

EVERY SUFFICIENTLY LARGE EVEN NUMBER IS THE SUM OF TWO PRIMES

Ricardo G. Barca

Abstract

The binary Goldbach conjecture asserts that every even integer greater than 4 is the sum of two primes. In this paper, we prove that there exists an integer $K_\alpha > 4$ such that every even integer $x > p_k^2$ can be expressed as the sum of two primes, where p_k is the k th prime number and $k > K_\alpha$. To prove this statement, we begin by introducing a type of double sieve of Eratosthenes as follows. Given a positive even integer $x > 4$, we sift from $[1, x]$ all those elements that are congruent to 0 modulo p or congruent to x modulo p , where p is a prime less than \sqrt{x} . Therefore, any integer in the interval $[\sqrt{x}, x]$ that remains unsifted is a prime q for which either $x - q = 1$ or $x - q$ is also a prime. Then, we introduce a new way of formulating a sieve, which we call the sequence of k -tuples of remainders. By means of this tool, we prove that there exists an integer $K_\alpha > 4$ such that $p_k/2$ is a lower bound for the sifting function of this sieve, for every even number x that satisfies $p_k^2 < x < p_{k+1}^2$, where $k > K_\alpha$, which implies that $x > p_k^2$ ($k > K_\alpha$) can be expressed as the sum of two primes.

1 Introduction

1.1 The sieve method and the Goldbach problem

In 1742, Goldbach wrote a letter to his friend Euler telling about a conjecture involving prime numbers. *Goldbach's conjecture: Every even number greater than 4 is the sum of two primes.* The Goldbach Conjecture is one of the oldest unproven conjectures in number theory [6]. This conjecture was verified many times with powerful computers but has not been proven. In May 26, 2013, T. Oliveira e Silva verified the conjecture for $n \leq 4 \times 10^{17}$ [8]. Mathematicians have achieved partial results in their efforts to prove this conjecture. In 1937, Vinogradov proved that every sufficiently large odd number is the sum of three primes [9]. Later, in 1973, J.R. Chen showed that every sufficiently large even number can be written as the sum of either two primes or a prime and the product of two primes [5]. In 1975, H. Montgomery and R.C. Vaughan showed that ‘most’ even numbers were expressible as the sum of two primes [7]. Recently, a proof of the related ternary Goldbach conjecture, that every odd integer greater than 5 is the sum of 3 primes, has been given by Harald Helfgott [10].

In this paper, we prove (Main Theorem, Section 8) the following: *There exists an integer $K_\alpha > 4$ such that every even integer greater than p_k^2 ($k > K_\alpha$) is the sum of two primes.* This proof is intended as a first step towards the resolution of the Goldbach problem.

One of the principal means of addressing the Goldbach conjecture has been sieve methods. Viggo Brun [4] was the first to obtain a result, as an approximation to Goldbach’s conjecture: *Every sufficiently large even integer is a sum of two integers, each having at most nine prime factors.* Later, other mathematicians in the area of sieve theory improved upon this initial result.

In the context of sieve theory, the sieve method consists of removing the elements of a list of integers, according to a set of rules; for instance, given a finite sequence A of integers, we could remove from A those members that lie in a given collection of arithmetic progressions. In the original sieve of Eratosthenes, we start with the integers in the interval $[1, x]$, where x is a positive real number, and sift out all those that are divisible by the primes $p < \sqrt{x}$. Therefore, any integer that remains unsifted is a prime in the interval $[\sqrt{x}, x]$.

We begin by briefly describing the sieve problem; we use, as far as possible, the concepts and notation in the book by Cojocaru and Ram Murty [2], Chapters 2 and 5. Let \mathcal{A} be a finite set of integers, let \mathcal{P} be the sequence of all primes, and let $z \geq 2$ be a positive real number. Furthermore, for each $p \in \mathcal{P}$, $p < z$ we have associated a subset \mathcal{A}_p of \mathcal{A} . The *sieve problem* is to estimate, from above and below, the size of the set

$$\mathcal{A} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p < z}} \mathcal{A}_p,$$

which consists of the elements of the set \mathcal{A} after removing the elements of all the subsets \mathcal{A}_p . We call the procedure of removing the elements of the subsets \mathcal{A}_p from the set \mathcal{A} the *sifting process*. The *sifting function* $S(\mathcal{A}, \mathcal{P}, z)$ is defined by the equation

$$S(\mathcal{A}, \mathcal{P}, z) = \left| \mathcal{A} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p < z}} \mathcal{A}_p \right|$$

and counts the elements of \mathcal{A} that have survived the sifting process. Now, let \mathcal{P}_z be the set of primes $p \in \mathcal{P}, p < z$, and for each subset I of \mathcal{P}_z , denote

$$\mathcal{A}_I = \bigcap_{p \in I} \mathcal{A}_p.$$

Then, the inclusion–exclusion principle gives us

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{I \subseteq \mathcal{P}_z} (-1)^{|I|} |\mathcal{A}_I|,$$

where for the empty set \emptyset , we have $\mathcal{A}_\emptyset = \mathcal{A}$. We often take \mathcal{A} to be a finite set of positive integers and \mathcal{A}_p to be the subset of \mathcal{A} consisting of elements lying in some congruence classes modulo p .

Using this notation, we can now formally define the sieve of Eratosthenes. Let $\mathcal{A} = \{n \in \mathbb{Z}_+ : n \leq x\}$, where $x \in \mathbb{R}, x > 1$, and let \mathcal{P} be the sequence of all primes. Let $z = \sqrt{x}$, and

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p.$$

Now, to each $p \in \mathcal{P}, p < z$, we associate the subset \mathcal{A}_p of \mathcal{A} , defined as follows: $\mathcal{A}_p = \{n \in \mathcal{A} : n \equiv 0 \pmod{p}\}$. Then, when we sift from \mathcal{A} all the elements of every set \mathcal{A}_p , the unsifted members of \mathcal{A} in the interval $[\sqrt{x}, x)$ are integers that are not divisible by primes of \mathcal{P} less than z ; that is to say, any integer remaining in $[\sqrt{x}, x)$ is a prime. Furthermore, if d is a squarefree integer such that $d|P(z)$, we define the set

$$\mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p.$$

Thus, from the inclusion–exclusion principle, we obtain

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d) |\mathcal{A}_d|, \tag{1}$$

where $\mu(d)$ is the Möbius function. Moreover, from (1), the Legendre formula can be derived

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d) |\mathcal{A}_d| = \sum_{d|P(z)} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

The sieve of Eratosthenes is useful for finding the prime numbers between \sqrt{x} and x . However, from a theoretical perspective, the experts in sieve theory are interested in estimating, for every x , the number of integers remaining after the sifting process has been performed.

