor \alpha m_\kappa + \beta \rfloor \tag{35}$$

for some $m_1, \ldots, m_\kappa \in \mathbb{N}$, then

$$(N - \kappa\beta)\alpha^{-1} \leqslant m_1 + \cdots + m_\kappa < (N - \kappa\beta)\alpha^{-1} + \kappa\alpha^{-1}.$$

Therefore, the relation (35) cannot hold if the fractional part $\{(N - \kappa\beta)\alpha^{-1}\}$ of $(N - \kappa\beta)\alpha^{-1}$ lies in the open interval $(0, 1 - \kappa\alpha^{-1})$, which happens for about $\frac{1}{2}(1 - \kappa\alpha^{-1})X$ positive integers $N \leqslant X$ with $N \equiv \kappa \pmod 2$. This proves the forward implications of the statements in Theorem 2.1. The reverse implications follow immediately from Theorems 2.2 and 2.3 combined with the lower bound of Proposition 2.13 and partial summation.

2.7 Remarks

For an irrational number α in the range $0 < \alpha < 1$, it is clear that the Beatty sequence $\mathcal{B}_{\alpha,\beta}$ contains all prime numbers. In this case, since $\psi^{(\kappa)}(x) = 1$ for all $\kappa \geqslant 1$ and $x \in \mathbb{R}$, the statements in Theorems 2.2 and 2.3 are consistent with known results for the number of representations of an integer N as a sum of κ prime numbers.

It would be interesting to see whether the results of this manuscript can be extended to include irrational numbers α of infinite type (with a weakened error term).

To address a question that was posed in a preprint of the present paper, Kumchev [34] has studied representations of the form $N = p_1 + p_2 + \cdots + p_k$ with each prime p_j lying in the Beatty sequence $\mathcal{B}_{\alpha_j,\beta_j}$, where the numbers α_j, β_j are real, each α_j is irrational (of finite type) and greater than one, and at least one ratio α_i/α_j is irrational.

During the course of our investigations, we observed an interesting phenomenon. If $\alpha, \beta, \beta' \in \mathbb{R}$ with $\alpha > 1$ and α is an irrational number of finite type, put

$$\mathcal{G}_\kappa(\alpha, \beta; N) = \sum_{\substack{n_1+\cdots+n_\kappa=N \\ n_1,\dots,n_\kappa \in \mathcal{B}_{\alpha,\beta}}} \Lambda(n_1) \cdots \Lambda(n_\kappa)$$

as before, and let $\mathcal{G}_\kappa(\alpha, \beta'; N)$ be defined similarly. If $\beta' = \beta + \alpha/\kappa$ for some fixed $\kappa > \alpha$, then it is easy to see that the Beatty sequences $\mathcal{B}_{\alpha,\beta}$ and $\mathcal{B}_{\alpha,\beta'}$ contain *different* sets of primes. Nevertheless, by Theorem 2.3 one can immediately conclude that

$$\mathcal{G}_\kappa(\alpha, \beta; N) \sim \mathcal{G}_\kappa(\alpha, \beta'; N) \qquad (N \to \infty).$$

Part 3

Sums with multiplicative functions over a Beatty sequence

3.1 Introduction

Let $A \geqslant 1$ be an arbitrary constant, and let $\mathscr{F}_A$ be the set of multiplicative functions such that $|f(p)| \leqslant A$ for all primes p, and

$$\sum_{n \leqslant N} |f(n)|^2 \leqslant A^2 N \qquad (N \in \mathbb{N}). \tag{36}$$

Exponential sums of the form

$$S_{\alpha,f}(N) = \sum_{n \leqslant N} f(n) e(n\alpha) \qquad (\alpha \in \mathbb{R},\ f \in \mathscr{F}_A), \tag{37}$$

where $e(z) = e^{2\pi i z}$ for all $z \in \mathbb{R}$, occur frequently in analytic number theory. Montgomery and Vaughan have shown (see [41, Corollary 1]) that the upper bound

$$S_{\alpha,f}(N) \ll_A \frac{N}{\log N} + \frac{N(\log R)^{3/2}}{R^{1/2}} \tag{38}$$

holds uniformly for all $f \in \mathscr{F}_A$ provided that $|\alpha - a/q| \leqslant q^{-2}$ with some reduced fraction a/q for which $2 \leqslant R \leqslant q \leqslant N/R$. They also proved that this bound is sharp apart from the logarithmic factor in R. In this manuscript, we use the Montgomery-Vaughan result to estimate sums of the form

$$G_{\alpha,\beta,f}(N) = \sum_{\substack{n \leqslant N \\ n \in \mathcal{B}_{\alpha,\beta}}} f(n), \tag{39}$$

where $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, $f \in \mathcal{F}_A$, and $\mathcal{B}_{\alpha,\beta}$ is defined as in Section 2.1.Our results are uniform over the family $\mathscr{F}_A$ and nontrivial whenever

$$\lim_{N \to \infty} \frac{\log N}{N \log\log N} \left| \sum_{n \leqslant N} f(n) \right| = \infty,$$

a condition which guarantees that the error term in Theorem 3.1 is smaller than the main term. One can remove this condition, at the expense of losing uniformity with

respect to f, and still obtain Theorem 3.1 for any bounded arithmetic function f (not necessarily multiplicative) for which the exponential sums in (37) satisfy

$$S_{\alpha,f}(N) = o\left(\sum_{n\leqslant N} f(n)\right) \qquad (N \to \infty).$$

The general problem of characterizing functions for which this relation holds appears to be rather difficult; see [3] for Bachman's conjecture and his related work on this problem.

We shall also assume that α is irrational and of finite type τ. For an irrational number γ, the type of γ is defined as in Section 2.2.2.

Our main result is the following:

Theorem 3.1. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. Then, for all $f \in \mathscr{F}_A$ we have*

$$G_{\alpha,\beta,f}(N) = \alpha^{-1} \sum_{n\leqslant N} f(n) + O\left(\frac{N \log\log N}{\log N}\right),$$

where the implied constant depends only on α and A.

The following corollaries are immediate applications of Theorem 3.1:

Corollary 3.2. *The number of integers not exceeding N that lie in the Beatty sequence $\mathcal{B}_{\alpha,\beta}$ and can be represented as a sum of two squares is*

$$\#\{n \leqslant N : n \in \mathcal{B}_{\alpha,\beta},\ n = \square + \square\} = \alpha^{-1} C \frac{N}{(\log N)^{1/2}} + O\left(\frac{N \log\log N}{\log N}\right)$$

as $N \to \infty$, where

$$C = 2^{-1/2} \prod_{p\equiv 3 \bmod 4} (1 - p^{-2})^{-1/2}. \tag{40}$$

To state the next result, we recall that an integer n is said to be *k-free* if $p^k \nmid n$ for every prime p.

Corollary 3.3. *For every $k \geqslant 2$, the number of k-free integers not exceeding N that lie in the Beatty sequence $\mathcal{B}_{\alpha,\beta}$ is*

$$\#\{n \leqslant N : n \in \mathcal{B}_{\alpha,\beta},\ n \ \ k\text{-free}\} = \alpha^{-1}\zeta^{-1}(k) N + O\left(\frac{N \log\log N}{\log N}\right)$$

as $N \to \infty$, where $\zeta(s)$ is the Riemann zeta function.

Finally, we consider the average value of the number of representations of an integer from a Beatty sequence as a sum of four squares. Our result is the following:

Corollary 3.4. *Let $r_4(n)$ denote the number of representations of n as a sum of four squares. Then,*

$$\sum_{\substack{n\leqslant N\\ n\in\mathcal{B}_{\alpha,\beta}}} r_4(n) = \frac{\pi^2 N^2}{2\alpha} + O\left(\frac{N^2 \log\log N}{\log N}\right),$$

where the implied constant depends only on α.

Any implied constants in the symbols O and $\ll$ may depend on the parameters α and A but are absolute otherwise. We recall that the notation $X \ll Y$ is equivalent to $X = O(Y)$.

3.2 Proofs

3.2.1 Proof of Theorem 3.1

We define the funtion ψ as in Section 2.1 and the function Ψ as in Section 2.3 from a result of Vinogradov (see [61, Chapter I, Lemma 12]).

Using Lemma 2.5, we rewrite the sum (39) in the form

$$G_{\alpha,\beta,f}(N) = \sum_{n\leqslant N} f(n)\psi(\gamma n + \delta).$$

Replacing ψ by Ψ we have

$$G_{\alpha,\beta,f}(N) = \sum_{n\leqslant N} f(n)\Psi(\gamma n + \delta) + O\left(\sum_{n\in\mathcal{V}(\mathcal{I},N)} f(n)\right), \tag{41}$$

where $\mathcal{V}(\mathcal{I}, N)$ is the set of positive integers $n \leqslant N$ for which

$$\{\gamma n + \delta\} \in \mathcal{I} = [0,\Delta) \cup (\gamma - \Delta, \gamma + \Delta) \cup (1 - \Delta, 1).$$

Since $|\mathcal{I}| = 4\Delta$, it follows from Lemma 2.4 and the definition (3) that

$$\left|\mathcal{V}(\mathcal{I}, N)\right| \ll \Delta N + N^{1-1/(2\tau)},$$

where we have used the fact that α and γ have the same type τ. Thus, taking (36) into account, we have by the Cauchy inequality:

$$\begin{aligned}\left|\sum_{n\in\mathcal{V}(\mathcal{I},N)} f(n)\right| &\leqslant \left|\mathcal{V}(\mathcal{I}, N)\right|^{1/2} \left(\sum_{n\leqslant N} |f(n)|^2\right)^{1/2} \\ &\ll \Delta^{1/2} N + N^{1-1/(4\tau)}.\end{aligned} \tag{42}$$

Next, let $K \geqslant \Delta^{-1}$ be a large real number (to be specified later), and let Ψ_K be the trigonometric polynomial given by

$$\Psi_K(x) = \sum_{|k|\leqslant K} g(k)\mathbf{e}(kx) = \gamma + \sum_{0<|k|\leqslant K} g(k)\mathbf{e}(kx) \qquad (x \in \mathbb{R}). \tag{43}$$

Using (9) we see that the estimate

$$\Psi_K(x) = \Psi(x) + O(K^{-1}\Delta^{-1})$$

holds uniformly for all $x \in \mathbb{R}$; therefore,

$$\sum_{n\leqslant N} f(n)\psi(\gamma n + \delta) = \sum_{n\leqslant N} f(n)\Psi_K(\gamma n + \delta) + O\left(K^{-1}\Delta^{-1}N\right), \tag{44}$$

where we have used the bound $\sum_{n\leqslant N} |f(n)| \ll N$, which follows from (36).

Combining (41), (42), (43) and (44) we derive that

$$G_{\alpha,\beta,f}(N) = \gamma \sum_{n\leqslant N} f(n) + H(N) + O\left(K^{-1}\Delta^{-1}N + \Delta^{1/2}N + N^{1-1/(4\tau)}\right),$$

where

$$H(N) = \sum_{0<|k|\leqslant K} g(k)\mathbf{e}(k\delta)S_{k\gamma,f}(N).$$

Put $R = (\log N)^3$. We claim that, if N is sufficiently large, then for every k in the above sum there is a reduced fraction a/q such that $|\alpha - a/q| \leqslant q^{-2}$ and $R \leqslant q \leqslant N/R$. Assuming this for the moment, (38) implies that

$$S_{k\gamma,f}(N) \ll \frac{N}{\log N} \qquad (0 < |k| \leqslant K),$$

and using (9) we deduce that

$$H(N) \ll \frac{N\log K}{\log N}.$$

Therefore,

$$G_{\alpha,\beta,f}(N) - \gamma \sum_{n\leqslant N} f(n) \ll \frac{N\log K}{\log N} + K^{-1}\Delta^{-1}N + \Delta^{1/2}N.$$

To balance the error terms, we choose

$$\Delta = (\log N)^{-2} \qquad \text{and} \qquad K = \Delta^{-3/2} = (\log N)^3,$$

obtaining the bound stated in the theorem.

To prove the claim, let k be an integer with $0 < |k| \leqslant K = (\log N)^3$, and let $r_i = a_i/q_i$ be the i-th convergent in the continued fraction expansion of $k\gamma$. Since γ is of finite type τ, for every $\mathbf{e}_p > 0$ there is a constant $C = C(\gamma, \mathbf{e}_p)$ such that

$$C(|k|q_{i-1})^{-(\tau+\mathbf{e}_p)} < [\![\gamma|k|q_{i-1}]\!] \leqslant \left|\gamma|k|q_{i-1} - a_{i-1}\right| \leqslant q_i^{-1}.$$

Put $\mathbf{e}_p = \tau$, and let j be the least positive integer for which $q_j \geqslant R$ (note that $j \geqslant 2$). Then,

$$R \leqslant q_j \ll (|k|q_{i-1})^{2\tau} \leqslant (KR)^{2\tau} = (\log N)^{6\tau},$$

and it follows that $R \leqslant q_j \leqslant N/R$ if N is sufficiently large, depending only on α. This concludes the proof.

3.2.2 Proof of Corollary 3.2

Let $f(n)$ be the characteristic function of the set of integers that can be represented as a sum of two squares. Then Corollary 3.2 follows immediately from Theorem 3.1 and the asymptotic formula (see for example [57]):

$$\sum_{n\leqslant N} f(N) = \frac{CN}{(\log N)^{1/2}} + O\left(\frac{N}{(\log N)^{3/2}}\right),$$

where C is given by (40).

3.2.3 Proof of Corollary 3.3

Fix $k \geqslant 2$ and let $f(n)$ be the characteristic function of the set of k-free integers. Then Corollary 3.3 follows from Theorem 3.1 and the following estimate of Gegenbauer [21] for the number of k-free integers not exceeding N:

$$\sum_{n\leqslant N} f(N) = \zeta^{-1}(k)N + O\left(N^{1/k}\right).$$

3.2.4 Proof of Corollary 3.4

Put $f(n) = r_4(n)/(8n)$. From Jacobi's formula for $r_4(n)$, namely

$$r_4(n) = 8(2 + (-1)^n) \sum_{\substack{d\,|\,n \\ d \text{ odd}}} d \qquad (n \geqslant 1),$$

it follows that $f(n)$ is multiplicative, and $f(p) \leqslant 3/2$ for every prime p. Moreover, using the formula of Ramanujan [49] (see also [59]):

$$\sum_{n\leqslant N} \sigma^2(n) = \frac{5}{6}\,\zeta(3)N^3 + O(N^2(\log N)^2),$$

we have by partial summation:

$$\sum_{n\leqslant N}|f(n)|^2\leqslant\sum_{n\leqslant N}\frac{\sigma^2(n)}{n^2}=\frac{5}{2}\,\zeta(3)N+O((\log N)^3).$$

Therefore, $f(n)\in\mathscr{F}_A$ for some constant $A\geqslant 1$. Applying Theorem 3.1, we deduce that

$$\sum_{\substack{n\leqslant N\\ n\in\mathcal{B}_{\alpha,\beta}}}\frac{r_4(n)}{n}=\alpha^{-1}\sum_{n\leqslant N}\frac{r_4(n)}{n}+O\left(\frac{N\log\log N}{\log N}\right),$$

where the implied constant depends only on α.

From the asymptotic formula (see for example [30, p22]):

$$\sum_{n\leqslant N}r_4(n)=\frac{\pi^2N^2}{2}+O(N\log N),$$

we have by partial summation:

$$\sum_{n\leqslant N}\frac{r_4(n)}{n}=\pi^2N+O((\log N)^2).$$

Consequently,

$$\sum_{\substack{n\leqslant N\\ n\in\mathcal{B}_{\alpha,\beta}}}\frac{r_4(n)}{n}=\alpha^{-1}\pi^2N+O\left(\frac{N\log\log N}{\log N}\right).$$

Using partial summation once more, we obtain the statement of Corollary 3.4.

Part 4

Nicolas and Robin Inequalities

4.1 Introduction

In 1903 Landau (see [36, pp. 217–219]) showed that

$$\overline{\lim_{n\to\infty}}\ \frac{n}{\varphi(n)\log\log n} = e^{\gamma}. \tag{45}$$

Eighty years later, in a highly interesting work, Nicolas [43] proved that the inequality

$$\frac{n}{\varphi(n)} > e^{\gamma}\log\log n$$

holds for infinitely many natural numbers n. Moreover, if N_k denotes the product of the first k primes, he proved that

$$\frac{N_k}{\varphi(N_k)} > e^{\gamma}\log\log N_k$$

holds for every $k \geqslant 1$ on the RH. Assuming RH is false, he also showed there are both infinitely many k for which this inequality holds and infinitely many k for which it does not hold. To acknowledge the many contributions of Nicolas to this subject, we denote by $\mathcal{N}$ the set of numbers $n \in \mathbb{N}$ that satisfy the *Nicolas inequality*:

$$\frac{n}{\varphi(n)} < e^{\gamma}\log\log n. \tag{46}$$

The principle aim of this manuscript is to exhibit a broad class of infinite subsets $\mathcal{S} \subset \mathbb{N}$ such that this inequality holds for all but finitely many $n \in \mathcal{S}$. This class includes a set that contains all natural numbers which can be expressed as a sum of two squares.