The Möbius function is a simple way to approach a sieve problem; however, satisfactory results are difficult to achieve unless z is very small. We illustrate this problem with the special case given in the book by Halberstam and Richert [1], Chapter 1, Section 5.

Let $\mathcal{A} = \{n \in \mathbb{Z}_+ : n \leq x\}$, and let $2 \leq z \leq x$. As usual in sieve theory, instead of $|\mathcal{A}|$, we can use a close approximation X to $|\mathcal{A}|$. Furthermore, for each prime p we choose a multiplicative function $w(p)$ such that $(w(p)/p)X$ approximates to $|\mathcal{A}_p|$. Then, for each squarefree integer d , we have that $(w(d)/d)X$ approximates to $|\mathcal{A}_d|$, and we can write

$$|\mathcal{A}_d| = \frac{w(d)}{d} X + R_d,$$

where R_d is the remainder term. Then, substituting this result into (1) gives

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d) \left(\frac{w(d)}{d} X + R_d \right) = \sum_{d|P(z)} \mu(d) \frac{w(d)}{d} X + \sum_{d|P(z)} \mu(d) R_d. \quad (2)$$

On the other hand, since w is a multiplicative function,

$$\sum_{d|P(z)} \mu(d) \frac{w(d)}{d} = \prod_{\substack{p \in \mathcal{P} \\ p < z}} \left(1 - \frac{w(p)}{p} \right) = W(z),$$

and substituting this result into (2) gives

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \sum_{d|P(z)} \mu(d) R_d.$$

Hence, we can write

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \theta \sum_{d|P(z)} |R_d| \quad (|\theta| \leq 1).$$

Furthermore, if we impose the conditions $|R_d| \leq w(d)$ and $w(p) \leq A_0$, for some constant $A_0 \geq 1$, we obtain

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \theta(1 + A_0)^z.$$

See [1, Theorem 1.1] for details. Now, taking $X = x$, $w(p) = 1$, and $A_0 = 1$, these conditions are satisfied, and we obtain

$$S(\mathcal{A}, \mathcal{P}, z) \leq x \prod_{\substack{p \in \mathcal{P} \\ p < z}} \left(1 - \frac{1}{p} \right) + 2^z. \quad (3)$$

From this illustrative case, we can see that the error term will be very large provided that z is not sufficiently small compared to x . Regardless, taking $z = \log x$, the formula in (3) can be used to obtain an elementary upper bound for $\pi(x)$. See [1, Ch. 1, (5.8)].

Now, suppose that the Goldbach problem is expressed as a sieve problem; clearly, a lower bound for the sifting function is required to prove this conjecture. However, a well-known phenomenon exists in sieve theory called the ‘parity barrier’ or the ‘parity problem’, which was first explained by Selberg (see [12]): sieve methods cannot distinguish between numbers with an even number of prime factors and an odd number of prime factors. The parity problem was described briefly by Terence Tao [11] as follows: ‘If A is a set whose elements are all products of an odd number of primes (or are all products of an even number of primes), then (without injecting additional ingredients), sieve theory is unable to provide non-trivial lower bounds on the size of A .’ This means that in order to solve the Goldbach problem, a suitable sieve must be found first; then, new procedures for estimating the sifting function must be introduced, which is very different from the usual methods of current sieve theory.

1.2 A sieve for the Goldbach problem

Let \mathcal{P} be the sequence of all primes, and given $p_k \in \mathcal{P}$, let $m_k = p_1 p_2 p_3 \cdots p_k$ (see Definition 2.4). Henceforth, for convenience, we take x to be an even integer greater than $p_4^2 = 49$ unless specified otherwise. Note that if p_k is the greatest prime less than \sqrt{x} , every even number $x > 49$ satisfies $p_k^2 < x < p_{k+1}^2 < m_k$; this fact is highly important for our purposes, as we shall see later.

Now, how can we construct a sieve to address the Goldbach problem? Given a positive even integer x , the sieve of Eratosthenes can be used to obtain the primes between \sqrt{x} and x . Assume that among the primes between \sqrt{x} and x there is at least one prime q such that $x - q$ is also a prime. Then, to address the Goldbach problem we require a sieve that can sift out all the integers in the interval $[1, x]$ that are divisible by the primes $p < \sqrt{x}$, as the sieve of Eratosthenes does, and that additionally can sift out from the primes q remaining in $[\sqrt{x}, x]$ all those such that $x - q$ is not a prime.

To construct such a sieve, we propose a modification of the sieve of Eratosthenes as follows. First, we sift out all the integers n in the interval $[1, x]$ such that $n \equiv 0 \pmod{p}$, where $p < \sqrt{x}$; thus, any integer that remains unsifted is a prime in the interval $[\sqrt{x}, x]$. Next, we sift out all the integers n that remain in $[\sqrt{x}, x]$ such that $n \equiv x \pmod{p}$.

Clearly, any number that remains unsifted in $[\sqrt{x}, x]$ is a prime q such that $x - q$ is not divisible by the primes $p < \sqrt{x}$; thus, either $x - q = 1$ or $x - q$ is a prime. We call it the Sieve associated with x , or alternatively the *Sieve I*.

More formally, let $\mathcal{A} = \{n \in \mathbb{Z}_+ : n \leq x\}$. Let \mathcal{P} be the sequence of all primes, and let $z = \sqrt{x}$. Let

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p = m_k.$$

Now, to each $p \in \mathcal{P}$, $p < z$, we associate the subset \mathcal{A}_p of \mathcal{A} , defined as follows: $\mathcal{A}_p = \{n \in \mathcal{A} : n \equiv 0 \pmod{p} \text{ or } n \equiv x \pmod{p}\}$. Furthermore, if d is a squarefree integer such that $d|P(z)$, we define the set

$$\mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p.$$

In this case, the sifting function

$$S(\mathcal{A}, \mathcal{P}, z) = \left| \mathcal{A} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p < z}} \mathcal{A}_p \right|$$

counts the primes q in the interval $[\sqrt{x}, x]$, such that $x - q$ is also a prime in $[\sqrt{x}, x]$ and counts 1 and $x - 1$ whenever $x - 1$ is a prime (see Theorem 8.1). As in the case of the sieve of Eratosthenes–Legendre, the inclusion–exclusion principle gives us

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d) |\mathcal{A}_d|.$$

Now, $S(\mathcal{A}, \mathcal{P}, z) > 2$ implies that x is the sum of two primes, and if this fact is proved for all x , the Goldbach conjecture would be proved. However, we cannot find a suitable lower bound for $S(\mathcal{A}, \mathcal{P}, z)$ by using the usual sieve methods due to the parity problem mentioned in this Introduction. Thus far, all attempts to solve the Goldbach problem by the usual sieve techniques have not succeeded. Therefore, the strategy used in this paper differs substantially from the usual approach in sieve theory. In the next subsection, we begin by introducing another way of formulating a sieve problem.