The analogue of (45) for this function was obtained by Gronwall [23], who proved that

$$\overline{\lim_{n\to\infty}}\ \frac{\sigma(n)}{n\log\log n} = e^{\gamma}.$$

Robin [51] showed that if RH is true, then the *Robin inequality*:

$$\frac{\sigma(n)}{n} < e^{\gamma}\log\log n \tag{47}$$

holds for every integer $n > 5040$, whereas if RH is false, then this inequality fails for infinitely many n. We denote by $\mathcal{R}$ the set of numbers $n \in \mathbb{N}$ that satisfy (47). In view of the elementary inequality

$$\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} \qquad (n > 1),$$

it is clear that $\mathcal{N} \subset \mathcal{R}$. Thus, for the class of subsets $\mathcal{S} \subset \mathbb{N}$ considered in the present manuscript, the Robin inequality holds for all but finitely many $n \in \mathcal{S}$.

Our work was originally inspired by a recent paper of Choie *et al* [15], which establishes the inclusion in $\mathcal{R}$ of various infinite subsets of the natural numbers $\mathbb{N}$. In particular, in [15] it is shown that $\mathcal{R}$ contains every square-free number $n > 30$, every odd integer $n > 9$, every powerful number $n > 36$, and every integer $n > 1$ not divisible by the fifth power of some prime. As a consequence it follows that the RH holds iff the Robin inequality holds for all natural numbers n divisible by the fifth power of some prime. Note that this criterion does not have the restriction $n \geqslant 5041$. Another "5041-free" criterion was given earlier by Lagarias [35], who showed that RH is true iff

$$\sigma(n) \leqslant H_n + e^{H_n} \log H_n,$$

where

$$H_n = \sum_{j \leqslant n} \frac{1}{j} \qquad (n \geqslant 1).$$

To state our results more precisely for any subset $\mathcal{A} \subset \mathbb{P}$, put

$$\pi_{\mathcal{A}}(x) = \#\big\{p \leqslant x \ : \ p \in \mathcal{A}\big\}$$

Let $\mathcal{P}$ be an arbitrary (fixed) subset of $\mathbb{P}$ such that

$$\overline{\delta} = \varlimsup_{x\to\infty} \frac{\pi_{\mathcal{P}}(x)}{\pi(x)} < 1 \qquad \text{and} \qquad \underline{\delta} = \varliminf_{x\to\infty} \frac{\pi_{\mathcal{P}}(x)}{\pi(x)} > 0. \tag{48}$$

Let $\mathcal{Q}$ denote the complementary set of primes (i.e., $\mathcal{Q} = \mathbb{P} \setminus \mathcal{P}$), and note that

$$\varlimsup_{x\to\infty} \frac{\pi_{\mathcal{Q}}(x)}{\pi(x)} = 1 - \underline{\delta} < 1 \qquad \text{and} \qquad \varliminf_{x\to\infty} \frac{\pi_{\mathcal{Q}}(x)}{\pi(x)} = 1 - \overline{\delta} > 0. \tag{49}$$

In this manuscript, we work with the set $\mathcal{S} = \mathcal{S}(\mathcal{P})$ defined by

$$\mathcal{S} = \big\{n \in \mathbb{N} \ : \ \text{if } p \in \mathcal{Q} \text{ and } p \mid n, \text{ then } p^2 \mid n\big\}. \tag{50}$$

Our main result is the following:

Theorem 4.1. *The set $\mathcal{N}$ contains all but finitely many of the numbers in $\mathcal{S}$.*

Corollary 4.2. *Of the numbers n which do not satisfy the Nicolas inequality, all but finitely many are divisible by a prime $q \in \mathcal{Q}$ such that $q^2 \nmid n$.*

In particular, for any fixed $a, m \in \mathbb{N}$ with $\gcd(a, m) = 1$, one can put

$$\mathcal{P} = \big\{p \in \mathbb{P} \ : \ p \not\equiv a \pmod{m}\big\}$$

and apply Corollary 4.2 to deduce the following:

Corollary 4.3. *Of the numbers n which do not satisfy the Nicolas inequality, all but finitely many are divisible by a prime $q \equiv a \pmod{m}$ such that $q^2 \nmid n$.*

In Section 4.3 we examine more closely the special case that

$$\mathcal{P} = \big\{p \in \mathbb{P} \ : \ p \equiv 1 \pmod 4\big\} \cup \{2\}.$$

Note that the corresponding set $\mathcal{S}$ contains all natural numbers of the form $n = a^2 + b^2$ (since, by a theorem of Fermat, every prime $q \equiv 3 \pmod 4$ appears with even multiplicity in the prime factorization of n if and only if n can be written as a sum of two squares). Using effective bounds from [50] on the number of primes in arithmetic progressions modulo 4, we are able to determine the set $\mathcal{S} \setminus \mathcal{N}$ completely, leading to:

Theorem 4.4. *The set $\mathcal{S} \setminus \mathcal{N}$ contains precisely* 347 *natural numbers. In particular, there are precisely* 246 *numbers which can be expressed as a sum of two squares and such that the Nicolas inequality* (46) *does not hold, the largest of which is the number* 52509581344222812810.

As an application, we obtain the unconditional result that

$$\{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 36, 72, 180, 360, 720\}$$

is a complete list of those natural numbers which can be expressed as a sum of two squares and such that the Robin inequality (47) does not hold; this result is consistent with the truth of the Riemann Hypothesis.

Results like those of Theorem 4.4 can be established for certain quadratic forms other than $a^2 + b^2$. For example, using similar techniques one finds that there are precisely 261 numbers that can be expressed in the form $n = a^2 + 3b^2$ and for which the Nicolas inequality (46) does not hold, the largest of which is the number 397999936131188090700.

Throughout this part, any implied constants in the symbols O, $\ll$, $\gg$ and $\asymp$ depend (at most) on the set $\mathcal{P}$ and are absolute otherwise.

4.2 Proof of Theorem 4.1

For every natural number n we put

$$F(n) = \frac{n}{\varphi(n)} = \prod_{p \,|\, n} \frac{p}{p-1}\,.$$

Note that

$$F(n) = F(\kappa(n)) \qquad \text{and} \qquad \omega(n) = \omega(\kappa(n)), \tag{51}$$

where $\omega(n)$ is the number of distinct prime divisors of n, and $\kappa(n)$ is the square-free kernel of n:

$$\kappa(n) = \prod_{p\,|\,n} p.$$

Let

$$\mathcal{N}^\circ = \mathbb{N} \setminus \mathcal{N} = \big\{n \in \mathbb{N} \ : \ F(n) \geqslant e^\gamma \log\log n\big\},$$

and for every integer $k \geqslant 0$, let

$$\mathcal{V}_k = \big\{n \in \mathbb{N} \ : \ \omega(n) \geqslant k\big\} \qquad \text{and} \qquad \mathcal{W}_k = \mathcal{S} \cap \mathcal{N}^\circ \cap \mathcal{V}_k.$$

Since $\mathcal{V}_0 = \mathbb{N}$, Theorem 4.1 is the assertion that $\mathcal{W}_0 = \mathcal{S} \cap \mathcal{N}^\circ$ is a finite set. In view of the next lemma, it suffices to show that $\mathcal{W}_k = \varnothing$ for some k.

Lemma 4.5. *For every $k \geqslant 0$, $\mathcal{W}_0 \setminus \mathcal{W}_k$ is a finite set.*

Since $\omega(n) < k$ and $F(n) \geqslant e^\gamma \log\log n$ for all $n \in \mathcal{W}_0 \setminus \mathcal{W}_k$, Lemma 4.5 is an immediate consequence of the following:

Lemma 4.6. *For every constant $K > 0$, there are at most finitely many natural numbers n such that $\omega(n) \leqslant K$ and $F(n) \geqslant e^\gamma \log\log n$.*

Proof. If $\overline{p}_1, \overline{p}_2, \ldots$ is the sequence of consecutive prime numbers, then for any such number n we have

$$\prod_{j \leqslant K} \frac{\overline{p}_j}{\overline{p}_j - 1} \geqslant \prod_{p\,|\,n} \frac{p}{p-1} = F(n) \geqslant e^\gamma \log\log n;$$

this shows that n is bounded by a constant which depends only on K. □

For every natural number n, let

$$s(n) = \Big(\prod_{\substack{p\,|\,n \\ p \in \mathcal{P}}} p\Big)\Big(\prod_{\substack{q\,|\,n \\ q \in \mathcal{Q}}} q^2\Big),$$

and put

$$\mathcal{Y} = \big\{n \in \mathbb{N} \ : \ n = s(n)\big\}.$$

Note that $\mathcal{Y} \subset \mathcal{S}$. The following statements are elementary:

($\mathscr{C}_1$) if $n = pm$ with $p \in \mathcal{P}$ and $p \nmid m$, then $n \in \mathcal{Y}$ if and only if $m \in \mathcal{Y}$;

($\mathscr{C}_2$) if $n = q^2 m$ with $q \in \mathcal{Q}$ and $q \nmid m$, then $n \in \mathcal{Y}$ if and only if $m \in \mathcal{Y}$;

($\mathscr{C}_3$) $s(n) \in \mathcal{S}$ for all n;

($\mathscr{C}_4$) $\kappa(s(n)) = \kappa(n)$ for all n;

($\mathscr{C}_5$) $s(n) \mid n$ for all $n \in \mathcal{S}$; in particular, $s(n) \leqslant n$.

Lemma 4.7. *If $\mathcal{W}_k \neq \varnothing$ and m_k is the least integer in $\mathcal{W}_k$, then $m_k \in \mathcal{Y}$.*

Proof. Clearly, $s(m_k) \in \mathcal{S}$ by ($\mathscr{C}_3$). Combining ($\mathscr{C}_4$) with (51) one sees that

$$F(s(n)) = F(n) \qquad \text{and} \qquad \omega(s(n)) = \omega(n) \qquad (n \in \mathbb{N}).$$

Then, using ($\mathscr{C}_5$) it follows that

$$F(s(m_k)) = F(m_k) \geqslant e^\gamma \log\log m_k \geqslant e^\gamma \log\log s(m_k),$$

which shows that $s(m_k) \in \mathcal{N}^\circ$. Finally, $s(m_k) \in \mathcal{V}_k$ since

$$\omega(s(m_k)) = \omega(m_k) \geqslant k.$$

Thus, we have shown that $s(m_k) \in \mathcal{S} \cap \mathcal{N}^\circ \cap \mathcal{V}_k = \mathcal{W}_k$. Since m_k is the *least* integer in $\mathcal{W}_k$, the equality $m_k = s(m_k)$ follows from ($\mathscr{C}_5$), hence $m_k \in \mathcal{Y}$. □

Next, for every integer $k \geqslant 0$ let

$$\mathcal{Z}_k = \big\{n \in \mathbb{N} \ : \ \Omega(n) = k\big\} \qquad \text{and} \qquad \mathcal{T}_k = \mathcal{N}^\circ \cap \mathcal{Y} \cap \mathcal{Z}_k.$$

Here, $\Omega(n)$ is the number of prime divisors of n, counted with multiplicity. Using Lemma 4.7 one sees that if $\mathcal{W}_\ell \neq \varnothing$ and m_ℓ is the least integer in $\mathcal{W}_\ell$, then $m_\ell \in \mathcal{T}_k$ for some $k \geqslant \ell$; in particular,

$$\bigcup_{k \geqslant \ell} \mathcal{T}_k = \varnothing \quad \Longrightarrow \quad \mathcal{W}_\ell = \varnothing.$$

As we mentioned earlier, in order to prove Theorem 4.1 it suffices to show that $\mathcal{W}_\ell = \varnothing$ for some ℓ, hence it is enough to show that $\mathcal{T}_k \neq \varnothing$ for at most finitely many integers $k \geqslant 0$.

When $\mathcal{T}_k \neq \varnothing$ we shall use the following notation. Let n_k denote the least integer in $\mathcal{T}_k$. Let $\widehat{p}_k$ be the largest prime $p \in \mathcal{P}$ that divides n_k, and put $\widehat{p}_k = 1$ if no such prime exists. Similarly, let $\widehat{q}_k$ be the largest prime $q \in \mathcal{Q}$ that divides n_k, and set $\widehat{q}_k = 1$ if no such prime exists. Finally, let

$$P_k^+ = \max\{\widehat{p}_k, \widehat{q}_k\} \qquad \text{and} \qquad P_k^- = \min\{\widehat{p}_k, \widehat{q}_k\}. \tag{52}$$

Note that P_k^+ is the largest prime factor of n_k.

Lemma 4.8. *Suppose $\mathcal{T}_k \neq \varnothing$:*

(*i*) *if $p \in \mathcal{P}$ with $p < \widehat{p}_k$, then $p \mid n_k$;*

(*ii*) *if $q \in \mathcal{Q}$ with $q < \widehat{q}_k$, then $q \mid n_k$.*

Proof. Suppose on the contrary that $p \in \mathcal{P}$ with $p < \widehat{p}_k$ and $p \nmid n_k$. Since $n_k = s(n_k)$ we can write $n_k = \widehat{p}_k m$ with $\widehat{p}_k \nmid m$. Put $n^* = pm$. Since $n_k \in \mathcal{N}^\circ$, $F(p) > F(\widehat{p}_k)$, and $n^* < n_k$, it follows that

$$F(n^*) = F(p)\,F(m) > F(\widehat{p}_k)\,F(m) = F(n_k) \geqslant e^\gamma \log\log n_k > e^\gamma \log\log n^*,$$

where we have used the fact that F is multiplicative; this shows that $n^* \in \mathcal{N}^\circ$. As $n_k \in \mathcal{Y}$, $(\mathscr{C}_1)$ implies that $n^* \in \mathcal{Y}$. Finally, since Ω is (completely) additive, we see that

$$\Omega(n^*) = \Omega(m) + 1 = \Omega(n_k) = k,$$

which shows that $n^* \in \mathcal{Z}_k$, and thus $n^* \in \mathcal{N}^\circ \cap \mathcal{Y} \cap \mathcal{Z}_k = \mathcal{T}_k$. But this is impossible since $n^* < n_k$ (the least number in $\mathcal{T}_k$), and this contradiction completes our proof of (i). Using $(\mathscr{C}_2)$, the proof of (ii) is similar; we omit the details. □

Lemma 4.9. *Suppose that $\mathcal{T}_k \neq \varnothing$ and $\widehat{p}_k < \widehat{q}_k$. Then there is at most one prime $p \in \mathcal{P}$ such that $\widehat{p}_k < p < \widehat{q}_k$.*

Proof. Suppose on the contrary that there are two primes $p_1, p_2 \in \mathcal{P}$ such that $\widehat{p}_k < p_1 < p_2 < \widehat{q}_k$. Since $n_k = s(n_k)$ we can write $n_k = \widehat{q}_k^{\,2} m$, and it is clear that $\gcd(m, p_1 p_2 \widehat{q}_k) = 1$. Put $n^* = p_1 p_2 m$. Since $n_k \in \mathcal{N}^\circ$, $F(p_1 p_2) > F(\widehat{q}_k^{\,2})$, and $n^* < n_k$, we have

$$F(n^*) = F(p_1 p_2)\,F(m) > F(\widehat{q}_k^{\,2})\,F(m) = F(n_k) \geqslant e^\gamma \log\log n_k > e^\gamma \log\log n^*,$$

which shows that $n^* \in \mathcal{N}^\circ$. As $n_k \in \mathcal{Y}$, $(\mathscr{C}_1)$ implies that $n^* \in \mathcal{Y}$. Finally, since

$$\Omega(n^*) = \Omega(m) + 2 = \Omega(n_k) = k,$$

we see that $n^* \in \mathcal{Z}_k$, and thus $n^* \in \mathcal{N}^\circ \cap \mathcal{Y} \cap \mathcal{Z}_k = \mathcal{T}_k$. But this is impossible since $n^* < n_k$, and this contradiction implies the result. □

Lemma 4.10. *Suppose that $\mathcal{T}_k \neq \varnothing$ and $\widehat{p}_k > \widehat{q}_k$. Let p be the largest prime in $\mathcal{P}$ that is less than $\widehat{p}_k$, and let q be the smallest prime in $\mathcal{Q}$ that is greater than $\widehat{q}_k$. Then $q > p/2$.*

Proof. Suppose on the contrary that $q \leqslant p/2$. Since $n_k = s(n_k)$ and $p \mid n_k$ (by Lemma 4.8) but $q \nmid n_k$ (since $q > \widehat{q}_k$), we can write $n_k = p\widehat{p}_k m$, where $\gcd(m, p\widehat{p}_k q) = 1$. Put $n^* = q^2 m$. As in the proofs of Lemmas 4.8 and 4.9, we see that $n^* \in \mathcal{Y} \cap \mathcal{Z}_k$. Since $p < \widehat{p}_k$ and $q \leqslant p/2$, we have

$$F(p\widehat{p}_k) = \frac{p\widehat{p}_k}{(p-1)(\widehat{p}_k - 1)} < \frac{p^2}{(p-1)^2} < \frac{q}{q-1} = F(q^2);$$

therefore,

$$F(n^*) = F(q^2)\, F(m) > F(p\widehat{p}_k)\, F(m) = F(n_k) \geqslant e^\gamma \log\log n_k > e^\gamma \log\log n^*,$$

which shows that $n^* \in \mathcal{N}^\circ$. Thus, $n^* \in \mathcal{N}^\circ \cap \mathcal{Y} \cap \mathcal{Z}_k = \mathcal{T}_k$. But this is impossible since $n^* < n_k$, and this contradiction implies the result. □

As mentioned above, in order to prove Theorem 4.1 it suffices to show that $\mathcal{T}_k \neq \varnothing$ for at most finitely many integers $k \geqslant 0$. Arguing by contradiction, we shall assume that the set

$$\mathcal{K} = \{k \geqslant 0 \ : \ \mathcal{T}_k \neq \varnothing\}$$

has infinitely many elements.

Since $\Omega(n_k) = k$, we see that $n_k \to \infty$ as $k \to \infty$ with $k \in \mathcal{K}$; using Lemma 4.6 it follows that $\omega(n_k) \to \infty$ as well, and therefore $P_k^+ \to \infty$.

We claim that

$$\widehat{p}_k \asymp \widehat{q}_k \qquad (k \in \mathcal{K}), \tag{53}$$

which by (52) is equivalent to

$$P_k^+ \asymp P_k^- \qquad (k \in \mathcal{K}). \tag{54}$$

To see this, we express $\mathcal{K}$ as a disjoint union $\mathcal{A} \cup \mathcal{B}$, where $\mathcal{A}$ [resp. $\mathcal{B}$] is the set of numbers $k \in \mathcal{K}$ for which $\widehat{p}_k < \widehat{q}_k$ [resp. $\widehat{p}_k > \widehat{q}_k$]. To prove (53) it suffices to show:

$(\mathscr{D}_1)$ $\quad \widehat{p}_k \gg \widehat{q}_k$ for all $k \in \mathcal{A}$;

$(\mathscr{D}_2)$ $\quad \widehat{p}_k \ll \widehat{q}_k$ for all $k \in \mathcal{B}$.

We use the following result, which is an easy consequence of the prime number theorem:

Lemma 4.11. *Let $c_{\mathcal{P}} = \overline{\delta}\,/\,\underline{\delta}$ and $c_{\mathcal{Q}} = (1 - \underline{\delta}\,)\,/\,\big(1 - \overline{\delta}\,\big)$. For every $\varepsilon > 0$ there is a number $x_0(\varepsilon)$ such that for all $x > x_0(\varepsilon)$:*

(*i*) *if p is the smallest prime in $\mathcal{P}$ greater than x, then $p \leqslant (c_{\mathcal{P}} + \varepsilon)\, x$;*

(*ii*) *if q is the smallest prime in $\mathcal{Q}$ greater than x, then $q \leqslant (c_{\mathcal{Q}} + \varepsilon)\, x$;*

(*iii*) *if p is the largest prime in $\mathcal{P}$ less than x, then $p \geqslant \big(c_{\mathcal{P}}^{-1} - \varepsilon\big)\, x$;*

(*iv*) *if q is the largest prime in $\mathcal{Q}$ less than x, then $q \geqslant \big(c_{\mathcal{Q}}^{-1} - \varepsilon\big)\, x$.*

To prove $(\mathscr{D}_1)$ we can assume that $\mathcal{A}$ is an infinite set. Let $k \in \mathcal{A}$, so that $\widehat{p}_k < \widehat{q}_k$. Since $\widehat{q}_k = P_k^+ \to \infty$ as $k \to \infty$ with $k \in \mathcal{A}$, the assertion $(\mathscr{D}_1)$ then follows from Lemmas 4.9 and 4.11.

To prove $(\mathscr{D}_2)$ we can assume that $\mathcal{B}$ is an infinite set. Let $k \in \mathcal{B}$, so that $\widehat{p}_k > \widehat{q}_k$. Let p, q be defined as in Lemma 4.10. Since $\widehat{p}_k = P_k^+ \to \infty$ as $k \to \infty$ with $k \in \mathcal{B}$, on combining Lemmas 4.10 and 4.11 it follows that

$$\widehat{p}_k \ll p \ll q \ll \widehat{q}_k,$$

which proves $(\mathscr{D}_2)$ and completes our proof of (53).

Next, for every $n \in \mathbb{N}$ let

$$\omega_{\mathcal{P}}(n) = \#\big\{p \in \mathcal{P} \ : \ p \mid n\big\} \qquad \text{and} \qquad \omega_{\mathcal{Q}}(n) = \#\big\{q \in \mathcal{Q} \ : \ q \mid n\big\}.$$

We claim that

$$\omega_{\mathcal{P}}(n_k) \asymp \omega_{\mathcal{Q}}(n_k) \qquad (k \in \mathcal{K}). \tag{55}$$

Indeed, by Lemma 4.8 it follows that $\omega_{\mathcal{P}}(n_k) = \pi_{\mathcal{P}}(\widehat{p}_k)$ and $\omega_{\mathcal{Q}}(n_k) = \pi_{\mathcal{Q}}(\widehat{q}_k)$. Therefore, using the prime number theorem together with (48), (49) and (53) we have

$$\omega_{\mathcal{P}}(n_k) = \pi_{\mathcal{P}}(\widehat{p}_k) \asymp \frac{\widehat{p}_k}{\log \widehat{p}_k} \asymp \frac{\widehat{q}_k}{\log \widehat{q}_k} \asymp \pi_{\mathcal{Q}}(\widehat{q}_k) = \omega_{\mathcal{Q}}(n_k),$$

which proves (55).

Finally, we need the following relation:

$$\log \kappa(n_k) \asymp \omega(n_k) \log \omega(n_k) \qquad (k \in \mathcal{K}). \tag{56}$$

To prove this, observe that the definition (52) and Lemma 4.8 together imply

$$\prod_{p \leqslant P_k^-} p \,\Big|\, \kappa(n_k) \qquad \text{and} \qquad \kappa(n_k) \,\Big|\, \prod_{p \leqslant P_k^+} p.$$

Consequently,

$$\sum_{p \leqslant P_k^-} \log p \leqslant \log \kappa(n_k) \leqslant \sum_{p \leqslant P_k^+} \log p,$$

and also

$$\pi(P_k^-) \leqslant \omega(n_k) \leqslant \pi(P_k^+).$$

By the prime number theorem, for either choice of the sign $\pm$ we have

$$\sum_{p\leqslant P_k^{\pm}} \log p \sim P_k^{\pm} \qquad \text{and} \qquad \pi(P_k^{\pm}) \sim \frac{P_k^{\pm}}{\log P_k^{\pm}} \qquad (k\to\infty,\ k\in\mathcal{K}),$$

therefore in view of (54) we see that

$$\log\kappa(n_k) \asymp P_k^{+} \qquad \text{and} \qquad \omega(n_k) \asymp \frac{P_k^{+}}{\log P_k^{+}}\,,$$

and (56) follows immediately.

Now we come to the heart of the argument. To complete the proof of Theorem 4.1, we seek a contradiction to our assumption that $\mathcal{K}$ is an infinite set. For this, it is enough to prove both of the following statements with a suitably chosen real number $\varepsilon > 0$:

($\mathscr{E}_1$) the inequality $n_k \leqslant \kappa(n_k)^{1+\varepsilon}$ holds for at most finitely many $k\in\mathcal{K}$;

($\mathscr{E}_2$) the inequality $n_k > \kappa(n_k)^{1+\varepsilon}$ holds for at most finitely many $k\in\mathcal{K}$.

In view of (55) and (56), there is a constant $C>1$ such that the inequalities

$$\omega_{\mathcal{P}}(n_k) \leqslant (C-1)\,\omega_{\mathcal{Q}}(n_k) \tag{57}$$

and

$$\log\kappa(n_k) \leqslant C\,\omega(n_k)\log\omega(n_k) \tag{58}$$

both hold if k is sufficiently large. Let C be fixed, and put $\varepsilon = C^{-3}$.

To prove ($\mathscr{E}_1$), we suppose on the contrary that $n_k \leqslant \kappa(n_k)^{1+\varepsilon}$ holds for infinitely many $k\in\mathcal{K}$. Let k be large, and put

$$r = \omega_{\mathcal{P}}(n_k) = \pi_{\mathcal{P}}(\widehat{p}_k) \qquad \text{and} \qquad s = \omega_{\mathcal{Q}}(n_k) = \pi_{\mathcal{Q}}(\widehat{q}_k)$$

By what we have already seen it is clear that $\min\{r,s\}\to\infty$ as $k\to\infty$ with $k\in\mathcal{K}$, thus by (57) we have

$$r \leqslant (C-1)s \tag{59}$$

if k is large enough. By Lemma 4.8 and the fact that $n_k\in\mathcal{Y}$, it follows that

$$n_k = \Bigg(\prod_{\substack{p\leqslant\widehat{p}_k\\ p\in\mathcal{P}}} p\Bigg)\Bigg(\prod_{\substack{q\leqslant\widehat{q}_k\\ q\in\mathcal{Q}}} q^2\Bigg) \qquad \text{and} \qquad \kappa(n_k) = \Bigg(\prod_{\substack{p\leqslant\widehat{p}_k\\ p\in\mathcal{P}}} p\Bigg)\Bigg(\prod_{\substack{q\leqslant\widehat{q}_k\\ q\in\mathcal{Q}}} q\Bigg).$$

Hence, our assumption that $n_k \leqslant \kappa(n_k)^{1+\varepsilon}$ implies that

$$\kappa(n_k) \geqslant \left(\frac{n_k}{\kappa(n_k)}\right)^{1/\varepsilon} = \Bigg(\prod_{\substack{q\leqslant\widehat{q}_k\\ q\in\mathcal{Q}}} q\Bigg)^{1/\varepsilon}. \tag{60}$$

If $\overline{p}_1, \overline{p}_2, \ldots$ is the sequence of consecutive prime numbers, then by the prime number theorem (and recalling our choice of ε) we derive that

$$\log \kappa(n_k) \geqslant C^3 \sum_{\substack{q \leqslant \widehat{q}_k \\ q \in \mathcal{Q}}} \log q \geqslant C^3 \sum_{p \leqslant \overline{p}_s} \log p \sim C^3 \overline{p}_s \sim C^3 s \log s$$

as $k \to \infty$ with $k \in \mathcal{K}$. On the other hand, using (58), (59) and the fact that $\omega(n_k) = r + s$, it follows that

$$\log \kappa(n_k) \leqslant C(r+s)\log(r+s) \leqslant C^2 s \log(Cs) \sim C^2 s \log s.$$

Since $C^3 > C^2$, these two inequalities for $\log \kappa(n_k)$ lead to a contradiction once k is sufficiently large, and this completes the proof of $(\mathscr{E}_1)$.

To prove $(\mathscr{E}_2)$ we use some ideas from Choie *et al* [15]. Suppose that $n_k > \kappa(n_k)^{1+\varepsilon}$, and put $t = \omega(n_k)$. We claim that either

$$\sum_{p \leqslant \overline{p}_t} \log p < (1+\varepsilon)^{-1/2}\, \overline{p}_t, \tag{61}$$

or

$$\overline{p}_t \leqslant \exp\big(2/\log(1+\varepsilon)\big). \tag{62}$$

Assuming the claim, it is easy to see that $\omega(n_k)$ is bounded above by a constant K that depends only on ε. By Lemma 4.6, n_k can take only finitely many distinct values, which implies $(\mathscr{E}_2)$.

To prove the claim, assume that (61) fails:

$$\log(\overline{p}_1 \cdots \overline{p}_t) = \sum_{p \leqslant \overline{p}_t} \log p \geqslant (1+\varepsilon)^{-1/2}\, \overline{p}_t.$$

Thanks to Rosser and Schoenfeld [52] it is known that

$$\prod_{p \leqslant x} \frac{p}{p-1} \leqslant e^{\gamma} \left(\log x + \frac{1}{\log x} \right) \qquad (x > 1).$$

Therefore, taking $x = \overline{p}_t$ and noting that $\kappa(n_k) \geqslant \overline{p}_1 \cdots \overline{p}_t$, we derive that

$$\begin{aligned} e^{\gamma} \left(\log \overline{p}_t + \frac{1}{\log \overline{p}_t} \right) &\geqslant \prod_{j=1}^{t} \frac{\overline{p}_j}{\overline{p}_j - 1} \geqslant \frac{n_k}{\varphi(n_k)} \geqslant e^{\gamma} \log\log n_k \\ &> e^{\gamma} \log\left((1+\varepsilon)\log \kappa(n_k)\right) \\ &\geqslant e^{\gamma} \log\left((1+\varepsilon)\log(\overline{p}_1 \cdots \overline{p}_t)\right) \\ &\geqslant e^{\gamma} \log\left((1+\varepsilon)^{1/2}\, \overline{p}_t\right) = e^{\gamma}\left(\log \overline{p}_t + 0.5 \log(1+\varepsilon)\right); \end{aligned}$$

that is,

$$\frac{1}{\log \overline{p}_t} \geqslant 0.5 \log(1+\varepsilon),$$

which is equivalent to (62). This proves the claim and completes our proof of Theorem 4.1.

4.3 Proof of Theorem 4.4

We continue to use the notation of the previous section, but we focus on the special case that

$$\mathcal{P} = \big\{p \in \mathbb{P} \ : \ p \equiv 1 \pmod 4\big\} \cup \{2\},$$
$$\mathcal{Q} = \big\{q \in \mathbb{P} \ : \ q \equiv 3 \pmod 4\big\}.$$

Note that the corresponding set $\mathcal{S}$ contains every natural number that can be expressed as a sum of two squares. As before, we write

$$\mathcal{T}_k = \big\{n \in \mathbb{N} \ : \ F(n) \geqslant e^\gamma \log\log n, \ n = s(n), \text{ and } \Omega(n) = k\big\}$$

and put

$$\mathcal{K} = \{k \geqslant 0 \ : \ \mathcal{T}_k \neq \varnothing\}.$$

Lemma 4.12. *If $k \in \mathcal{K}$, then $P_k^- < 50000$.*

Proof. For every real number $x \geqslant 10$, let

- $g_{\mathcal{P}}(x)$ = the smallest prime in $\mathcal{P}$ greater than x;
- $g_{\mathcal{Q}}(x)$ = the smallest prime in $\mathcal{Q}$ greater than x;
- $\ell_{\mathcal{P}}(x)$ = the largest prime in $\mathcal{P}$ less than x;
- $\ell_{\mathcal{Q}}(x)$ = the largest prime in $\mathcal{Q}$ less than x.

Also, put

$$\vartheta_{\mathcal{P}}(x) = \sum_{\substack{p \leqslant x \\ p \in \mathcal{P}}} \log p \qquad \text{and} \qquad \vartheta_{\mathcal{Q}}(x) = \sum_{\substack{q \leqslant x \\ q \in \mathcal{Q}}} \log q.$$

Using the explicit bounds of Theorems 1 and 2 of Ramaré and Rumely [50], we see that the inequalities

$$0.49\, x < \vartheta_{\mathcal{P}}(x) < 0.51\, x \qquad \text{and} \qquad 0.49\, x < \vartheta_{\mathcal{Q}}(x) < 0.51\, x. \tag{63}$$

hold for all $x \geqslant 45000$ (note that $\vartheta_{\mathcal{P}}(x) = \log 2 + \theta(x; 4, 1)$ and $\vartheta_{\mathcal{Q}}(x) = \theta(x; 4, 3)$ in the notation of [50]). Consequently, for any $x \geqslant 50000$ we have

$$\tfrac{49}{51}\, x < \ell_{\mathcal{P}}(x) < x < g_{\mathcal{P}}(x) < \tfrac{51}{49}\, x$$

and

$$\tfrac{49}{51}\, x < \ell_{\mathcal{Q}}(x) < x < g_{\mathcal{Q}}(x) < \tfrac{51}{49}\, x.$$

Now suppose that $P_k^- \geqslant 50000$. Using Lemma 4.9 and the preceding bounds we have

$$\widehat{q}_k < g_{\mathcal{P}}(g_{\mathcal{P}}(\widehat{p}_k)) < \left(\tfrac{51}{49}\right)^2 \widehat{p}_k.$$

On the other hand, by Lemma 4.10 we have

$$\tfrac{51}{49}\,\widehat{q}_k > g_{\mathcal{Q}}(\widehat{q}_k) > \tfrac{1}{2}\,\ell_{\mathcal{P}}(\widehat{p}_k) > \tfrac{49}{102}\,\widehat{p}_k.$$

Hence, it follows that

$$0.92\,\widehat{q}_k < \widehat{p}_k < 2.2\,\widehat{q}_k. \tag{64}$$

By Lemma 4.8 it is clear that

$$\log \kappa(n_k) = \sum_{\substack{p \leqslant \widehat{p}_k \\ p \in \mathcal{P}}} \log p + \sum_{\substack{q \leqslant \widehat{q}_k \\ q \in \mathcal{Q}}} \log q = \vartheta_{\mathcal{P}}(\widehat{p}_k) + \vartheta_{\mathcal{Q}}(\widehat{q}_k).$$

On the other hand, arguing as in the proof of Theorem 4.1, it follows from (60) that

$$\log \kappa(n_k) \geqslant \varepsilon^{-1} \vartheta_{\mathcal{Q}}(\widehat{q}_k)$$

if $\varepsilon > 0$ is fixed and $n_k \leqslant \kappa(n_k)^{1+\varepsilon}$. Combining the two preceding results with (63), we see that

$$0.51\,(\widehat{p}_k + \widehat{q}_k) \geqslant \vartheta_{\mathcal{P}}(\widehat{p}_k) + \vartheta_{\mathcal{Q}}(\widehat{q}_k) \geqslant \varepsilon^{-1} \vartheta_{\mathcal{Q}}(\widehat{q}_k) \geqslant 0.49\,\varepsilon^{-1} \widehat{q}_k$$

since $P_k^- \geqslant 50000$; taking into account (64), we further have

$$0.51\,(1 + 2.2)\,\widehat{q}_k \geqslant 0.51\,(\widehat{p}_k + \widehat{q}_k) \geqslant 0.49\,\varepsilon^{-1} \widehat{q}_k,$$

which implies that $\varepsilon \geqslant 0.3002$. Thus, for the smaller value $\varepsilon = 0.3$, we see that the condition $n_k \leqslant \kappa(n_k)^{1.3}$ implies $P_k^- < 50000$.