1.3 The sequence of k -tuples of remainders

In this paper, we propose to use another formulation for this type of sieve that is able to illustrate all the details of the sifting process and will allow us to obtain a lower bound for the number of elements that remain unsifted. For this purpose, we begin by introducing the notion of the sequence of k -tuples of remainders. Let $\{p_1, p_2, p_3, \dots, p_k\}$ be the ordered set of the first k prime numbers. Suppose that for every natural number n , we form a k -tuple, the elements of which are the remainders of dividing n by $p_1, p_2, p_3, \dots, p_k$; thus, we have a sequence of k -tuples of remainders. If we arrange these k -tuples from top to bottom, the sequence of k -tuples of remainders can be seen as a matrix formed by k columns and infinitely many rows, where each column is a periodic sequence of remainders modulo $p_h \in \{p_1, p_2, p_3, \dots, p_k\}$. The sequence of k -tuples of remainders can easily be proven to be periodic, and the period is $m_k = p_1 p_2 p_3 \cdots p_k$ (see Proposition 2.1).

Suppose that within the periods of every sequence of remainders modulo p_h (a given column of the matrix), we define some (not all) of the remainders as *selected* remainders, regardless of the criterion for selecting the remainders. Consequently, some k -tuples have one or more selected remainders, and other k -tuples do not have any selected remainder. If a given k -tuple has one or more selected remainders, we say that it is a *prohibited* k -tuple; otherwise, we say that it is a *permitted* k -tuple. We more formally define the sequence of k -tuples and related concepts in Section 2.

Now, in a general context, a sieve is a tool or device that separates, for instance, coarser from finer particles. Then, given a sieve device, we can define a ‘sieve problem’, for instance, to count the number of finer particles that pass through the sieve device. We can think of a sequence of k -tuples as a ‘sieve device’, in the sense that when a set of integers is ‘fed’ into the sieve device (the sequence of k -tuples), the integers associated to permitted k -tuples are separated from integers associated to prohibited k -tuples. The sieve problem, in this case, is to estimate the number of integers that ‘pass through’ the sieve device, that is, to estimate the number of permitted k -tuples attached to some of the integers in the input set.

Given an even integer $x > 49$, we formulate Sieve I (the Sieve associated with x) by means of a sequence of k -tuples as follows. Let \mathcal{P} be the sequence of all primes; let $z = \sqrt{x}$, and let p_k be the greatest prime less than

z . With the index k corresponding to the prime p_k , we construct the sequence of k -tuples of remainders, where the rules for selecting remainders are the following: If a given k -tuple of the sequence has 0 as an element or has its h th element equal to the remainder of dividing x by $p_h \in \{p_1, p_2, p_3, \dots, p_k\}$, these elements are defined as selected remainders. Therefore, within the periods of every sequence of remainders modulo p_h (a given column of the matrix), the remainder 0 is always a selected remainder; moreover, if p_h does not divide x , the resulting remainder is a second selected remainder. Let \mathcal{A} be the set consisting of the indices n of the sequence of k -tuples that lie in the interval $[1, x]$. For each $p \in \mathcal{P}$, $p < z$, the set $\mathcal{A}_p \subset \mathcal{A}$ consists of the indices n for which the corresponding element in the sequence of remainders modulo p is a selected remainder. Then, the indices of the prohibited k -tuples lying in \mathcal{A} are sifted out, and the indices of the permitted k -tuples lying in \mathcal{A} remain unsifted. The *sifting* function is given by the number of permitted k -tuples whose indices lie in the interval $[1, x]$. In Section 8, we more formally define the formulation of Sieve I based on a sequence of k -tuples.

Remark 1.1. Note that given a k -tuple whose index is $n < x$, if $n \equiv 0 \pmod{p}$ or $n \equiv x \pmod{p}$ for at least one $p < \sqrt{x}$, then it is a prohibited k -tuple, and if $n \not\equiv 0 \pmod{p}$ and $n \not\equiv x \pmod{p}$ for every $p < \sqrt{x}$, then it is a permitted k -tuple.