On the other hand, if $n_k > \kappa(n_k)^{1.3}$, we put $t = \omega(n_k)$ as in the proof of Theorem 4.1. Since $\varepsilon = 0.3$, we derive from (61) and (62) that either

$$\vartheta(\overline{p}_t) = \sum_{p \leqslant \overline{p}_t} \log p < (1.3)^{-1/2}\,\overline{p}_t < 0.88\,\overline{p}_t, \tag{65}$$

or

$$\overline{p}_t \leqslant \exp(2/\log 1.3) < 2045.$$

Using again Theorems 1 and 2 of Ramaré and Rumely [50] (see also [52]), it is easy to see that the inequality (65) implies $\overline{p}_t < 300$, hence the inequality $\overline{p}_t < 2045$ holds in both cases. It follows that $t < 310$, and therefore,

$$\min\{\pi_{\mathcal{P}}(\widehat{p}_k), \pi_{\mathcal{Q}}(\widehat{q}_k)\} = \min\{\omega_{\mathcal{P}}(n_k), \omega_{\mathcal{Q}}(n_k)\} \leqslant \omega(n_k) = t < 310,$$

which implies that $P_k^- < 5000$. This completes the proof. □

Corollary 4.13. *If $k \in \mathcal{K}$, then $k < 10000$.*

Proof. For any $k \in \mathcal{K}$ we have

$$k = \Omega(n_k) = \omega_{\mathcal{P}}(n_k) + 2\,\omega_{\mathcal{Q}}(n_k) = \pi_{\mathcal{P}}(\widehat{p}_k) + 2\,\pi_{\mathcal{Q}}(\widehat{q}_k).$$

If $P_k^- = \widehat{p}_k$ (i.e., $\widehat{p}_k < \widehat{q}_k$), then by Lemmas 4.9 and 4.12 it follows that

$$\begin{aligned} k &\leqslant \max_{p<50000} \big\{\pi_{\mathcal{P}}(p) + 2\,\pi_{\mathcal{Q}}\big(g_{\mathcal{P}}(g_{\mathcal{P}}(p))\big)\big\} \\ &\leqslant \pi_{\mathcal{P}}(50000) + 2\,\pi_{\mathcal{Q}}\big(g_{\mathcal{P}}(g_{\mathcal{P}}(50000))\big) = 7718. \end{aligned}$$

If $P_k^- = \widehat{q}_k$ (i.e., $\widehat{q}_k < \widehat{p}_k$), then by Lemmas 4.10 and 4.12 it follows that

$$\begin{aligned} k &\leqslant \max_{q<50000} \max_{\substack{p\in\mathbb{P} \\ \ell_{\mathcal{P}}(p)<2g_{\mathcal{Q}}(q)}} \{\pi_{\mathcal{P}}(p) + 2\,\pi_{\mathcal{Q}}(q)\} \\ &= \max_{q<50000} \max_{\substack{p\in\mathbb{P} \\ \ell_{\mathcal{P}}(p)<2g_{\mathcal{Q}}(q)}} \{1 + \pi_{\mathcal{P}}(\ell_{\mathcal{P}}(p)) + 2\,\pi_{\mathcal{Q}}(q)\} \\ &\leqslant \max_{q<50000} \{1 + \pi_{\mathcal{P}}(2\,g_{\mathcal{Q}}(q)) + 2\,\pi_{\mathcal{Q}}(q)\} \\ &\leqslant 1 + \pi_{\mathcal{P}}(2\,g_{\mathcal{Q}}(50000)) + 2\,\pi_{\mathcal{Q}}(50000) = 9951. \end{aligned}$$

The result follows. □

Now let $\overline{\overline{p}}_1, \overline{\overline{p}}_2, \ldots$ be the sequence of consecutive primes in $\mathcal{P}$, and let $\overline{\overline{q}}_1, \overline{\overline{q}}_2, \ldots$ be the consecutive primes in $\mathcal{Q}$. For any integers $r, s \geqslant 0$, let

$$N_{r,s} = \Big(\prod_{i=1}^{r} \overline{\overline{p}}_i\Big)\Big(\prod_{j=1}^{s} \overline{\overline{q}}_j^{\,2}\Big).$$

It is easy to see that $N_{r,s} \in \mathcal{Y}$ for all $r, s \geqslant 0$, and for every $k \in \mathcal{K}$ one has

$$n_k = N_{r,s}, \qquad \widehat{p}_k = \overline{\overline{p}}_r, \qquad \widehat{q}_k = \overline{\overline{q}}_s \qquad \text{and} \qquad k = r + 2s,$$

where $r = \omega_{\mathcal{P}}(n_k)$ and $s = \omega_{\mathcal{Q}}(n_k)$. By a straightforward computation, one verifies the following:

Lemma 4.14. *If $r, s \geqslant 0$, then $N_{r,s} \in \mathcal{N}^\circ$ if and only if the pair (r, s) lies in the set*

$$\begin{aligned} \mathcal{X} = \big\{&(0,0),(1,0),(0,1),(2,0),(1,1),(2,1),(1,2),(3,1),(2,2),(4,1), \\ &(3,2),(2,3),(4,2),(3,3),(5,2),(4,3),(3,4),(5,3),(4,4),(6,3), \\ &(5,4),(4,5),(7,3),(6,4),(5,5),(7,4),(6,5),(7,5),(8,5)\big\}. \end{aligned}$$

We remark that, in view of Corollary 4.13, it suffices to check the condition $N_{r,s} \in \mathcal{N}^\circ$ only for those pairs (r, s) with $r + 2s < 10000$.

Corollary 4.15. *If $k \in \mathcal{K}$, then $k \leqslant 18$.*

Corollary 4.16. *If $n \in \mathcal{S} \cap \mathcal{N}^\circ$, $r = \omega_{\mathcal{P}}(n)$ and $s = \omega_{\mathcal{Q}}(n)$, then $(r,s) \in \mathcal{X}$. In particular, $\omega(n) \leqslant 13$.*

Proof. Since

$$F(N_{r,s}) = \Big(\prod_{i=1}^{r} \frac{\overline{\overline{p}}_i}{\overline{\overline{p}}_i - 1}\Big)\Big(\prod_{j=1}^{s} \frac{\overline{\overline{q}}_j}{\overline{\overline{q}}_j - 1}\Big) \geqslant \Big(\prod_{\substack{p \,|\, n \\ p \in \mathcal{P}}} \frac{p}{p-1}\Big)\Big(\prod_{\substack{q \,|\, n \\ q \in \mathcal{Q}}} \frac{q}{q-1}\Big) = F(n)$$

and

$$n \geqslant s(n) = \Big(\prod_{\substack{p \,|\, n \\ p \in \mathcal{P}}} p\Big)\Big(\prod_{\substack{q \,|\, n \\ q \in \mathcal{Q}}} q^2\Big) \geqslant \Big(\prod_{i=1}^{r} \overline{\overline{p}}_i\Big)\Big(\prod_{j=1}^{s} \overline{\overline{q}}_j^{\,2}\Big) = N_{r,s},$$

we have

$$F(N_{r,s}) \geqslant F(n) \geqslant e^{\gamma} \log\log n \geqslant e^{\gamma} \log\log N_{r,s},$$

which shows that $N_{r,s} \in \mathcal{N}^\circ$. □

We now turn to a description of our method for generating the elements of $\mathcal{S} \setminus \mathcal{N} = \mathcal{S} \cap \mathcal{N}^\circ$. For any given $n \in \mathcal{S} \cap \mathcal{N}^\circ$ with $r = \omega_{\mathcal{P}}(n)$ and $s = \omega_{\mathcal{Q}}(n)$, we can write

$$s(n) = p_1 \cdots p_r \, q_1^2 \cdots q_s^2,$$

where $p_1 < \cdots < p_r$ are primes in $\mathcal{P}$ and $q_1 < \cdots < q_s$ are primes in $\mathcal{Q}$. For fixed $i = 1, \ldots, r$, let γ_i be the largest non-negative integer such that the number

$$\Big(\prod_{\ell=1}^{i-1} \overline{\overline{p}}_\ell\Big)\Big(\prod_{\ell=i}^{r} \overline{\overline{p}}_{\ell+\gamma_i}\Big)\Big(\prod_{j=1}^{s} \overline{\overline{q}}_j^{\,2}\Big)$$

lies in $\mathcal{N}^\circ$, which exist by Lemma 4.6. Using an argument similar to that in the proof of Lemma 4.8, one can deduce that

$$\overline{\overline{p}}_i \leqslant p_i \leqslant \overline{\overline{p}}_{i+\gamma_i} \qquad (i = 1, \ldots, r). \tag{66}$$

Similarly, for fixed $j = 1, \ldots, s$, let δ_j be the largest non-negative integer such that the number

$$\Big(\prod_{i=1}^{r} \overline{\overline{p}}_i\Big)\Big(\prod_{\ell=1}^{j-1} \overline{\overline{q}}_\ell^{\,2}\Big)\Big(\prod_{\ell=j}^{s} \overline{\overline{q}}_{\ell+\delta_j}^{\,2}\Big)$$

lies in $\mathcal{N}^\circ$. Then,

$$\overline{\overline{q}}_j \leqslant q_j \leqslant \overline{\overline{q}}_{j+\gamma_j} \qquad (j = 1, \ldots, s). \tag{67}$$

Therefore, for fixed $(r,s) \in \mathcal{X}$, if $n \in \mathcal{S} \cap \mathcal{N}^\circ$ with $r = \omega_{\mathcal{P}}(n)$ and $s = \omega_{\mathcal{Q}}(n)$, then the number $s(n)$ must lie in the finite set $\mathcal{A}_{r,s}$ of integers of the form

$$m = p_1 \cdots p_r \, q_1^2 \cdots q_s^2, \tag{68}$$

where $p_1 < \cdots < p_r$ are primes in $\mathcal{P}$, $q_1 < \cdots < q_s$ are primes in $\mathcal{Q}$, the primes p_i and q_j satisfy the bounds (66) and (67), and $m \in \mathcal{N}^\circ$. The set $\mathcal{A}_{r,s}$ can be explicitly determined by a numerical computation, and we obtain a finite list of "admissible" values for the quantity $s(n)$.

To determine explicitly all of the numbers $n \in \mathcal{S} \cap \mathcal{N}^\circ$ with $r = \omega_{\mathcal{P}}(n)$ and $s = \omega_{\mathcal{Q}}(n)$, for every $m \in \mathcal{A}_{r,s}$ we need to find all such numbers for which $s(n) = m$. To do this, factor m as in (68). For fixed $i = 1, \ldots, r$, let α_i be the largest integer such that the number $mp_i^{\alpha_i - 1}$ lies in $\mathcal{N}^\circ$. Similarly, for fixed $j = 1, \ldots, s$, let β_j be the largest integer such that the number $mq_j^{\beta_j - 1}$ lies in $\mathcal{N}^\circ$. Put

$$M = m \cdot p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1} q_1^{\beta_1 - 1} \cdots q_s^{\beta_s - 1}.$$

Then, it is easy to see that $m \mid n$ and $n \mid M$ for any $n \in \mathcal{S} \cap \mathcal{N}^\circ$ such that $s(n) = m$. Hence, n can take only finitely many values which can be determined explicitly for each $m \in \mathcal{A}_{r,s}$.

For example, taking $r = s = 2$ we find that

$$\{4410, 8820, 10890, 13230, 17640, 21780, 22050, 26460, 30870, 35280, 39690,$$
$$44100, 52920, 61740, 66150, 70560, 79380, 88200, 92610, 105840, 110250\}$$

is a complete list of the numbers $n \in \mathcal{S} \setminus \mathcal{N}$ with $\omega_{\mathcal{P}}(n) = \omega_{\mathcal{Q}}(n) = 2$. Examining the lists generated as (r,s) varies over the pairs in $\mathcal{X}$, we are lead to the statement of Theorem 4.4.

4.4 Evaluation of $\overline{\lim}_{n \in S} \frac{n}{\varphi(n) \log\log n}$ and $\overline{\lim}_{n \in S} \frac{\sigma(n)}{n \log\log n}$

We conclude the manuscript by giving two propositions and two corollaries that yield the analogue of the work of Landau [36] and Gronwall [23] for any set $\mathcal{S}$ of the form (50) and for the set of natural numbers equal to a sum of two squares. In fact, Corollary 4.19 shows that Theorem 4.1 is nontrivial in the sense that $F(n)/\log\log n$ cannot be bounded away from e^γ by any positive constant for all large $n \in \mathcal{S}$. We will use the notation $f(n) = o(g(n))$ to mean that $\lim_{n \to \infty} f(n)/g(n) = 0$.

Proposition 4.17. *Let $\{a_n\}$ be an infinite sequence of positive integers such that if we write $a_n = \prod_p p^{v(p,n)}$ we have:*

(*i*) $\kappa(a_n) = \prod_{p \leqslant n} p$ (*i.e.*, $v(p,n) = 0 \iff p > n$);

(*ii*) $a_n = \exp(n^{1+o(1)})$;

(*iii*) $\lim_{n\to\infty} v(p,n) = \infty$ *for each* p.

Then,

$$\lim_{n\to\infty} \frac{\sigma(a_n)}{a_n \log\log a_n} = e^{\gamma}.$$

Proof. For all $n \geqslant 1$, let

$$b_n = \prod_{p \leqslant n} p \qquad \text{and} \qquad c_n = \frac{\sigma(a_n)}{a_n}\,\frac{\varphi(b_n)}{b_n},$$

and observe that (*i*) implies

$$c_n = \left(\prod_{p\leqslant n} \frac{p^{v(p,n)+1}-1}{p^{v(p,n)}(p-1)}\right)\left(\prod_{p\leqslant n}\frac{p-1}{p}\right) = \prod_{p\leqslant n}\left(1-\frac{1}{p^{v(p,n)+1}}\right).$$

Since $v(p,n)+1 \geqslant 2$ for every prime $p \leqslant n$, we have for any $m \leqslant n$:

$$1 \geqslant c_n > \prod_{p\leqslant m}\left(1-\frac{1}{p^{v(p,n)+1}}\right)\prod_{p>m}\left(1-\frac{1}{p^2}\right).$$

Using (*iii*) we have for every fixed integer m:

$$1 \geqslant \varlimsup_{n\to\infty} c_n \geqslant \varliminf_{n\to\infty} c_n \geqslant \prod_{p>m}\left(1-\frac{1}{p^2}\right).$$

The product on the right tends to one as $m \to \infty$, hence $\lim_{n\to\infty} c_n = 1$; therefore,

$$\lim_{n\to\infty}\frac{\sigma(a_n)}{a_n\log n} = \lim_{n\to\infty}\frac{b_n}{\varphi(b_n)\log n}.$$

Our assumption (*ii*) implies that $\log\log a_n = (1+o(1))\log n$, and using Mertens' theorem (see, for example, [52]) we have

$$\frac{\varphi(b_n)}{b_n} = \prod_{p\leqslant n}\left(1-\frac{1}{p}\right) = (1+o(1))\,\frac{e^{-\gamma}}{\log n},$$

and the result follows. □

Using similar ideas (and an easier argument) one can obtain the following analogue of Proposition 4.17 for the Euler totient function:

Proposition 4.18. *Let* $\{a_n\}$ *be an infinite sequence of positive integers such that:*

(*i*) $\kappa(a_n) = \prod_{p \leqslant n} p$;

(*ii*) $a_n = \exp(n^{1+o(1)})$.

Then,

$$\lim_{n\to\infty} \frac{a_n}{\varphi(a_n)\log\log a_n} = e^\gamma.$$

Corollary 4.19. *For any set $\mathcal{S}$ defined by* (50)*, we have*

$$\overline{\lim_{n\in\mathcal{S}}} \frac{\sigma(n)}{n\log\log n} = \overline{\lim_{n\in\mathcal{S}}} \frac{n}{\varphi(n)\log\log n} = e^\gamma.$$

Proof. Since

$$\overline{\lim_{n\to\infty}} \frac{\sigma(n)}{n\log\log n} = \overline{\lim_{n\to\infty}} \frac{n}{\varphi(n)\log\log n} = e^\gamma$$

by [23] and [36], respectively, it suffices to show that there is a sequence $\{a_n\}$ in $\mathcal{S}$ such that

$$\lim_{n\to\infty} \frac{\sigma(a_n)}{a_n\log\log a_n} = \lim_{n\to\infty} \frac{a_n}{\varphi(a_n)\log\log a_n} = e^\gamma.$$

Let $a_1 = 1$, and for every integer $n \geqslant 2$, let

$$b_n = \prod_{p\leqslant n} p, \qquad d_n = \left\lfloor n^{(\log n)^{-1/2}} \right\rfloor \qquad \text{and} \qquad a_n = b_n^{d_n}.$$

It is easy to see that $d_n \geqslant 2$ for $n \geqslant 2$, $d_n = n^{o(1)}$, and d_n tends to infinity with n. Clearly, $a_n \in \mathcal{S}$ for all $n \geqslant 1$, and by the Prime Number Theorem in the form $\sum_{p\leqslant x} \log p = x(1+o(1))$ as $x \to \infty$ we see that

$$\log a_n = d_n \log b_n = n^{o(1)} \sum_{p\leqslant n} \log p = n^{1+o(1)} \qquad (n \to \infty).$$

The sequence $\{a_n\}$ therefore satisfies the hypotheses of Propositions 4.17 and 4.18, and the result follows. □

Corollary 4.20. *We have*

$$\overline{\lim_{n=a^2+b^2}} \frac{\sigma(n)}{n\log\log n} = \overline{\lim_{n=a^2+b^2}} \frac{n}{\varphi(n)\log\log n} = e^\gamma.$$

Proof. Defining a_n for all $n \geqslant 1$ as in the proof of Corollary 4.19, it is easy to see that the sequence $\{a_n^2\}$ satisfies the hypotheses of Propositions 4.17 and 4.18; it follows that

$$\overline{\lim_{n=a^2}} \frac{\sigma(n)}{n\log\log n} = \overline{\lim_{n=a^2}} \frac{n}{\varphi(n)\log\log n} = e^\gamma,$$

and this implies the stated result. □

Part 5

Primitive characters and the Riemann Hypothesis

5.1 Introduction

For any natural number n, let $\mathcal{X}_n$ be the set of Dirichlet characters modulo n, and let $\mathcal{X}'_n$ be the subset of *primitive* characters in $\mathcal{X}_n$.

The purpose of the present note is to establish a connection between the *classical* Riemann hypothesis and the collection of sets $\{\mathcal{X}'_n : n \in \mathbb{N}\}$. Our work is motivated by and relies on the 1983 paper of J.-L. Nicolas [43] in which a relation is established between the Riemann hypothesis and certain values of $\varphi(n)$; see also [51].

Theorem 5.1. *For every $k \geqslant 1$, let n_k be the product of the first k primes. Let C_2 be the twin prime constant.*

(*i*) *If the Riemann hypothesis is true, then the inequality*

$$|\mathcal{X}'_{2n_k}| \leqslant C_2\, e^{-\gamma}\, \frac{\varphi(2n_k)}{\log\log(2n_k)} \tag{69}$$

holds for all $k \geqslant 1$.

(*ii*) *If the Riemann hypothesis is false, then there are infinitely many k for which* (69) *holds and infinitely many k for which it fails to hold.*

We recall that

$$C_2 = \prod_{p>2} \frac{p(p-2)}{(p-1)^2} = 0.6601618158\cdots .$$

To prove the theorem, we study the ratios

$$\rho(n) = \frac{|\mathcal{X}'_n|}{|\mathcal{X}_n|} \qquad (n \in \mathbb{N}).$$

Note that $\rho(n)$ is the *proportion* of Dirichlet characters modulo n that are primitive characters. Since $\rho(n) \leqslant 1$ for all $n \in \mathbb{N}$, and $\rho(p) = 1 - 1/(p-1)$ for every prime p, it is clear that

$$\overline{\lim_{n\to\infty}}\, \rho(n) = 1.$$

As for the minimal order, we shall prove the following:

$$\varliminf_{\substack{n\to\infty \\ n\not\equiv 2 \,(\mathrm{mod}\, 4)}} \rho(n)\log\log n = C_2\, e^{-\gamma}. \tag{70}$$

Note that natural numbers $n \equiv 2 \pmod 4$ are excluded since $\rho(n) = 0$ for those numbers; see (74) below.

In Section 5.2 we show that the inequalities

$$\rho(2n_k)\log\log(2n_k) \leqslant \rho(n)\log\log n \qquad (n \not\equiv 2 \,(\mathrm{mod}\, 4),\ \omega(n) = k) \tag{71}$$

hold for every fixed $k > 1$, where $\omega(n)$ is the number of distinct prime divisors of n, and we also show that

$$\lim_{k\to\infty} \rho(2n_k)\log\log(2n_k) = C_2\, e^{-\gamma}. \tag{72}$$

Clearly, (70) is an immediate consequence of (71) and (72).

Since $|\mathcal{X}_n| = \varphi(n)$ for all $n \in \mathbb{N}$, the inequality (69) is clearly equivalent to

$$\rho(2n_k)\log\log(2n_k) \leqslant C_2\, e^{-\gamma}. \tag{73}$$

In Section 5.3 we study this inequality using techniques and results from [43], and these investigations lead to the statement of Theorem 5.1.

5.2 Small values of $\rho(n)$

The cardinality of $\mathcal{X}_n$ is $\varphi(n)$, and that of $\mathcal{X}'_n$ is

$$|\mathcal{X}'_n| = n \prod_{p\,\|\,n} \left(1 - \frac{2}{p}\right) \prod_{p^2\,|\,n} \left(1 - \frac{1}{p}\right)^2$$

(see, for example, [42, § 9.1]); hence, it follows that

$$\rho(n) = \frac{\varphi(n)}{n} \prod_{p\,\|\,n} \frac{p(p-2)}{(p-1)^2} \qquad (n \in \mathbb{N}). \tag{74}$$

Turning to the proof of (71), let $k > 1$ be fixed, and denote by $\mathcal{S}$ the set of integers $n \not\equiv 2 \pmod 4$ with $\omega(n) = k$. Let $p_1, p_2, \ldots$ be the sequence of consecutive prime numbers. For each integer $j \in \{0, \ldots, k\}$, let $\mathcal{S}_j$ be the set of numbers $n \in \mathcal{S}$ that have precisely j distinct prime divisors larger than p_k. Since $\mathcal{S}$ is the union of the sets $\{\mathcal{S}_j\}$, to prove (71) it suffices to show that the inequalities

$$\rho(2n_k)\log\log(2n_k) \leqslant \rho(n)\log\log n \qquad (n \in \mathcal{S}_j) \tag{75}$$

hold for every fixed $j \in \{0, \dots, k\}$.

For any $n \in \mathcal{S}_0$ we can write $n = 2p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with each $\alpha_j \geqslant 1$. Using (74) and the fact that $2n_k = 2p_1 \cdots p_k$ we have

$$\rho(2n_k) = \rho(n) \prod_{\substack{j=2 \\ (\alpha_j \geqslant 2)}}^{k} \frac{p_j(p_j-2)}{(p_j-1)^2} \leqslant \rho(n).$$

Since $2n_k \leqslant n$ we also have $\log\log(2n_k) \leqslant \log\log n$, and (75) follows for $j = 0$.

Proceeding by induction, let us suppose that (75) has been established for some $j \in \{0, \dots, k-1\}$. If n' is an arbitrary element of $\mathcal{S}_{j+1}$, then $q \mid n'$ for some prime $q > p_k$; note that $q \geqslant 5$ since $k > 1$. Writing $n' = q^\alpha m$ with $q \nmid m$, we have $\omega(m) = k-1$, hence for at least one index $i \in \{1, \dots, k\}$ the prime p_i does not divide m. Put $n = p_i^\beta m$, where $\beta = 2$ if $p_i = 2$ and $\beta = 1$ otherwise. Clearly, $n \in \mathcal{S}_j$. Also, $n \leqslant n'$ since $q > \max\{p_i, 2^2\}$, and thus $\log\log n \leqslant \log\log n'$. Finally, using (74) we see that

$$\frac{\rho(n')}{\rho(m)} = \begin{cases} 1 - 1/(q-1) & \text{if } \alpha = 1, \\ 1 - 1/q & \text{if } \alpha \geqslant 2, \end{cases}$$

and

$$\frac{\rho(n)}{\rho(m)} = \begin{cases} 1 - 1/(p_i-1) & \text{if } \beta = 1, \\ 1/2 & \text{if } \beta = 2. \end{cases}$$

As $q > p_i$, we have $\rho(n) \leqslant \rho(n')$ in all cases. Putting everything together, we see that

$$\rho(2n_k)\log\log(2n_k) \leqslant \rho(n)\log\log n \leqslant \rho(n')\log\log n'.$$

Since $n' \in \mathcal{S}_{j+1}$ is arbitrary, we obtain (75) with j replaced by $j+1$, which completes the induction and finishes our proof of (71).

Next, we turn to the proof of (72). Using the Prime Number Theorem in the form

$$\log n_k = \sum_{p \leqslant p_k} \log p = (1 + o(1))p_k \qquad (k \to \infty)$$

together with Mertens' theorem (see [42, Theorem 2.7(e)]), it is easy to see that

$$\lim_{k\to\infty} \left\{ \log\log(2n_k) \prod_{p \leqslant p_k} \left(1 - \frac{1}{p}\right) \right\} = e^{-\gamma}. \tag{76}$$

Also,

$$\lim_{k\to\infty} \prod_{2 < p \leqslant p_k} \frac{p(p-2)}{(p-1)^2} = \lim_{k\to\infty} C_2 \prod_{p > p_k} \left(1 + \frac{1}{p(p-2)}\right) = C_2. \tag{77}$$

By (74) we have

$$\rho(2n_k) = \prod_{p \leqslant p_k} \left(1 - \frac{1}{p}\right) \prod_{2 < p \leqslant p_k} \frac{p(p-2)}{(p-1)^2} \qquad (k \geqslant 1),$$

and thus (72) is an immediate consequence of (76) and (77).

5.3 Proof of Theorem 5.1

As in [43, Théorème 3] we put

$$f(x) = e^{\gamma} \log \vartheta(x) \prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) \qquad (x \geqslant 2),$$

where $\vartheta(x) = \sum_{p \leqslant x} \log p$ is the Chebyshev ϑ-function. For our purposes, it is convenient to define

$$g(x) = e^{\gamma} \log\left(\vartheta(x) + \log 2\right) \prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) \prod_{p > x} \left(1 + \frac{1}{p(p-2)}\right) \qquad (x \geqslant 2),$$

This definition is motivated by the fact that

$$g(p_k) = C_2^{-1} e^{\gamma} \rho(2n_k) \log\log(2n_k) \qquad (k \geqslant 1).$$

As mentioned earlier, the inequalities (69) and (73) are equivalent, and (73) is clearly equivalent to

$$\log g(p_k) \leqslant 0.$$

Thus, to prove Theorem 5.1 it suffices to study the sign of $\log g(x)$.

By the trivial inequality $\log(1+t) \leqslant t$ for all $t > -1$ and the fact that $g(x) > f(x)$ for all $x \geqslant 2$, it is easy to see that

$$0 < \log \frac{g(x)}{f(x)} \leqslant \frac{\log 2}{\vartheta(x) \log \vartheta(x)} + \frac{1}{x-2} \qquad (x > 2). \tag{78}$$

Here, we have used the fact that

$$\sum_{p > x} \frac{1}{p(p-2)} \leqslant \sum_{n \geqslant \lfloor x \rfloor + 1} \frac{1}{n(n-2)} = \frac{2\lfloor x \rfloor - 1}{2\lfloor x \rfloor (\lfloor x \rfloor - 1)} < \frac{1}{x-2} \qquad (x > 2).$$

First, let us suppose that the Riemann hypothesis is true. In this case, we have from [43, p. 383]:

$$\log f(x) \leqslant -\frac{0.8}{\sqrt{x}\, \log x} \qquad (x \geqslant 3000).$$

Using this bound in (78) together with the inequality $\vartheta(x) \geqslant 4x/5$ (which holds unconditionally for $x \geqslant 121$ by [52, Theorems 4 and 18]), one sees that

$$\log g(x) \leqslant \frac{\log 2}{(4x/5)\log(4x/5)} + \frac{1}{x-2} - \frac{0.8}{\sqrt{x}\, \log x} \leqslant -\frac{0.6}{\sqrt{x}\, \log x}$$

for all $x \geqslant 3000$. This implies the desired bound (73) for all $k \geqslant 431$; for smaller values of k, the bound (73) may be verified by a direct computation. This proves Theorem 5.1 under the Riemann hypothesis.

Next, suppose that the Riemann hypothesis is false, and let θ denote the supremum of the real parts of the zeros of the Riemann zeta function. Then, by [43, Théorème 3c] one has

$$\overline{\lim_{x\to\infty}}\, x^b \log f(x) > 0 \qquad \text{and} \qquad \underline{\lim_{x\to\infty}}\, x^b \log f(x) < 0$$

for any fixed number b such that $1-\theta < b < 1/2$. In view of (78) and the Chebyshev bound $\vartheta(x) \gg x$ it is clear that

$$\log g(x) = \log f(x) + O(x^{-1});$$

hence, we also have

$$\overline{\lim_{x\to\infty}}\, x^b \log g(x) > 0 \qquad \text{and} \qquad \underline{\lim_{x\to\infty}}\, x^b \log g(x) < 0.$$

In particular, $\log g(p_k)$ changes sign infinitely often, which implies Theorem 5.1 if the Riemann hypothesis is false.

Part 6

On the congruence $n \equiv a \pmod{\varphi(n)}$

6.1 Introduction

In 1932, D. H. Lehmer [38] asked whether there are any *composite* numbers n for which $\varphi(n) \mid n-1$, and the answer to this question is still unknown.

In what follows, for any set $\mathcal{S} \subseteq \mathbb{N}$ we put $\mathcal{S}(x) = \mathcal{S} \cap [1, x]$ for all $x \geqslant 1$. In a series of papers (see [46, 47, 48]) C. Pomerance considered the problem of bounding the cardinality of $\mathscr{L}(x)$, where $\mathscr{L}$ is the (possibly empty) set of composite numbers n such that $\varphi(n) \mid n-1$. In his third paper [48] Pomerance established the bound

$$\#\mathscr{L}(x) \ll x^{1/2}(\log x)^{3/4} \tag{79}$$

and remarked that

> *There is still clearly a wide gap between the possibility that $\mathscr{L} = \varnothing$ and [(79)], for the latter does not even establish that the members of $\mathscr{L}$ are as scarce as squares!*

Refinements of the underlying method of [48] led to subsequent improvements of the bound (79):

$$\#\mathscr{L}(x) \ll x^{1/2}(\log x)^{1/2}(\log\log x)^{-1/2} \qquad \text{(Shan [56])}$$
$$\#\mathscr{L}(x) \ll x^{1/2}(\log\log x)^{1/2} \qquad \text{(Banks and Luca [10])}$$

In the present note, we use similar techniques to show that the members of $\mathscr{L}$ are *scarcer than squares*, i.e., that $\#\mathscr{L}(x) = o(x^{1/2})$ as $x \to \infty$. More precisely, we prove the following:

Theorem 6.1. *For any fixed $\varepsilon > 0$ the bound*

$$\#\mathscr{L}(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta-\varepsilon}}$$

holds, where $\Theta = 0.129398\cdots$ is the least positive solution to the equation

$$2\Theta(\log\Theta - 1 - \log\log 2) = -\log 2. \tag{80}$$

As in the earlier papers [10, 46, 47, 48, 56] where bounds on the cardinality of $\mathscr{L}(x)$ are given, Theorem 6.1 admits a natural generalization. For an arbitrary integer a, let

$$\mathscr{L}_a = \big\{n \in \mathbb{N} \ : \ n \equiv a \pmod{\varphi(n)}\big\},$$

and put

$$\mathscr{L}'_a = \big\{n \in \mathscr{L}_a \ : \ n \neq pa \text{ for } p \text{ prime}, p \nmid a\big\}.$$

Since $\mathscr{L}'_1 = \mathscr{L} \cup \{1\}$, Theorem 6.1 is the special case $a = 1$ of the following:

Theorem 6.2. *Let $a \in \mathbb{Z}$ and $\varepsilon > 0$ be fixed. Then,*

$$\#\mathscr{L}'_a(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta-\varepsilon}},$$

where Θ is the least positive solution to the equation (80).

We remark that for $a = 0$ one has $\#\mathscr{L}'_0(x) \asymp (\log x)^2$, which follows from the result of Sierpiński [58, p. 232]:

$$\mathscr{L}'_0 = \{1\} \cup \big\{2^i\, 3^j \ : \ i \geqslant 1,\ j \geqslant 0\big\}.$$

Hence, we shall assume that $a \neq 0$ in the sequel.