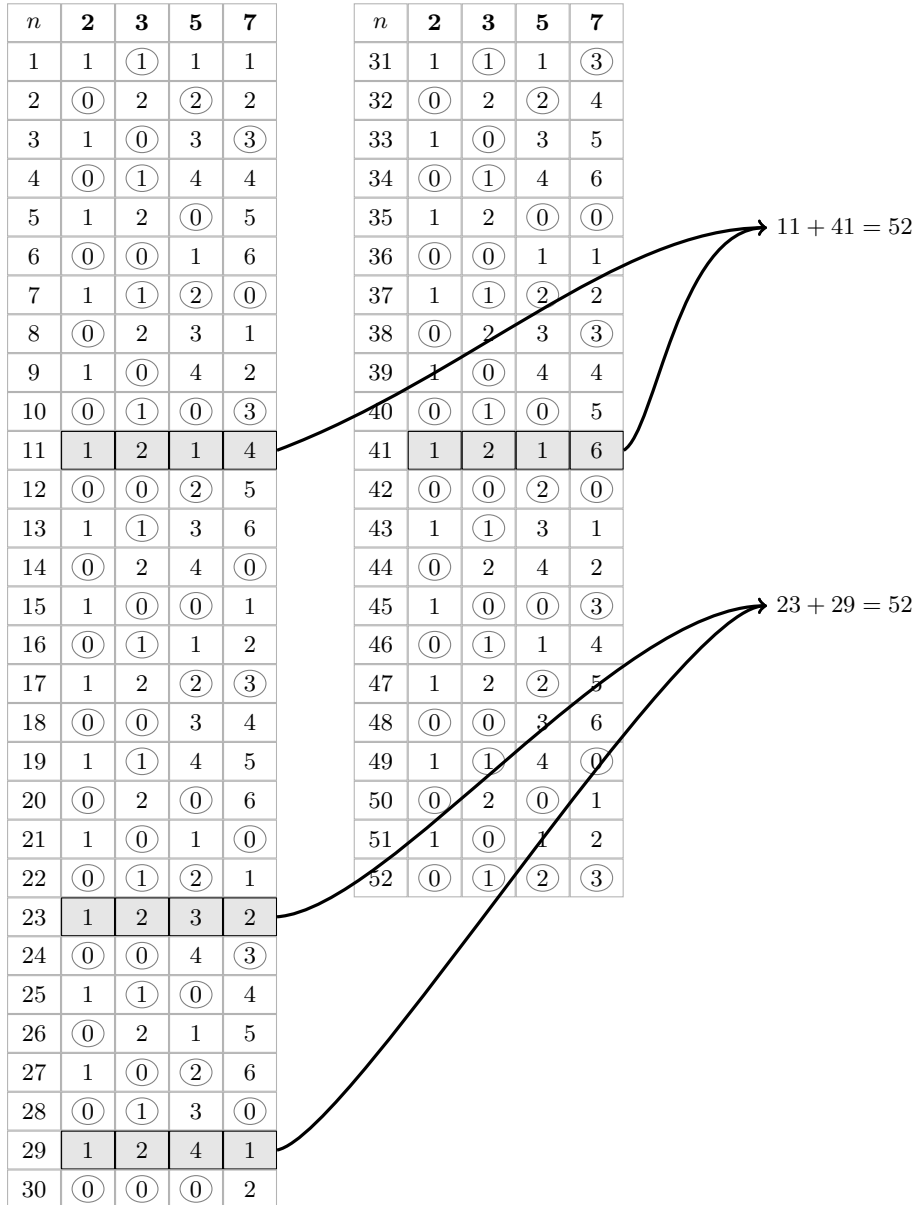


Figure 1

Therefore, given an even integer $x > 49$ ($p_k^2 < x < p_{k+1}^2$), the ordered set of k -tuples whose indices lie in the interval $[1, x]$ of the sequence is only an alternative formulation of the Sieve associated with x (Sieve I), which was described before by using the usual sieve theory notation. We shall prove (Theorem 8.1) that the indices (greater than 1) of the permitted k -tuples lying within $[1, x]$ are primes q such that either $x - q$ is a prime or $x - q = 1$. Note

that this form of the sieve gives us a detailed picture of the sifting process; other reasons for using this formulation for sieves based on a sequence of k -tuples will be explained later.

Example 1.1. Figure 1 illustrates how Sieve I can be used to find some Goldbach partitions for the even number $x = 52$. We proceed as follows:

1. We make a list of the primes less than $\sqrt{52}$. We obtain $\{2, 3, 5, 7\}$.
2. We compute the remainders of dividing $x = 52$ by the prime moduli of the list. We obtain $\{0, 1, 2, 3\}$.
3. In every k -tuple, we select each 0 and the elements $\{1, 2, 3\}$ corresponding to the moduli $\{3, 5, 7\}$, respectively. (The selected remainders are circled.)
4. Now, we colour grey the permitted k -tuples. The arrows show the corresponding Goldbach partitions. Note that there is no permitted k -tuple for the partition $47 + 5$.

1.4 Auxiliary Sieve II

To prove the main theorem, we need to find a lower bound for the sifting function of the Sieve associated to x for every even number $x > p_k^2$, where k is sufficiently large. However, we can see that, regardless of the formulation, Sieve I is a ‘static’ sieve; that is, given an even number x , we can formulate a specific Sieve I for the even number x . For our purposes, we require a ‘dynamic’ sieve that works as $x \rightarrow \infty$. Suppose that given $x > 49$ and using Sieve I we have a way to compute the number of permitted k -tuples whose indices lie in $[1, x]$; then, we could prove the main theorem by constructing a sequence of sieves associated with every even number $x > 49$; that is, we could construct a sequence where the elements are sequences of k -tuples, each one for every even number $x > 49$, and compute the number of permitted k -tuples whose indices lie in the interval $[1, x]$ of each sequence of k -tuples.

Now, using Sieve I, the implementation of this idea faces some difficulties. For instance, if $x = 50$, Sieve I can be described as follows. Since the greatest prime less than $\sqrt{50}$ is $p_4 = 7$, we have $k = 4$; thus, we construct the sequence of 4-tuples of remainders. In every 4-tuple of the sequence, if the h th element is 0 or is equal to the remainder of dividing x by $p_h \in \{p_1, p_2, p_3, p_4\}$, this element is a selected remainder. Let \mathcal{A} be the set consisting of the indices of the sequence of 4-tuples that lie in the interval $[1, 50]$.

Suppose that we proceed to the next even integer $x = 52$. In this case, we again have $k = 4$, and the sequence of 4-tuples of remainders is the same as before. However, the set \mathcal{A} now consists of the indices that lie in $[1, 52]$, and the selected remainders take specific values for $x = 52$. In addition, as x runs through the even numbers, when $x > 121$, we have $k > 4$ because the greatest prime less than \sqrt{x} will be $p_k > p_4$. The difficulty resides in the handling of all these variables as x proceeds through all the even numbers. On the other hand, given $k \geq 4$, when x is divisible by a prime $p_h \in \{p_1, p_2, p_3, \dots, p_k\}$, the remainder is 0; therefore, in each sequence of remainders modulo p_h ($1 \leq h \leq k$) that form the sequence of k -tuples, there could exist one or two selected remainders within the period of the sequence (see Remark 8.1). This problem is an additional serious difficulty in deriving a formula for computing the sifting function.

For all these reasons, a more general kind of sieve is preferred, for which the sequence of k -tuples is more ‘homogeneous’ than that corresponding to Sieve I in the sense that in each sequence of remainders modulo p_h ($1 < h \leq k$) that form the sequence of k -tuples of this new sieve, there always exist two selected remainders in every period of the sequence. Therefore, we introduce another sieve, which we call simply *Sieve II*. We describe Sieve II in the form proposed previously by means of a sequence of k -tuples, as follows. Let \mathcal{P} be the sequence of all primes, and let p_k ($k \geq 4$) be a prime of the sequence. With the index k corresponding to the prime p_k , we construct the sequence of k -tuples of remainders, where the rules for selecting remainders are the following. In every sequence of remainders modulo p_h ($1 < h \leq k$) that form the sequence of k -tuples, there are always two selected remainders r and r' modulo p_h . In the sequence of remainders modulo $p_1 = 2$, there is only one selected remainder r modulo p_1 . Let \mathcal{B} be the set consisting of the indices of the sequence of k -tuples that lie in the interval $[1, y]$, where y is an integer that satisfies $y > p_k$. For each $p \in \mathcal{P}$, $p \leq p_k$, the set $\mathcal{B}_p \subset \mathcal{B}$ consists of the indices n for which the corresponding element in the sequence of remainders modulo p is a selected remainder. The indices of the prohibited k -tuples lying in \mathcal{B} are sifted out, and the indices of the permitted k -tuples lying in \mathcal{B} remain unsifted. The sifting function is defined by the equation

$$T(\mathcal{B}, \mathcal{P}, p_k) = \left| \mathcal{B} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p \leq p_k}} \mathcal{B}_p \right|,$$

and counts the number of permitted k -tuples whose indices lie in \mathcal{B} . We more formally define Sieve II in Section 2.