6.2 Preliminaries

According to [48, Lemma 1] the inequality

$$\#\mathscr{L}'_a(x) \leqslant 4a^2 + \sum_{d \,|\, a} \#\mathscr{L}''_{a/d}(x/d)$$

holds, where

$$\mathscr{L}''_a = \big\{n \in \mathscr{L}'_a : n \text{ is square-free}\big\}.$$

Thus, to prove Theorem 6.2 it suffices to show that

$$\#\mathscr{L}''_a(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta-\varepsilon}}. \tag{81}$$

The following result is due to Pomerance [48, Theorem 1]:

Lemma 6.3. *Suppose that $n \geqslant 16a^2$, $n \in \mathscr{L}''_a$, and $K = \omega(n)$. Let the prime factorization of n be $p_1 \cdots p_K$, where $p_1 > \cdots > p_K$. Then, for $1 \leqslant i \leqslant K$ we have*

$$p_i < (i+1)\left(1 + \prod_{j=i+1}^{K} p_j\right).$$

We also need the following lemma from [56]:

Lemma 6.4. *Suppose that $\delta \geqslant 0$, $a_1 \geqslant \cdots \geqslant a_t = 0$, and $a_i \leqslant \delta + \sum_{j=i+1}^{t} a_j$ for $1 \leqslant i \leqslant t-1$. Then, for any real number ρ such that $0 \leqslant \rho < \sum_{i=1}^{t} a_i$, there is a subset $\mathcal{I}$ of $\{1, \dots, t\}$ such that $\rho - \delta < \sum_{i \in \mathcal{I}} a_i \leqslant \rho$.*

Our principal tool is the following (see, for example, [18, Proposition 3]):

Lemma 6.5. *For fixed $0 < \lambda < 1$, the counting function of the set*

$$\mathcal{V}_\lambda = \big\{n \ : \ \omega(n) < \lambda \log\log n\big\}$$

satisfies

$$\#\mathcal{V}_\lambda(x) \asymp \frac{x}{(\log x)^{1+\lambda\log(\lambda/e)}}\,.$$

For fixed $\lambda > 1$, the counting function of the set

$$\mathcal{W}_\lambda = \big\{n \ : \ \omega(n) > \lambda \log\log n\big\}$$

satisfies

$$\#\mathcal{W}_\lambda(x) \asymp \frac{x}{(\log x)^{1+\lambda\log(\lambda/e)}}\,.$$

Finally, we recall the well known inequality of Landau [36]:

$$\frac{n}{\varphi(n)} \ll \log\log n \qquad (n \geqslant 3). \tag{82}$$

6.3 Proof of Theorem 6.2

We write the bound of [10] in the form:

$$\#\mathscr{L}_a''(x) \leqslant \#\mathscr{L}_a'(x) \leqslant x^{1/2}(\log x)^{o(1)} \qquad (x \to \infty). \tag{83}$$

Let $\varepsilon > 0$ be small fixed parameter. Let α and β be fixed real numbers such that

$$\Theta - \varepsilon < \alpha/2 < \beta < \Theta,$$

where Θ is defined as in Theorem 6.1, and put

$$A = (\log x)^\alpha \qquad \text{and} \qquad B = (\log x)^\beta.$$

Note that (83) implies

$$\#\mathscr{L}_a''(x/A) \leqslant x^{1/2}(\log x)^{-\alpha/2+o(1)} \qquad (x \to \infty),$$

and since $\alpha/2 > \Theta - \varepsilon$ it follows that

$$\#\mathscr{L}_a''(x/A) \ll x^{1/2}(\log x)^{-\Theta+\varepsilon}. \tag{84}$$

Now let $n \in \mathscr{L}_a''$ be fixed with $16a^2 \leqslant x/A < n \leqslant x$. Put $K = \omega(n)$, and factor $n = p_1 \cdots p_K$ where $p_1 > \ldots > p_K$. By Lemma 6.3 we have

$$\log p_i < \log(2K) + \sum_{j=i+1}^{K} \log p_j \qquad (1 \leqslant i \leqslant K).$$

Applying Lemma 6.4 with $\delta = \log(2K)$, $t = K+1$, $a_i = \log p_i$ for $1 \leqslant i \leqslant K$, $a_t = 0$, and $\rho = \log(x^{1/2}/B)$, we conclude that n has a positive divisor d such that $\rho - \delta < \log d \leqslant \rho$; in other words,

$$\frac{x^{1/2}}{2\,\omega(n)B} \leqslant d \leqslant \frac{x^{1/2}}{B}\,. \tag{85}$$

Setting $m = n/d$, it is also clear that

$$\frac{x^{1/2}B}{A} \leqslant m \leqslant 2\,\omega(n)Bx^{1/2}. \tag{86}$$

First, suppose that $n \in \mathcal{W}_{20}$. Since n is square-free we have

$$\omega(d) + \omega(m) = \omega(dm) = \omega(n) > 20 \log\log n,$$

hence either $d \in \mathcal{W}_{10}$ or $m \in \mathcal{W}_{10}$. Using the trivial bound $\omega(n) \leqslant 2\log x$ and the inequality $A \leqslant B^2$, we see that n has a divisor $k \in \mathcal{W}_{10}$ such that

$$\frac{x^{1/2}}{4B\log x} \leqslant k \leqslant 4Bx^{1/2}\log x.$$

Note that $\gcd(k, \varphi(k)) \mid a$ since $k \mid n$ and $n \equiv a \pmod{\varphi(n)}$. On the other hand, if k is fixed with the above properties, and n is a number in $\mathscr{L}_a$ that is divisible by k, then

$$n \equiv 0 \pmod{k} \qquad \text{and} \qquad n \equiv a \pmod{\varphi(k)}.$$

By the Chinese Remainder Theorem, we see that n is uniquely determined modulo $\operatorname{lcm}[k, \varphi(k)]$. Hence, the number of integers $n \leqslant x$ with $n \in \mathscr{L}_a'' \cap \mathcal{W}_{20}$ and $k \mid n$ does not exceed

$$1 + \frac{x}{\operatorname{lcm}[k,\varphi(k)]} \leqslant 1 + \frac{xa}{k\varphi(k)} \ll 1 + \frac{x\log\log x}{k^2}\,,$$

where we have used (82) in the last step. Put $y = x^{1/2}/(4B\log x)$ and $z = 4Bx^{1/2}\log x$. Summing the contributions over all such integers k, we derive that

$$\begin{aligned}\#\big\{n \in \mathscr{L}_a'' \cap \mathcal{W}_{20} \ : \ x/A \leqslant n \leqslant x\big\} &\ll \sum_{\substack{y \leqslant k \leqslant z \\ k \in \mathcal{W}_{10}}} \left(1 + \frac{x \log\log x}{k^2}\right) \\ &\leqslant \sum_{\substack{k \leqslant z \\ k \in \mathcal{W}_{10}}} 1 + x\log\log x \sum_{\substack{k \geqslant y \\ k \in \mathcal{W}_{10}}} \frac{1}{k^2} \\ &\ll \frac{z}{(\log z)^{14}} + \frac{x\log\log x}{y(\log y)^{14}}\,.\end{aligned}$$

Here, we have used Lemma 6.5, the inequality $1 + 10\log(10/e) > 14$, and the estimate

$$\sum_{\substack{k \geqslant y \\ k \in \mathcal{W}_\lambda}} \frac{1}{k^2} \ll \frac{1}{y(\log y)^{1+\lambda\log(\lambda/e)}}\,,$$

which follows from Lemma 6.5 by partial summation. Inserting the definitions of y, z and B into the bound above, and noting that $\beta < \Theta < 1$, we derive that

$$\begin{aligned}\#\big\{n \in \mathscr{L}_a'' \cap \mathcal{W}_{20} \ : \ x/A \leqslant n \leqslant x\big\} &\ll \frac{Bx^{1/2}\log\log x}{(\log x)^{13}} \\ &\ll x^{1/2}(\log x)^{\beta - 12} \\ &\ll x^{1/2}(\log x)^{-\Theta}.\end{aligned} \tag{87}$$

Next, we consider the case that $n \notin \mathcal{W}_{20}$. Since $\omega(n) \leqslant 20\log\log x$, the inequalities (85) and (86) can be replaced by

$$\frac{x^{1/2}}{40B\log\log x} \leqslant d \leqslant \frac{x^{1/2}}{B} \tag{88}$$

and

$$\frac{x^{1/2}B}{A} \leqslant m \leqslant 40Bx^{1/2}\log\log x, \tag{89}$$

respectively. Let $\mathcal{T}$ be the collection of pairs (d, m) of natural numbers such that $dm \in \mathscr{L}_a''$ and the inequalities (88) and (89) hold. Then,

$$\#\big\{n \in \mathscr{L}_a'' \setminus \mathcal{W}_{20} \ : \ x/A \leqslant n \leqslant x\big\} \leqslant \#\mathcal{T}. \tag{90}$$

Lemma 6.6. *If x is sufficiently large, then for every integer m there is at most one integer d such that $(d, m) \in \mathcal{T}$.*

Proof. Suppose (d_1, m) and (d_2, m) both lie in $\mathcal{T}$. Since $d_1 m$ and $d_2 m$ are numbers in $\mathscr{L}_a''$, we have

$$\varphi(m) \mid d_1 m - a \qquad \text{and} \qquad \varphi(m) \mid d_2 m - a.$$

Hence it follows that

$$d_1 \equiv d_2 \pmod{\varphi(m)/\mu}, \tag{91}$$

where $\mu = \gcd(m, \varphi(m))$; note that $\mu \ll 1$ since $d_1 m \equiv a \pmod{\varphi(m)}$. By (88) we have the bound

$$\max\{d_1, d_2\} \leqslant \frac{x^{1/2}}{B} = x^{1/2}(\log x)^{-\beta},$$

whereas by (82) and (89) we have

$$\frac{\varphi(m)}{\mu} \gg \frac{m}{\log\log m} \geqslant x^{1/2}(\log x)^{\beta-\alpha+o(1)} \qquad (x \to \infty).$$

Since $\beta > \alpha/2$, it follows that for all sufficiently large x, both d_1 and d_2 are smaller than the modulus in (91), so the congruence becomes an equality $d_1 = d_2$. This completes the proof. □

From now on, we assume that x is large enough to yield the conclusion of Lemma 6.6. Let $\mathcal{M}$ denote the set of integers m such that $(d, m) \in \mathcal{T}$ for some integer d. By Lemma 6.6, the map $(d, m) \mapsto m$ provides a bijection $\mathcal{T} \xleftrightarrow{\sim} \mathcal{M}$; in particular, $\#\mathcal{T} = \#\mathcal{M}$, and (90) can be restated as

$$\#\{n \in \mathscr{L}_a'' \setminus \mathcal{W}_{20} \ : \ x/A \leqslant n \leqslant x\} \leqslant \#\mathcal{M}. \tag{92}$$

Let $\vartheta = 0.373365\cdots$ be the unique solution in the interval $(0, 1)$ to the equation

$$1 + \vartheta \log(\vartheta/e) = \vartheta \log 2.$$

From (80) it follows that

$$2\Theta = 1 + \vartheta \log(\vartheta/e) = \vartheta \log 2. \tag{93}$$

We now express $\mathcal{M}$ as a disjoint union $\mathcal{M}_1 \cup \mathcal{M}_2$, where

$$\mathcal{M}_1 = \mathcal{M} \cap \mathcal{V}_\vartheta \qquad \text{and} \qquad \mathcal{M}_2 = \mathcal{M} \setminus \mathcal{V}_\vartheta.$$

Using Lemma 6.5, (89) and (93) we derive the bound

$$\#\mathcal{M}_1 \leqslant \#\mathcal{V}_\vartheta(40Bx^{1/2}\log\log x) \ll \frac{Bx^{1/2}\log\log x}{(\log x)^{1+\vartheta\log(\vartheta/e)}} \leqslant x^{1/2}(\log x)^{\beta-2\Theta+o(1)}$$

as $x \to \infty$. Since $\beta < \Theta$, it follows that

$$\#\mathcal{M}_1 \ll x^{1/2}(\log x)^{-\Theta}. \tag{94}$$

Lemma 6.7. *If x is sufficiently large, then for every integer d there is at most one integer $m \in \mathcal{M}_2$ such that $(d, m) \in \mathcal{T}$.*

Proof. Suppose (d, m_1) and (d, m_2) both lie in $\mathcal{T}$, where $m_1, m_2 \in \mathcal{M}_2$. From the lower bound of (89) we see that both numbers m_1 and m_2 have at least $\kappa = \lfloor \vartheta \log\log(x^{1/2}B/A) \rfloor$ distinct odd prime divisors; hence both integers $\varphi(m_1)$ and $\varphi(m_2)$ are divisible by 2^κ. Since dm_1 and dm_2 are numbers in $\mathscr{L}_a''$, we can write

$$dm_1 = a + 2^\kappa \varphi(d) s_1 \qquad \text{and} \qquad dm_2 = a + 2^\kappa \varphi(d) s_2$$

for some natural numbers s_1, s_2. Hence it follows that

$$m_1 \equiv m_2 \pmod{2^\kappa \varphi(d)/\mu} \tag{95}$$

where $\mu = \gcd(d, 2^\kappa \varphi(d))$; note that $\mu \ll 1$ as in the proof of Lemma 6.6 (taking into account that d is square-free). By (89) we have the bound

$$\max\{m_1, m_2\} \leqslant 40Bx^{1/2}\log\log x = x^{1/2}(\log x)^{\beta + o(1)} \qquad (x \to \infty).$$

On the other hand, since $\kappa = (\vartheta + o(1))\log\log x$ as $x \to \infty$, using (82), (88) and (93) we derive the lower bound

$$\frac{2^\kappa \varphi(d)}{\mu} \gg \frac{d \cdot 2^\kappa}{\log\log d} \geqslant \frac{x^{1/2}(\log x)^{\vartheta \log 2 + o(1)}}{B(\log\log x)^2} = x^{1/2}(\log x)^{2\Theta - \beta + o(1)}.$$

Since $\beta < \Theta$, it follows that $2^\kappa \varphi(d)/\mu > \max\{m_1, m_2\}$ once x is sufficiently large. The congruence (95) then becomes an equality $m_1 = m_2$, which finishes the proof. □

We now assume that x is large enough to yield the conclusion of Lemma 6.7. Let $\mathscr{D}$ denote the set of integers d such that $(d, m) \in \mathcal{T}$ for some integer $m \in \mathcal{M}_2$. Applying Lemma 6.6 and using the upper bound of (88), we see that

$$\#\mathcal{M}_2 = \#\mathscr{D} \leqslant \frac{x^{1/2}}{B} = x^{1/2}(\log x)^{-\beta}.$$

Since $\beta > \Theta - \varepsilon$ we obtain

$$\#\mathcal{M}_2 \leqslant x^{1/2}(\log x)^{-\Theta + \varepsilon}. \tag{96}$$

Combining (84), (87), (92), (94) and (96), and taking into account that $\#\mathcal{M} = \#\mathcal{M}_1 + \#\mathcal{M}_2$, we derive the bound (81), and this finishes the proof of Theorem 6.2.

Part 7

Guiga's conjecture and Lehmer's totient problem

7.1 Introduction

7.1.1 Carmichael numbers

In a letter to Frenicle dated October 18, 1640, Fermat wrote that if p is a prime number, then p divides $a^{p-1} - 1$ for any integer a not divisible by p. This result, known as *Fermat's little theorem*, is equivalent to the statement:

$$a^p \equiv a \pmod{p} \qquad \text{for all } a \in \mathbb{Z}.$$

Almost three centuries later, Carmichael [14] began an in-depth study of *composite* natural numbers n with the property that

$$a^n \equiv a \pmod{n} \qquad \text{for all } a \in \mathbb{Z};$$

these are now called *Carmichael numbers*. More than eighty years elapsed after Carmichael's initial investigations before the existence of infinitely many Carmichael numbers was established by Alford, Granville, and Pomerance [1]. Denoting by $\mathcal{C}$ the set of Carmichael numbers, it is shown in [1] that for every $\varepsilon > 0$ and all sufficiently large X, the lower bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C}\}\big| \geqslant X^{\beta-\varepsilon} \tag{97}$$

holds, where

$$\beta = \beta_0 = \frac{5}{12}\left(1 - \frac{1}{2\sqrt{e}}\right) = 0.290306\cdots > \frac{2}{7}\,.$$

More recently, Harman [26] has shown that the lower bound (97) holds with the larger constant $\beta = \beta_1 = 0.3322408$.

The purpose of the present note is to show that the bound (97) with $\beta = \beta_1$ also holds with a set of Carmichael numbers $n \leqslant X$ that are consistent with *Giuga's conjecture* and support the nonexistence of examples to *Lehmer's totient problem*. Our results are described in more detail below.

7.1.2 Giuga's conjecture

Fermat's little theorem implies

$$p \mid 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} + 1$$

for every prime p. In 1950, Giuga [22] conjectured that the converse is true, i.e., that there are no *composite* natural numbers n for which

$$1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} \equiv -1 \pmod{n},$$

and he verified this conjecture for all $n \leqslant 10^{1000}$. Any counterexample to Giuga's conjecture is called a *Giuga number*.

Denoting by $\mathcal{G}$ the (presumably empty) set of Giuga numbers, Giuga showed that $n \in \mathcal{G}$ if and only if n is composite and

$$p^2(p-1) \mid n - p \qquad \text{for every prime } p \text{ dividing } n. \tag{98}$$

As this condition implies that n is squarefree, every Giuga number is a Carmichael number in view of the following criterion.

Korselt's criterion. *For a positive integer n, $a^n \equiv a \pmod{n}$ for all integers a if and only if n is squarefree and $p-1$ divides $n-1$ for every prime p dividing n.*

The condition (98) appears to be a much stronger requirement for a composite natural number n to satisfy than Korselt's criterion, thus it is reasonable to expect that there are infinitely many Carmichael numbers which are *not* Giuga numbers. Indeed, it is widely believed (see [1]) that

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C}\}\big| = X^{1+o(1)} \qquad \text{as } X \to \infty,$$

whereas Luca, Pomerance and Shparlinski [40] have established the bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{G}\}\big| \ll \frac{X^{1/2}}{(\log X)^2}, \tag{99}$$

improving slightly on a result of Tipu [60]. However, the result that $\mathcal{C} \setminus \mathcal{G}$ is an infinite set does not follow from (99) and the unconditional bound (97) with $\beta = \beta_1$. Nevertheless, we are able to prove the following result.

Theorem 7.1. *For any fixed $\varepsilon > 0$ and all sufficiently large X, we have*

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C} \setminus \mathcal{G}\}\big| \geqslant X^{\beta_1 - \varepsilon}.$$

It is known that if n is a Giuga number, then

$$-\frac{1}{n}+\sum_{p\,|\,n}\frac{1}{p}\in\mathbb{N}. \tag{100}$$

There are known composites that satisfy (100), for example $n=30$. A *weak Giuga number* is a composite number n satisfying (100). Denoting by $\mathcal{W}$ the set of weak Giuga numbers, we have $\mathcal{G}\subset\mathcal{W}$, hence Theorem 7.1 is an immediate consequence of the following theorem.

Theorem 7.2. *For any fixed $\varepsilon>0$ and all sufficiently large X, we have*

$$\big|\{n\leqslant X\ :\ n\in\mathcal{C}\setminus\mathcal{W}\}\big|\geqslant X^{\beta_1-\varepsilon}.$$

Our proof of Theorem 7.2 is given in §7.2 below.

7.1.3 Lehmer's totient problem

Using notation from Part 6 we have the folling theorem.

Theorem 7.3. *For any fixed $\varepsilon>0$ and all sufficiently large X, we have*

$$\big|\{n\leqslant X\ :\ n\in\mathcal{C}\setminus\mathcal{L}\}\big|\geqslant X^{\beta_1-\varepsilon}.$$

Our proof of Theorem 7.3 is given in §7.2 below.

7.2 Construction

Let $\mathcal{N}$ denote the set of composite natural numbers n such that

$$\sum_{p\,|\,n}\frac{1}{p}<\frac{1}{3}\,.$$

Lemma 7.4. *The sets $\mathcal{N}$ and $\mathcal{W}$ are disjoint.*

Proof. Let $n\in\mathcal{N}$. Since

$$\frac{1}{n}<\sum_{p\,|\,n}\frac{1}{p}<\frac{1}{3}<1+\frac{1}{n}\,,$$

it is clear that

$$\sum_{p\,|\,n}\frac{1}{p}\not\equiv\frac{1}{n}\pmod 1,$$

hence n is not a weak Giuga number. □

Lemma 7.5. *The sets $\mathcal{N}$ and $\mathcal{L}$ are disjoint.*

Proof. Let $n \in \mathcal{N}$. Using the inequality

$$\log(1-t) > -2\,t \qquad (0 < t \leqslant 1/2),$$

we have

$$\log \frac{\varphi(n)}{n} = \log \prod_{p\,|\,n} \left(1 - \frac{1}{p}\right) = \sum_{p\,|\,n} \log\left(1 - \frac{1}{p}\right) > -2 \sum_{p\,|\,n} \frac{1}{p} > -\frac{2}{3}\,.$$

Consequently,

$$\frac{n-1}{\varphi(n)} < \frac{n}{\varphi(n)} < e^{2/3} < 2, \tag{101}$$

and it follows that $n \notin \mathcal{L}$. Indeed, (101) and the condition $\varphi(n) \mid n-1$ together imply that $n = 1$ or $\varphi(n) = n-1$, which possibilities cannot occur for a composite natural number n. □

In view of Lemmas 7.4 and 7.5, Theorems 7.2 and 7.3 follow from the following result.

Theorem 7.6. *For any fixed $\varepsilon > 0$ and all sufficiently large X, we have*

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C} \cap \mathcal{N}\}\big| \geqslant X^{\beta_1 - \varepsilon}.$$

Proof. As mentioned earlier, Harman [26, Theorem 1] has shown that for every $\varepsilon > 0$ and all sufficiently large X, the lower bound

$$\big|\{n \leqslant X \ : \ n \in \mathcal{C}\}\big| \geqslant X^{\beta_1 - \varepsilon} \tag{102}$$

holds. To prove Theorem 7.6, it suffices to show that the Carmichael numbers constructed by Harman all lie in $\mathcal{N}$ if X is large enough.

The proof of (102) is based on the well known construction of Carmichael numbers given by Alford, Granville and Pomerance [1] and relies on the following statement, which is Theorem 3 of Harman [26].

Lemma 7.7. *Let $\varepsilon > 0$, and suppose $y \geqslant y_0(\varepsilon)$. Put*

$$\delta = \frac{\varepsilon\,\theta}{1.888}\,, \qquad x = \exp\left(y^{1+\delta}\right), \qquad \theta = \frac{1}{0.2961}\,.$$

Then there is a positive integer $k < x^{0.528}$ and a set of squarefree numbers $\mathcal{B}$ such that

(*i*) $\mathcal{B} \subset [x^{0.4}, x^{0.472}]$;

(*ii*) $|\mathcal{B}| > x^{\beta_1 - \varepsilon}$;

(*iii*) $dk+1$ *is prime for every* $d \in \mathcal{B}$;

(*iv*) *if* $p \mid d$, *then*

$$0.5\, y^{\theta} < p < y^{\theta}, \qquad p \nmid k, \qquad P(p-1) < y,$$

where $P(n)$ *denotes the greatest prime factor of* n.

Let n be one of the Carmichael numbers constructed in [26, Theorem 1]. Such a number n is composed of at most $t = \exp\left(y^{1+\delta/2}\right)$ primes of the form $p = dk+1$ with $d \in \mathcal{B}$, so that

- $n \leqslant X$, where $X = x^t$;
- $p \geqslant x^{0.4}$ for every prime $p \mid n$.

Taking into account that $t = x^{o(1)}$ as $x \to \infty$, it follows that

$$\sum_{p \mid n} \frac{1}{p} \leqslant t\, x^{-0.4} < \frac{1}{3}$$

if x is sufficiently large. Since the value of x is determined uniquely by X, this shows that the Carmichael number n lies in $\mathcal{N}$ once X is large enough, completing the proof. □

We remark that the proof in [1] also supports the assertion that there are infinitely many Carmichael numbers in $\mathcal{N}$, but there are not so many of them constructed in that paper as in [26]. In [2] it is shown that for each fixed k there are infinitely many Carmichael numbers n with $\sum_{p|n} 1/p < 1/(\log n)^k$. On the other hand, it is not known if there is some $\varepsilon > 0$ such that for infinitely many Carmichael numbers n we have $\sum_{p|n} 1/p > \varepsilon$. In particular, it is not known if the set $\mathcal{C} \setminus \mathcal{N}$ is infinite.

Part 8

Descartes Numbers

8.1 Introduction

> *...Mais je pense pouvoir démontrer qu'il n'y en a point de pairs qui soient parfaits, excepté ceux d'Euclide; & qu'il n'y en a point aussi d'impairs, si ce n'est qu'ils soient composés d'un seul nombre premier, multiplié par un carré dont la racine soit composée de plusieurs autres nombres premiers. Mais je ne vois rien qui empêche qu'il ne s'en trouve quelques uns de cette sorte: car, par exemple, si 22021 était nombre premier, en le multipliant par 9018009, qui est un carré dont la racine est composée des nombres premiers 3, 7, 11 & 13, on aurait 198585576189, qui serait nombre parfait...*
>
> – Réne Descartes, *Letter to Mersenne*, November 15, 1638.

Recall that an integer $n \geqslant 1$ is said to be a *perfect number* if $\sigma(n) = 2n$. If $2^p - 1$ is a prime number (that is, a *Mersenne prime*), then $n = 2^{p-1}(2^p - 1)$ is a perfect number. This fact was first observed by Euclid (Proposition 36 in Book IX of *Elements*; see [27]), and many of Euclid's successors implicitly assumed that every perfect number has this form. The idea that every *even* perfect number has this form was first proposed by Descartes in the letter to Mersenne quoted above. More than two hundred years later, Euler (in posthumous [20]) published the first proof that Euclid's construction yields all even perfect numbers.

To this day, it is not known whether there exist any *odd* perfect numbers. Descartes believed that such numbers might exist, and he stated (without proof) that every odd perfect number must be of the form $p^a m^2$, where m is an integer, p is a prime number, and $p \equiv a \equiv 1 \pmod 4$. The first rigorous proof of this assertion was given by Euler [19]; however, it is reasonably certain that Descartes himself must have been in possession of such a proof.

Perhaps because of the popularity of Euler's works, Descartes did not receive a great deal of credit for his numerous contributions to the study of perfect numbers (see Dickson [17]). However, the depth of his understanding of the subject should not be underestimated, as is evident from the following example of an odd number $\mathfrak{D}$ which he discovered:

$$\mathfrak{D} = 3^2\, 7^2\, 11^2\, 13^2\, 22021 = 198585576189. \tag{103}$$

The number $\mathfrak{D}$ comes "very close to perfection." In fact, as Descartes himself observed, $\mathfrak{D}$ would be an odd perfect number if only 22021 were a prime number, since

$$\sigma(3^2\,7^2\,11^2\,13^2)\,(22021+1) = 2\cdot 3^2\,7^2\,11^2\,13^2\,22021 = 2\mathfrak{D}. \tag{104}$$

Alas, $22021 = 19^2\,61$ is composite, and the number $\mathfrak{D}$ is not perfect.

Inspired by the example (103) and the identity (104), let us call an integer n a *Descartes number/* if n is *odd*, and if $n = km$ for two integers $k, m > 1$ such that

$$\sigma(k)(m+1) = 2n. \tag{105}$$

Then $\mathfrak{D}$ is a Descartes number, and this is the only currently known example. We remark that if $n = km$ is a Descartes number such that m is prime and $m \nmid k$, then n is an odd perfect number.

In this manuscript, for simplicity, we investigate *cube-free* Descartes numbers n (that is, $p^3 \nmid n$ for every prime p); note that $\mathfrak{D}$ is cube-free.

To state our results, recall that a positive integer k is said to be *almost perfect* if $\sigma(k) = 2k - 1$. Every nonnegative power of 2 is almost perfect, and it is generally believed that these are the *only* examples of such integers (see Guy [25]). In particular, it is believed that $k = 1$ is the only *odd* almost perfect number. We remark that if $k > 1$ is an odd almost perfect number, then $n = k\sigma(k)$ is a Descartes number.

Theorem 8.1. *If n is a cube-free Descartes number which is not divisible by 3, then $n = k\,\sigma(k)$ for some odd almost perfect number k, and n has more than one million distinct prime divisors.*

Theorem 8.2. *The number $\mathfrak{D}$ is the only cube-free Descartes number with fewer than seven distinct prime divisors.*

8.2 Preparations

We use the following elementary results:

Lemma 8.3. *Let a and b be integers such that $2a > b \geqslant 1$ and $(2a - b) \mid a$. Then $a = de$ and $b = d(2e-1)$ for some positive integers d and e.*

Proof. Put $d = \gcd(a, b)$, and write $a = de$, $b = df$, where $\gcd(e, f) = 1$. The hypothesis $(2a - b) \mid a$ implies $(2e - f) \mid e$; therefore, since $2e > f$ we have

$$2e - f = \gcd(2e - f, e) = \gcd(-f, e) = 1,$$

or $f = 2e - 1$ as required. □

Lemma 8.4. *If p and q are primes such that $p^2+p+1 \equiv 0 \pmod{q}$, then $q = 3$ or $q \equiv 1 \pmod{3}$. If s is square-free, then the number $\sigma(s^2)$ has no prime divisor $q \equiv 2 \pmod{3}$.*

Proof. To prove the first statement, we note that

$$(2p+1)^2 + 3 = 4p^2 + 4p + 4 \equiv 0 \pmod{q}.$$

If $q \neq 3$, this shows that -3 is a quadratic residue modulo q, which is only possible if $q \equiv 1 \pmod{3}$. For a square-free number s we have

$$\sigma(s^2) = \prod_{p \mid s} (p^2+p+1), \tag{106}$$

hence the second statement follows from the first. □

Finally, in our proof of Theorem 8.2 we use the following:

Lemma 8.5 (Pomerance [45])**.** *Every odd perfect number has at least seven distinct prime divisors.*

8.3 Cube-free Descartes numbers

Let n be a Descartes number, and write $n = km$ with odd integers $k, m > 1$ satisfying (105). Then,

$$\sigma(k) \cdot \frac{m+1}{2} = n = km, \tag{107}$$

and therefore,

$$m = \frac{\sigma(k)}{2k - \sigma(k)} = -1 + 2 \cdot \frac{k}{2k - \sigma(k)}. \tag{108}$$

From (107) we deduce that $\sigma(k)$ is odd, hence $k = s^2$ for some integer $s \geqslant 1$. Using (108) together with the fact that $2k - \sigma(k)$ is odd, we also see that $(2k - \sigma(k)) \mid k$; hence, by Lemma 8.3 we have

$$k = s^2 = de \qquad \text{and} \qquad \sigma(k) = \sigma(s^2) = d(2e-1) \tag{109}$$

for some positive integers d and e. Substituting these expressions into (108), it follows that $m = 2e - 1$, and therefore,

$$\sigma(k) = \sigma(s^2) = dm. \tag{110}$$

Suppose now that n is cube-free. As $s^2 \mid n$, it follows that s is square-free. We claim that $3 \nmid e$. Indeed, if $3 \mid e$, it follows that $m = 2e - 1 \equiv 2 \pmod{3}$, hence there

is a prime $q \equiv 2 \pmod 3$ dividing m; but this is not possible in view of Lemma 8.4 since $m \mid \sigma(s^2)$.

Next, we claim that $e \equiv 1 \pmod 3$. Indeed, if a prime $q \equiv 2 \pmod 3$ divides e, then $q \mid s$, and $q^2 \mid s^2 = de$. But q cannot divide d, for otherwise q would divide $\sigma(s^2)$, contradicting Lemma 8.4. Hence, $q^2 \mid e$, and therefore $q^2 \parallel e$ since e is cube-free. Since $3 \nmid e$, we now see that

$$e = \Bigg(\prod_{\substack{q^a \parallel e \\ q \equiv 1 \pmod 3}} q^a \Bigg) \Bigg(\prod_{\substack{q \mid e \\ q \equiv 2 \pmod 3}} q^2 \Bigg),$$

and the congruence $e \equiv 1 \pmod 3$ is obvious.

For any integer t, we have $3 \mid (t^2 + t + 1)$ if and only if $t \equiv 1 \pmod 3$, and in this case, $t^2 + t + 1 \equiv 3 \pmod 9$. Therefore, observing that $n = e\,\sigma(s^2)$, we deduce from (106):

$$\#\big\{p \ : \ p \mid s \text{ and } p \equiv 1 \pmod 3\big\} = v_3(\sigma(s^2)) = v_3(e\,\sigma(s^2)) = v_3(n). \tag{111}$$

Here, v_3 denotes the standard 3-*adic valuation*, and we have used the fact that $3 \nmid e$ to derive the second equality.

8.4 Proof of Theorem 8.1

We continue to use the notation of the previous section. In particular, n is a cube-free Descartes number. In what follows, we assume that $3 \nmid n$.

Since d divides n, we have $3 \nmid d$. By (111), we also see that d is not divisible by any prime $p \equiv 1 \pmod 3$. Finally, since $d \mid \sigma(s^2)$, Lemma 8.4 shows that d is not divisible by any prime $q \equiv 2 \pmod 3$. Therefore, $d = 1$. Now we have $n = k\sigma(k)$ by (107) and (110), and $\sigma(k) = 2k - 1$ by (109). Since k is odd, this proves the first assertion of Theorem 8.1.

As $k = s^2$ and $\sigma(k) = 2k - 1$, for every prime q dividing $\sigma(s^2)$ we have $2s^2 \equiv 1 \pmod q$, and thus $q \equiv \pm 1 \pmod 8$ (since 2 is a quadratic residue modulo q). Consequently, if p is any prime dividing s, then $p^2 + p + 1$ is composed of primes $q \equiv \pm 1 \pmod 8$; this implies that $p \equiv 5$ or $7 \pmod 8$. Also, $p \neq 3$ since we are assuming that $3 \nmid n$, and $p \not\equiv 1 \pmod 3$ by (111). We have therefore shown that every prime divisor of s lies in the set

$$\mathcal{P} = \big\{p \ : \ p \equiv 5 \text{ or } 23 \pmod{24}\big\}.$$

Let $p_1 < p_2 < p_3 < \cdots$ denote the primes in $\mathcal{P}$. Now, assuming that s has at most one million distinct prime divisors, we derive that

$$\frac{\sigma(s^2)}{s^2} = \prod_{p \,|\, s} \left(\frac{p^2 + p + 1}{p^2} \right) \leqslant \prod_{j=1}^{10^6} \left(\frac{p_j^2 + p_j + 1}{p_j^2} \right) < 1.995.$$

On the other hand, noting that $s \neq 1$ (since $s^2 = k > 1$), we have $s \geqslant 100$ since the equation $\sigma(s^2) = 2s^2 - 1$ has no solutions in the range $1 < s < 100$. Therefore,

$$\frac{\sigma(s^2)}{s^2} = 2 - \frac{1}{s^2} \geqslant 1.9999.$$

This contradiction, together with the fact that $n = s^2\,\sigma(s^2)$, implies the second assertion of Theorem 8.1, and this completes the proof.

8.5 Proof of Theorem 8.2

We continue to use the notation of Section 8.3. In what follows, we assume that n is a cube-free Descartes number such that $3 \mid n$ and $\omega(n) \leqslant 6$, where $\omega(n)$ denotes the number of distinct prime factors of n.