Remark 1.2. In this case, given a k -tuple whose index is n , if $n \equiv r \pmod{p}$ or $n \equiv r' \pmod{p}$ for at least one $p \leq p_k$, where r, r' are the selected remainders modulo p , then it is a prohibited k -tuple, and if $n \not\equiv r \pmod{p}$ and $n \not\equiv r' \pmod{p}$ for every $p \leq p_k$, then it is a permitted k -tuple.

Note that the unsifted elements in \mathcal{B} may or may not be prime numbers; indeed, Sieve II is a collection of sieves, one for each particular choice of selected remainder.

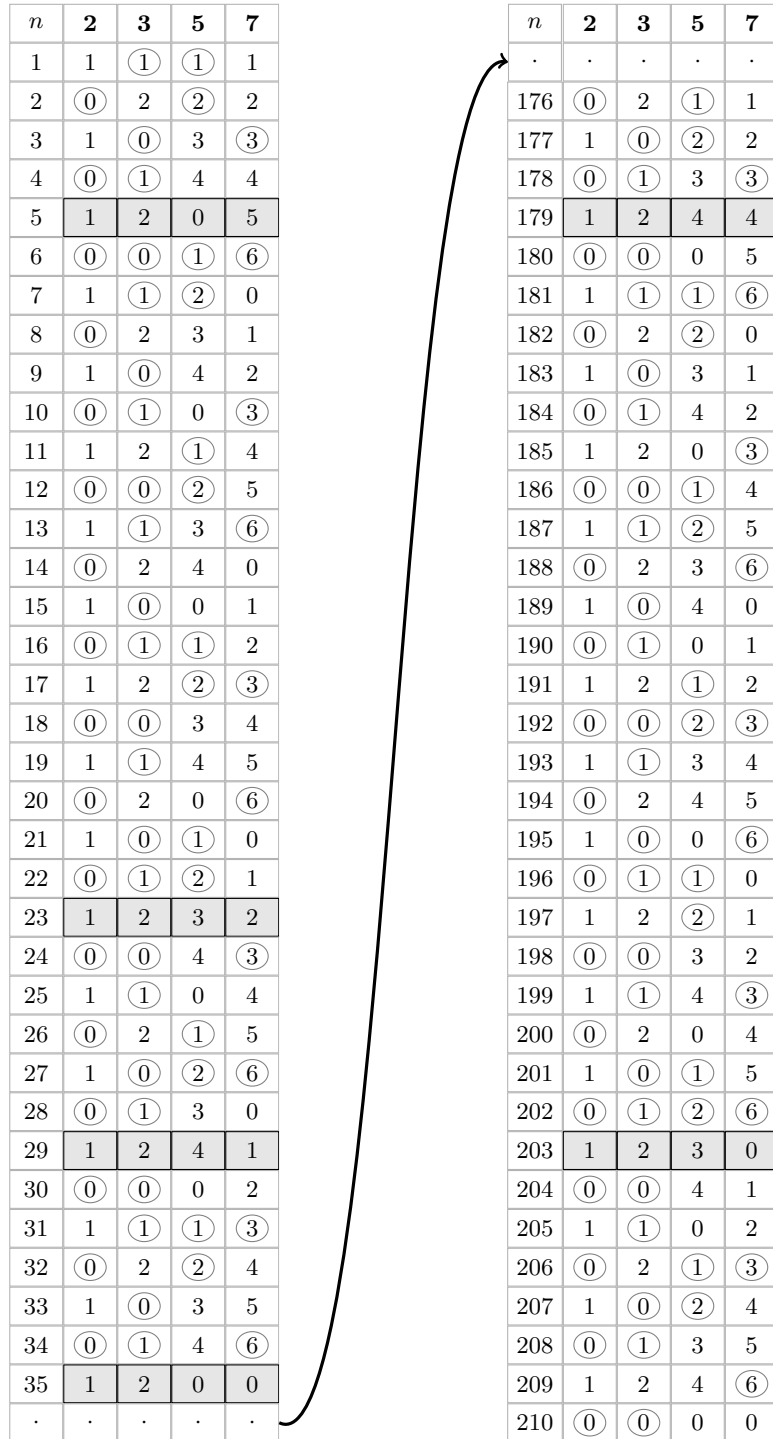


Figure 2

Now, suppose that in Sieve II, we take $\mathcal{B} = \{n : 1 \leq n \leq p_k^2\}$. Given an even number $x > 49$ that satisfies $p_k^2 < x < p_{k+1}^2$, we can construct the sequence of k -tuples associated to Sieve I, and using the same k , we can construct the sequence of k -tuples associated to Sieve II. Thus, we can compare, for every even number $x > 49$, the sifting function of Sieve I with the sifting function of the attached Sieve II. That is, we can compare the number of permitted k -tuples whose indices lie in the interval $[1, x]$ of the sequence of k -tuples corresponding to Sieve I with the number of permitted k -tuples whose indices lie in the interval $[1, p_k^2]$ of the sequence of k -tuples corresponding to Sieve II. We shall prove later (Lemma 8.2) that for every even number $x > 49$, under the given conditions, the value of the sifting function corresponding to Sieve I is greater than or equal to the minimum value of the sifting function corresponding

to Sieve II.

Example 1.2. For $k = 4$ ($p_k = 7$), the period of the sequence of k -tuples is equal to 210. The first 35 and the last 35 of the 4-tuples in the interval $[1, 210]$ (the first period of the sequence) are pictured in Figure 2 for a given choice of selected remainders. Sieve II is given by the k -tuples whose indices lie in $[1, 7^2]$.

We can now construct a sequence indexed by k , where every element of the sequence is a sequence of k -tuples; that is, we have a sequence of sequences of k -tuples. In each of these sequences of k -tuples, we have a Sieve II, which is given by the ordered set of k -tuples whose indices lie in the interval $[1, p_k^2]$ of the sequence of k -tuples. Therefore, our problem is now, given Sieve II, how to compute the number of permitted k -tuples whose indices lie within $[1, p_k^2]$.

1.5 Using the inclusion–exclusion principle for computing the number of permitted k -tuples in a period of the sequence of k -tuples of Sieve II

The sieve method usually consists of operations on the formula given by the inclusion–exclusion principle to obtain bounds for the sifting function, as we have illustrated in the first subsection. In our approach, the starting point is also the inclusion–exclusion principle, but only as a first step towards obtaining a lower bound for the sifting function of Sieve II. That is, from the formula given by this principle, we compute the number of permitted k -tuples within a period of the corresponding sequence of k -tuples, as follows.

Let us again consider Sieve II but now taking $\mathcal{B} = \{n : 1 \leq n \leq m_k\}$; that is, \mathcal{B} is now the set of indices corresponding to the first period of the sequence of k -tuples. Given $p \in \mathcal{P}$, $2 < p \leq p_k$, we have $|\mathcal{B}_p| = 2m_k/p$ since $p|m_k$ and there are two selected remainders r, r' for each modulus $p > 2$, by definition. Furthermore, given a squarefree integer d such that $d|m_k, 2 \nmid d$, the set \mathcal{B}_d is the intersection of the subsets \mathcal{B}_p such that $p|d$ ($p \neq 2$). Hence,

$$|\mathcal{B}_d| = \frac{2^{\nu(d)}}{d} m_k \quad (d|m_k, 2 \nmid d),$$

where $\nu(d)$ is the number of distinct prime divisors of d . Furthermore, we have the identity

$$\sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) \frac{2^{\nu(d)}}{d} = \prod_{\substack{2 < p \leq p_k \\ p \in \mathcal{P}}} \left(1 - \frac{2}{p}\right). \quad (4)$$

On the other hand, the subset \mathcal{B}_{p_1} consists of the integers $n \in \mathcal{B}$ such that $n \equiv r \pmod{p_1}$, where r is the selected remainder for the modulus p_1 in the sequence of k -tuples of Sieve II. Then, $|\mathcal{B}_{p_1}| = m_k/p_1$ since $p_1|m_k$ and there is only one selected remainder for the modulus p_1 , by definition. Furthermore, given a squarefree integer d such that $d|m_k, 2 \mid d$, the set \mathcal{B}_d is the intersection of the subsets \mathcal{B}_p such that $p|d$, and one subset \mathcal{B}_p is \mathcal{B}_{p_1} . Hence,

$$|\mathcal{B}_d| = \frac{2^{\nu(d)-1}}{d} m_k \quad (d|m_k, 2 \mid d).$$

Now, by the inclusion–exclusion principle,

$$\begin{aligned} T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k) &= \sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) |\mathcal{B}_d| = \sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) \frac{2^{\nu(d)}}{d} m_k + \sum_{\substack{d|m_k \\ 2 \mid d}} \mu(d) \frac{2^{\nu(d)-1}}{d} m_k = \\ &= \sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) \frac{2^{\nu(d)}}{d} m_k - \frac{1}{2} \sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) \frac{2^{\nu(d)}}{d} m_k = \frac{1}{2} \sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) \frac{2^{\nu(d)}}{d} m_k. \end{aligned}$$

Thus, by means of (4), we can see that the number of permitted k -tuples whose indices lie in the interval $[1, m_k]$ (the first period of the sequence of k -tuples associated to Sieve II) is given by

$$T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k) = \frac{1}{2} m_k \prod_{\substack{2 < p \leq p_k \\ p \in \mathcal{P}}} \left(1 - \frac{2}{p}\right), \quad (5)$$

regardless of the selected remainders $r, r' \pmod{p}$, for every $p \in \mathcal{P}$, $p \leq p_k$.

1.6 The structure of the first period of the sequence of k -tuples of remainders

Until now, we have arranged the elements of each k -tuple horizontally, from left to right, and we have arranged the k -tuples of the sequence vertically, from top to bottom. Hence, the first period of the sequence of k -tuples can be seen as a matrix, with columns from $h = 1$ to $h = k$ and $m_k = p_1 p_2 p_3 \cdots p_k$ rows. Note that for each h ($1 \leq h \leq k$), we also have a sequence of h -tuples with period $m_h = p_1 p_2 p_3 \cdots p_h$.

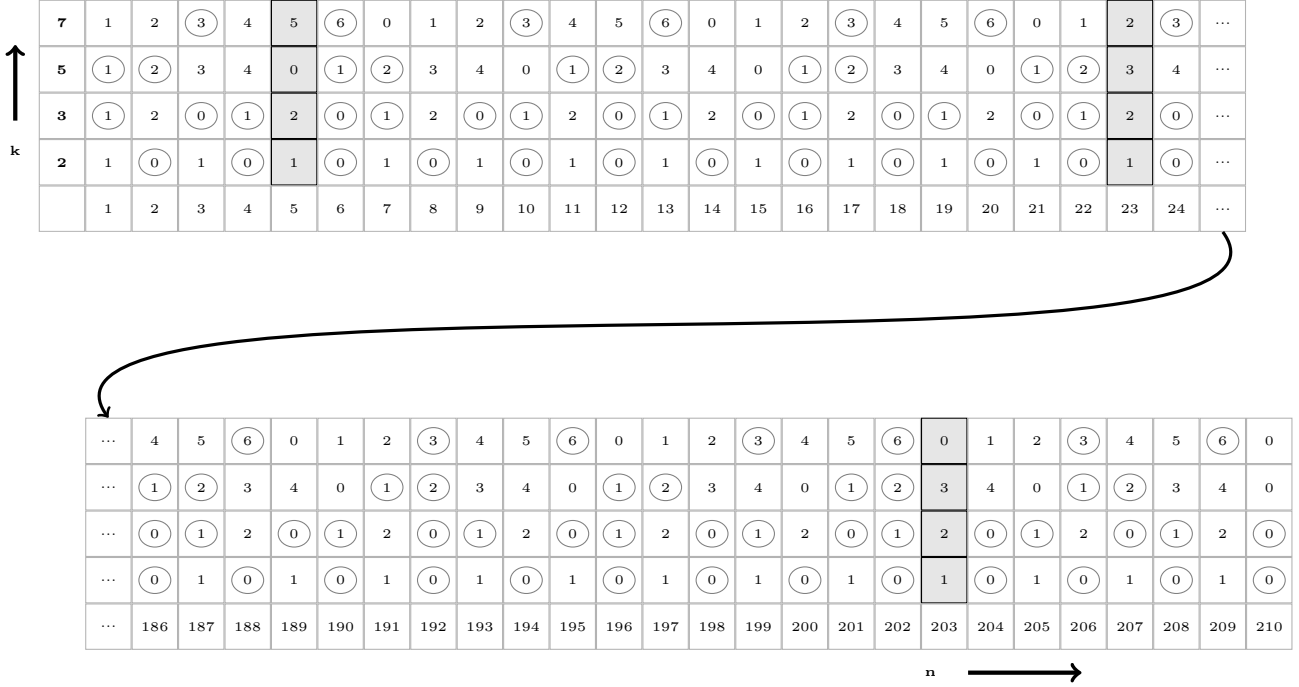


Figure 3

Consider now the sequence of k -tuples in horizontal position (see Definition 3.1). Consequently, we can think of the first period of the sequence of k -tuples as a matrix formed by k rows and m_k columns. Each row of this matrix, from $h = 1$ to $h = k$, is formed by the remainders of dividing the integers from $n = 1$ to $n = m_k$ by the modulus p_h . For every n ($1 \leq n \leq m_k$), the corresponding column matrix is the k -tuple of the remainders of dividing n by the moduli p_1, p_2, \dots, p_k .