Since $m = 2e - 1 \equiv 1 \pmod 3$, and $(m+1)/2$ is odd by (107), we have

$$m \equiv 1 \pmod{12}. \tag{112}$$

Since $3 \mid n$ it follows that $3 \mid k = s^2$, thus $3^2 \mid k \mid n$; as n is cube-free, this means that $3^2 \parallel n$, and by (111) we see that

$$\#\big\{p \,:\, p \mid k \text{ and } p \equiv 1 \pmod 3\big\} = 2. \tag{113}$$

Since $n = km$ is cube-free and $k = s^2$, it is clear that $\gcd(k, m) = 1$. The number m cannot be prime, for otherwise the equation $\sigma(k)(m+1) = 2km$ implies n is an odd perfect number, and by Lemma 8.5 it has at least *seven* distinct prime divisors. Since $m \mid \sigma(s^2)$, Lemma 8.4 shows that m is not divisible by any prime $q \equiv 2 \pmod 3$; hence, from (112) it follows that $m \geqslant 49$. On the other hand, it must also be the case that $\omega(k) \geqslant 4$, for otherwise

$$\frac{\sigma(k)}{k} \leqslant \frac{\sigma(3^2\,7^2\,13^2)}{3^2\,7^2\,13^2} < \frac{2m}{m+1}$$

for any $m \geqslant 49$. We therefore have two distinct cases to consider:

(*A*) $m = p^2$ for some prime p, and $\omega(k) = 4$ or 5;

(B) $\omega(m) = 2$ and $\omega(k) = 4$.

Lemma 8.6. $5 \nmid k$.

Proof. Suppose on the contrary that $5 \mid k$, and write $k = s^2 = 3^2\,5^2\,\ell^2$ with some square-free integer ℓ. Then,

$$13 \cdot 31\,\sigma(\ell^2)(m+1) = 2 \cdot 3^2\,5^2\,\ell^2 m. \tag{114}$$

Since $5 \nmid \sigma(\ell^2)$ by Lemma 8.4, it follows that $5^2 \mid (m+1)$; using (112) and the Chinese Remainder Theorem we deduce that

$$m \equiv 49 \pmod{300}. \tag{115}$$

It cannot be the case that $(13 \cdot 31) \mid \ell$, for otherwise

$$\frac{\sigma(k)}{k} \geqslant \frac{\sigma(3^2\,5^2\,13^2\,31^2)}{3^2\,5^2\,13^2\,31^2} > 2 > \frac{2m}{m+1}.$$

Hence, by (114) we see that $13 \mid m$ or $31 \mid m$. But this is already impossible in case (A) as neither 13^2 nor 31^2 is congruent to 49 (mod 300); thus, we can assume that (B) holds for the rest of the proof.

Note that m is not divisible by *both* 13 and 31 since m is cube-free, $\omega(m) = 2$, and

$$13^\alpha\,31^\beta \not\equiv 49 \pmod{300} \qquad (1 \leqslant \alpha, \beta \leqslant 2).$$

Suppose that $13 \mid m$. Then $m \equiv 949 \pmod{3900}$ by (115) and the Chinese Remainder Theorem. Also, from (114) it follows that $31 \mid \ell$ (since $31 \nmid m$), and thus $k = 3^2\,5^2\,31^2\,q^2$ for some prime q. However, since $m \geqslant 949$ we have

$$\frac{2 \cdot 949}{950} \leqslant \frac{2m}{m+1} = \frac{\sigma(k)}{k} = \frac{\sigma(3^2\,5^2\,31^2)}{3^2\,5^2\,31^2}\,\frac{(q^2+q+1)}{q^2} < 2,$$

and it is easy to see that there is no integer q for which both inequalities are satisfied. This shows that $13 \nmid m$. By a similar argument, one also sees that $31 \nmid m$, and we obtain the desired contradiction for case (B). □

On the other hand, we can now see that $7 \mid k$, for otherwise the inequality

$$\frac{2m}{m+1} = \frac{\sigma(k)}{k} \leqslant \frac{\sigma(3^2\,11^2\,13^2\,17^2\,19^2)}{3^2\,11^2\,13^2\,17^2\,19^2}$$

is not possible for any $m \geqslant 49$. Let us write $k = s^2 = 3^2\,7^2\,\ell^2$ with some square-free integer ℓ; then,

$$13 \cdot 19\,\sigma(\ell^2)(m+1) = 2 \cdot 3 \cdot 7^2\,\ell^2 m. \tag{116}$$

We observe that $(13 \cdot 19) \nmid \ell$, for otherwise we have $3^2\,7^2\,13^2\,19^2 \mid k$, and this contradicts (113). Hence, by (116) it follows that $13 \mid m$ or $19 \mid m$.

In case (A), these observations imply that $m = 13^2$ or 19^2. However, if $m = 13^2$, then $5 \mid (m+1)$, and from (116) we deduce that $5 \mid k$, which contradicts Lemma 8.6. On the other hand, if $m = 19^2$, then $181 \mid (m+1)$, and from (116) we conclude that $3^2\,7^2\,13^2\,181^2 \mid k$, which contradicts (113). Hence, we can assume that (B) holds from now on.

Suppose first that $(13 \cdot 19) \mid m$. Since m is cube-free, $\omega(m) = 2$, and $m \equiv 1 \pmod{12}$, it follows that $m = 13 \cdot 19^2$ or $13^2\,19^2$. If $m = 13^2\,19^2$, then $5 \mid (m+1)$, and (116) leads to the conclusion that $5 \mid k$, which contradicts what we have already shown. On the other hand, if $m = 13 \cdot 19^2$, then (116) implies

$$2347\,\sigma(\ell^2) = 3 \cdot 7^2\,19\,\ell^2.$$

Writing $\ell = 2347q$ for some prime q, this relation becomes

$$397 \cdot 661\,(q^2+q+1) = 7 \cdot 19 \cdot 2347\,q^2,$$

which does not have an integer solution q. Therefore, $(13 \cdot 19) \nmid m$.

Next, suppose that $19 \mid \ell$ and $13 \mid m$, and write $\ell = 19q$ for some prime q; note that (113) implies $q \equiv 2 \pmod 3$. From (116) we deduce that

$$13 \cdot 127\,(q^2+q+1)(m+1) = 2 \cdot 7^2\,19\,q^2 m. \tag{117}$$

Since $q \equiv 2 \pmod 3$, it follows that $(13 \cdot 127) \mid m$. As m is cube-free, $\omega(m) = 2$, and $m \equiv 1 \pmod{12}$, we must have $m = 13 \cdot 127^2$ or $13^2\,127^2$. However, if $m = 13 \cdot 127^2$ then (117) becomes

$$17 \cdot 881\,(q^2+q+1) = 7 \cdot 19 \cdot 127\,q^2,$$

and if $m = 13^2\,127^2$ we have

$$397 \cdot 3433\,(q^2+q+1) = 7^2\,13 \cdot 19 \cdot 127\,q^2,$$

and neither equation has an integer solution q.

Finally, we are reduced to the case that $13 \mid \ell$ and $19 \mid m$. Write $\ell = 13q$ for some prime q, and note that (113) implies that $q \equiv 2 \pmod 3$ as before. From (116) it follows that

$$19 \cdot 61\,(q^2+q+1)(m+1) = 2 \cdot 7^2\,13\,q^2 m. \tag{118}$$

Since $q \equiv 2 \pmod 3$, we have $(19 \cdot 61) \mid m$. As m is cube-free, $\omega(m) = 2$, and $m \equiv 1 \pmod{12}$, we must have $m = 19^2\,61$ or $19^2\,61^2$. If $m = 19^2\,61^2$ then (118) implies

$$337 \cdot 1993\,(q^2+q+1) = 7^2\,13 \cdot 19 \cdot 61\,q^2,$$

which has no integer solution q. On the other hand, if $m = 19^2\,61$, then (118) becomes

$$11^2\,(q^2 + q + 1) = 7 \cdot 19\,q^2,$$

which implies that $q = 11$. In this case, we see that

$$n = 3^2\,7^2\,11^2\,13^2\,19^2\,61 = \mathfrak{D},$$

and this completes the proof of Theorem 8.2.

References

[1] W. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers,' *Ann. of Math. (2)* **139** (1994), no. 3, 703–722.

[2] W. Alford, A. Granville and C. Pomerance, 'On the difficulty of finding reliable witnesses,' in Algorithmic Number Theory Proceedings (ANTS-I), Lecture Notes in Computer Sci. **877** (1994), Springer-Verlag, Berlin, pp. 1–16.

[3] G. Bachman, 'On exponential sums with multiplicative coefficients, II', *Acta Arith.* **106** (2003), no. 1, 41–57.

[4] A. Balog and A. Perelli, 'Exponential sums over primes in an arithmetic progression', *Proc. Amer. Math. Soc.* **93** (1985), 578–582.

[5] W. Banks, A. Güloğlu, F. Saidak and W. Nevans, 'Descartes numbers,' CRM Proceedings and Lecture Notes, **46**, American Mathematical Society, 2008.

[6] W. Banks, A. Güloğlu and W. Nevans, 'Representations of integers as sums of primes from a Beatty sequence,' *Acta Arithmetica* **130**(2007), no. 3, 255-275.

[7] W. Banks, A. Güloğlu and W. Nevans, 'On the congruence $n \equiv a \pmod{\varphi(n)}$,' *Integers* **8(1)** (2008), A59, 8 pp. (electronic)

[8] W. Banks, A. Güloğlu and W. Nevans, 'On primitive Dirichlet characters and the Riemann hypothesis,' *Journal of Number Theory* **130**(2010), no. 3, 574-579.

[9] W. Banks, D. Hart, P. Moree and W. Nevans, 'The Nicolas and Robin inequalities with sums of two squares,' *Monatshefte für Mathematik* **157**(2009), no. 4, 303-322.

[10] W. D. Banks and F. Luca, 'Composite integers n for which $\varphi(n) \mid n-1$,' *Acta Math. Sinica, English Series* **23** (2007), no. 10, 1915–1918.

[11] W. Banks, C. Pomerance and W. Nevans, 'A remark on Giuga's conjecture and Lehmer's totient problem,' *Albanian J. Math* **3** (2009), no. 2, 81-85.

[12] W. Banks and I. Shparlinski, 'Prime numbers with Beatty sequences,' preprint, 2006 (available from `http://arxiv.org/abs/0708.1015`).

[13] Y. Bugeaud, *Approximation by algebraic numbers*. Cambridge Tracts in Mathematics, **160**. Cambridge University Press, Cambridge, 2004.

[14] R. D. Carmichael, 'Note on a new number theory function,' *Bull. Amer. Math. Soc.* **16** (1910), no. 5, 232–238.

[15] Y.-J. Choie, N. Lichiardopol, P. Moree and P Solé, 'On Robin's criterion for the Riemann hypothesis,' *J. Théor. Nombres Bordeaux* **19** (2007), 351–366.

[16] R. Descartes (1596–1650), *Œuvres de Descartes*, publiées par Charles Adam & Paul Tannery sous les auspices du Ministère de l'instruction publique, Paris, L. Cerf, 1898.

[17] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1 (pp. 3–50), 1st ed., Carnegie Inst., Washington, 1919.

[18] P. Erdős and J.-L. Nicolas, 'Sur la fonction: nombre de facteurs premiers de N,' *Enseign. Math. (2)* **27** (1981), no. 1-2, 3–27.

[19] L. Euler, 'Tractatus de numerorum doctrina capita sedecim, quae supersunt,' *Commentationes Arithmeticae* **2** (1849) p. 514; reprinted in *Opera Posthuma, 1*, pp. 14–15, 1862.

[20] L. Euler, 'De numeris amicabilibus,' *Commentationes Arithmeticae* **2** (1849) p. 630 (written in 1747); reprinted in *Opera Posthuma, 1*, p. 88, 1862.

[21] L. Gegenbauer, 'Aymptotische Gesetze der Zahlentheori', *Denkschirften Akad. Wien* **49** (1885), no. 1, 37–80.

[22] G. Giuga, 'Su una presumible proprietá caratteristica dei numeri primi,' *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat.* **14(83)** (1950), 511–528.

[23] T. H. Gronwall, 'Some asymptotic expressions in the theory of numbers,' *Trans. Amer. Math. Soc.* **14** (1913), no. 1, 113–122.

[24] A. Güloğlu and W. Nevans, 'Sums with multiplicative functions over a Beatty sequence,' *Bul. Aust. Math. Soc.* **78**(2008), no. 2, 327-334.

[25] R. K. Guy, *Unsolved Problems in Number Theory*, (§B2, pp. 45–53) 2nd ed., Springer-Verlag, New York, 1994.

[26] G. Harman, 'On the number of Carmichael numbers up to x,' *Bull. London Math. Soc.* **37** (2005), 641–650.

[27] T. L. Heath, *The Thirteen Books of Euclid's Elements*, University Press, Cambridge, 1908; 2nd ed. reprinted by Dover, New York, 1956.

[28] L. K. Hua, *Introduction to Number Theory*. Springer-Verlag, Berlin Heidelberg New York 1982.

[29] M. N. Huxley, *The distribution of prime numbers. Large sieves and zero-density theorems*. Clarendon Press, Oxford, 1972.

[30] H. Iwaniec and E. Kowalski, *Analytic number theory*. American Mathematical Society Colloquium Publications, **53**. American Mathematical Society, Providence, RI, 2004.

[31] A. Y. Khinchin, 'Zur metrischen Theorie der diophantischen Approximationen', *Math. Z.* **24** (1926), no. 4, 706–714.

[32] N. M. Korobov, *Exponential sums and their applications*. Mathematics and its Applications (Soviet Series), **80**. Kluwer Academic Publishers Group, Dordrecht, 1992.

[33] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*. Pure and Applied Mathematics. Wiley-Interscience, New York-London-Sydney, 1974.

[34] A. Kumchev, 'On sums of primes from Beatty sequences', preprint, 2007 (available from `http://arxiv.org/abs/0706.0943`).

[35] J. C. Lagarias, 'An elementary problem equivalent to the Riemann hypothesis,' *Amer. Math. Monthly* **109** (2002), no. 6, 534–543.

[36] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig, 1909.

[37] A. F. Lavrik, 'Analytic method of estimates of trigonometric sums by the primes of an arithmetic progression', (Russian) *Dokl. Akad. Nauk SSSR* **248** (1979), no. 5, 1059–1063.

[38] D. H. Lehmer, 'On Euler's totient function,' *Bull. Amer. Math. Soc.*, **38** (1932), 745–757.

[39] F. Luca and C. Pomerance, 'On composite integers n such that $\phi(n) \mid n-1$,' preprint, 2009.

[40] F. Luca, C. Pomerance and I. Shparlinski, 'On Giuga numbers,' *Int. J. Mod. Math.* **4** (2009), 13–28.

[41] H. L. Montgomery, R. C. Vaughan, 'Exponential sums with multiplicative coefficients', *Invent. Math.* **43** (1977), no. 1, 69–82.

[42] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory.* Cambridge Studies in Advanced Mathematics, **97**. Cambridge University Press, Cambridge, 2007.

[43] J. L. Nicolas, 'Petites valeurs de la fonction d'Euler,' *J. Number Theory* **17** (1983), no. 3, 375–388.

[44] K. K. Norton, 'Upper bounds for sums of powers of divisor functions', *J. Number Theory* **40** (1992), no. 1, 60–85.

[45] C. Pomerance, 'Odd perfect numbers are divisible by at least seven distinct primes,' *Acta Arithmetica* **25** (1973) pp. 265–300.

[46] C. Pomerance, 'On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$,' *Acta Arith.* **26** (1974/75), no. 3, 265–272.

[47] C. Pomerance, 'On composite n for which $\varphi(n) \mid n-1$,' *Acta Arith.* **28** (1975/76), no. 4, 387–389.

[48] C. Pomerance, 'On composite n for which $\varphi(n) \mid n-1$, II,' *Pacific J. Math.* **69** (1977), no. 1, 177–186.

[49] S. Ramanujan, 'Some formulae in the analytic theory of numbers', *Messenger Math.* **45** (1916), 81–84.

[50] O. Ramaré and R. Rumely, 'Primes in arithmetic progressions,' *Math. Comp.* **65** (1996), no. 213, 397–425.

[51] G. Robin, 'Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann,' *J. Math. Pures Appl. (9)* **63** (1984), no. 2, 187–213.

[52] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers,' *Illinois J. Math.* **6** (1962), 64–94.

[53] K. F. Roth, 'Rational approximations to algebraic numbers', *Mathematika* **2** (1955), 1–20.

[54] K. F. Roth, 'Corrigendum to "Rational approximations to algebraic numbers"', *Mathematika* **2** (1955), 168.

[55] W. M. Schmidt, *Diophantine approximation.* Lecture Notes in Mathematics, **785**. Springer, Berlin, 1980.

[56] Z. Shan, 'On composite n for which $\varphi(n)|n-1$,' *J. China Univ. Sci. Tech.*, **15** (1985), 109–112.

[57] D. Shanks, 'The second-order term in the asymptotic expansion of $B(x)$' *Math. Comp.* **18** (1964), no. 85, 75–86.

[58] W. Sierpiński, *Elementary theory of numbers*, Warsaw, 1964.

[59] R. A. Smith, 'An error term of Ramanujan', *J. Number Theory* **2** (1970), 91–96.

[60] V. Tipu, 'A note on Giuga's conjecture,' *Canad. Math. Bull.* **50** (2007), 158–160.

[61] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers.* Dover Publications, Inc., Mineola, NY, 2004.

[62] B. M. Wilson, 'Proofs of some formulae enunciated by Ramanujan', *Proc. London Math. Soc.* **21** (1922), 235–255.

[63] E. Wirsing, 'Das asymptotische Verhalten von Summen über multiplikative Funktionen'. *Math. Ann.* **143** (1961), 75–102.