Note that if we let $k \rightarrow \infty$, the period of the sequence and the size of the involved k -tuples grow simultaneously.

Example 1.3. Figure 3 illustrates the first period of the sequence of 4-tuples pictured in Figure 2 in horizontal position.

The sequences of k -tuples in general are defined more formally in Section 2; now, we require the following definition.

Definition 1.1. Given a sequence of k -tuples and using the order relation given by index n , we define an interval of k -tuples, denoted by $I[m, n]_k$, to be the set of consecutive k -tuples associated with an integer interval $[m, n] \cap \mathbb{Z}_+$, where m is the index of the first k -tuple, and n is the index of the last k -tuple. We also use the notation $I[m, n] = I[m, n]_k$ for this interval. We define the *size* of $I[m, n]$ by the equation $|I[m, n]| = n - m + 1$, and we use the notation $I[\]_k$, or alternatively $I[\]$, to denote the empty interval.

Specifically, let us consider the sequence of k -tuples associated to Sieve II. Since this sequence is periodic, it suffices to consider the first period, between $n = 1$ and $n = m_k$ (the interval $I[1, m_k]$). Note that for $p_k \geq 7$ ($k \geq 4$), the interval $I[1, p_k^2]$ is completely included within the first period of the sequence of k -tuples. Although this is the interval that interests us, to understand the properties of the sequence of k -tuples and the behaviour as $k \rightarrow \infty$, the entire fundamental period of the sequence, not just the interval $I[1, p_k^2]$, must be studied.

The following step in our approach consists of dividing the first period of the sequence of k -tuples into two parts: the left interval $I[1, p_k^2]$ and the right interval $I[p_k^2 + 1, m_k]$ (see Definition 6.3). Since for every h ($1 \leq h \leq k$), there is a sequence of h -tuples of remainders, the interval $I[1, m_k]_h$ of each sequence is subdivided into two intervals: the left interval $I[1, p_k^2]_h$ and the right interval $I[p_k^2 + 1, m_k]_h$. If we think of the first period of the sequence of k -tuples as a matrix, we can see that this matrix has been partitioned into two blocks: the left block, formed by the columns from $n = 1$ to $n = p_k^2$; and the right block, formed by the columns from $n = p_k^2 + 1$ to $n = m_k$.

Recall that within the first period of the sequence of k -tuples (the interval $I[1, m_k]$), the exact number of permitted k -tuples is given by (5). Furthermore, for every h such that $1 \leq h < k$, since the number of permitted h -tuples in a period of the sequence of h -tuples is given by (5) and the period m_h divides m_k , we can compute precisely the

number of permitted h -tuples in each interval $I[1, m_k]_h$. For every h ($1 \leq h \leq k$), the number of permitted h -tuples in $I[1, m_k]_h$ is the same, regardless of the choice of the selected remainders in the sequence of h -tuples. However, within both the left interval $I[1, p_k^2]_h$ and the right interval $I[p_k^2 + 1, m_k]_h$, the number of permitted h -tuples could change when the selected remainders in the sequence of h -tuples are changed because the positions of the permitted h -tuples along the interval $I[1, m_k]_h$ are modified.

The following question may have occurred to the reader at this point: What is the advantage of the formulation of sieves based on a sequence of k -tuples of remainders? We shall explain the principal reason in what follows.

Let us consider again the sequence of k -tuples of Sieve II, in horizontal position, where $k \geq 4$. For a given choice of selected remainders, the interval $I[1, p_k^2]$ of this sequence is a sieve device that sifts out the prohibited k -tuples that lie in $I[1, p_k^2]$ and allows the permitted k -tuples in this interval to remain. Furthermore, for every h ($1 \leq h < k$), there is also a sequence of h -tuples of remainders and the interval $I[1, p_k^2]_h$ of every sequence is also a sieve device that sifts out the prohibited h -tuples and allows the permitted h -tuples in $I[1, p_k^2]_h$ to remain. Thus, we have decomposed the sifting process into several stages, from $h = 1$ to $h = k$, where each ‘partial’ sieve device contributes to the whole sifting process. Hence, we can study the behaviour of these partial sieve devices to determine the behaviour of the overall sieve; the advantage of this perspective will become apparent in the rest of this section. It is obvious that as h goes from 1 to k , the number of permitted h -tuples decreases as a result of the sifting process in each stage of the entire sifting process.

1.7 The density of permitted k -tuples

In Sieve II, we have taken first the set $\mathcal{B} = \{n : 1 \leq n \leq p_k^2\}$; therefore, the sifting function $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$ is equal to the number of permitted k -tuples in the interval $I[1, p_k^2]$ of the sequence of k -tuples associated to Sieve II. However, this sifting function depends on the choice of the selected remainders in the sequence of k -tuples associated to Sieve II. Obtaining of a lower bound for this sifting function is the main task of this paper.

On the other hand, in Sieve II, we have next taken the set $\mathcal{B} = \{n : 1 \leq n \leq m_k\}$; here, the sifting function $T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k)$ is equal to the number of permitted k -tuples in the interval $I[1, m_k]$ of the sequence of k -tuples associated to Sieve II. In this case, the sifting function does not depend on the choice of the selected remainders in the sequence of k -tuples and can be computed precisely using (5).

A natural question arises: How can we take advantage of the exact computation of $T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k)$ for obtaining an estimate of $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$?

Let us consider the interval $I[1, m_k]$ (the first period of the sequence of k -tuples of Sieve II); furthermore, consider the intervals $I[1, p_k^2]$ and $I[p_k^2 + 1, m_k]$. For a given choice of selected remainders in the sequence of k -tuples, if the proportion of permitted k -tuples in $I[1, p_k^2]$ is less than the proportion in $I[1, m_k]$, the proportion of permitted k -tuples in $I[p_k^2 + 1, m_k]$ must be greater than the proportion in $I[1, m_k]$ and vice versa.

Suppose that the proportion of permitted k -tuples in the interval $I[1, p_k^2]$ was equal to the proportion of permitted k -tuples in the interval $I[1, m_k]$. In this case, we could immediately compute the exact number of permitted k -tuples in the interval $I[1, p_k^2]$ since we know this quantity for the interval $I[1, m_k]$ by (5). Certainly, our assumption on the proportion of permitted k -tuples in these intervals is unlikely to be true; however, we could say that in some sense, this assumption is ‘approximately’ true, which suggests the possibility of working with this value (the proportion of permitted k -tuples in a given interval) to obtain the expected results.

Now, assume that for every k the proportion of permitted k -tuples in $I[1, p_k^2]$ is greater than some constant $C > 0$; in this case, the number of permitted k -tuples within this interval would be greater than Cp_k^2 . This result implies that the number of permitted k -tuples within $I[1, p_k^2]$ tends to infinity with k . However, this constant is unlikely to exist since it follows from (5) that the proportion of permitted k -tuples in the interval $I[1, m_k]$ is given by

$$\frac{1}{2} \prod_{h=2}^k \left(1 - \frac{2}{p_h}\right),$$

which tends slowly to 0 as $k \rightarrow \infty$. This fact makes working with this value (the proportion of permitted k -tuples) not very useful.

Thus, it is more convenient to work with a new quantity that we call the density of permitted k -tuples, or simply the k -density, which is defined formally in Section 3. This value is defined for a given interval as the quotient of the number of permitted k -tuples within the interval and the number of subintervals of size p_k . That is, for a given interval, the density is the average number of permitted k -tuples within the subintervals of size p_k . We denote by c_k and δ_k the number of permitted k -tuples and the density of permitted k -tuples within the period $I[1, m_k]$ of the sequence of k -tuples, respectively (see Definition 2.9 and Definition 3.4). Since c_k does not depend on the choice of the selected remainders in the sequence of k -tuples, neither does δ_k . We shall prove later (Lemma 3.2 and Theorem 3.4) that δ_k increases and tends to infinity as $k \rightarrow \infty$. For some values of k , Table 1 gives c_k , the ratio c_k/m_k , and δ_k .

Suppose that the minimum value of the density of permitted k -tuples within the left interval $I[1, p_k^2]$ is greater than some constant $C > 0$. This assumption implies that the number of permitted k -tuples within this interval is greater

than Cp_k since the number of subintervals of size p_k in $I[1, p_k^2]$ is equal to p_k , which in turn implies that the number of permitted k -tuples in $I[1, p_k^2]$ (that is, the sifting function of Sieve II) tends to infinity as $k \rightarrow \infty$.

Table 1: Quotient c_k/m_k and density δ_k .

k	p_k	m_k	c_k	c_k/m_k	δ_k
4	7	210	15	0.071	0.500
5	11	2310	135	0.058	0.643
6	13	30030	1485	0.049	0.643
7	17	510510	22275	0.044	0.742
8	19	9699690	378675	0.039	0.742
9	23	223092870	7952175	0.036	0.820
10	29	-	-	0.033	0.962
11	31	-	-	0.031	0.962
12	37	-	-	0.029	1.087
13	41	-	-	0.028	1.145
14	43	-	-	0.027	1.145
15	47	-	-	0.025	1.199
16	53	-	-	0.024	1.301
17	59	-	-	0.024	1.399
18	61	-	-	0.023	1.399
19	67	-	-	0.022	1.490
20	71	-	-	0.022	1.535
21	73	-	-	0.021	1.535
22	79	-	-	0.020	1.619
23	83	-	-	0.020	1.660
24	89	-	-	0.019	1.740
.

1.8 Short explanation of the main ideas

Let us again consider the interval $I[1, m_k]$ of the sequence of k -tuples of Sieve II, in horizontal position, for k sufficiently large. As we have seen before, we can consider the first period of the sequence of k -tuples as a matrix of k rows and m_k columns. Recall that for every h ($1 \leq h \leq k$), the rows from 1 to h are part of a sequence of h -tuples. We shall say that h is the level of this sequence (see Definition 2.1). Note that since δ_h increases (see the preceding subsection), $\delta_k > \delta_4$ for sufficiently large k .

Suppose that for every level h ($1 \leq h \leq k$), the permitted h -tuples are placed in positions that follow an approximately regular pattern along the interval $I[1, m_k]$ of the corresponding sequence of h -tuples, regardless of the choice of the selected remainders in the sequence of k -tuples. In this case, for each level h , the density of permitted h -tuples in both intervals $I[1, p_k^2]$ and $I[p_k^2 + 1, m_k]$ of the sequence of h -tuples should be close to δ_h . Therefore, the density of permitted k -tuples in the interval $I[1, p_k^2]$ of the sequence of k -tuples (no matter the choice of the selected remainders) should be greater than δ_4 for sufficiently large k .

We shall prove that there exists an integer $K_\alpha > 4$ such that the density of permitted k -tuples in the interval $I[1, p_k^2]$ of the sequence of k -tuples (for all choices of the selected remainders) is greater than $\delta_4 = 1/2$ for every $k > K_\alpha$. Therefore, the quantity of permitted k -tuples in $I[1, p_k^2]$ (the value of the sifting function of Sieve II) must be greater than $p_k \delta_4 = p_k/2$, for $k > K_\alpha$. Furthermore, for every even number x that satisfy $p_k^2 < x < p_{k+1}^2$, the value of the sifting function of Sieve I is greater than or equal to the minimum value of the sifting function of Sieve II, as we have seen in Subsection 1.4. From this result, it follows that $p_k/2$ is also a lower bound for the sifting function of Sieve I for all even numbers x such that $p_k^2 < x < p_{k+1}^2$ ($k > K_\alpha$). This fact is clearly what is required to prove the main theorem.

Now, an obvious question arises at this point: How the parity barrier has been overcome? As we have seen in Subsection 1.5, given Sieve II we can compute $T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k)$ using the formula (5), which was derived from the inclusion–exclusion principle, because in the case of the set $\mathcal{B} = \{n : 1 \leq n \leq m_k\}$ the cardinality of the subsets \mathcal{B}_d can be computed precisely, since the square free integer d divides m_k . On the other hand, it is clear that, for our purposes, we need a lower bound for $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$.

Given k , let us consider Sieve II taking $\mathcal{B} = \{n : 1 \leq n \leq p_k^2\}$; thus, \mathcal{B} is the set of indices corresponding to the interval $I[1, p_k^2]$ of the sequence of k -tuples associated to Sieve II. (Assume given a choice of selected remainders in this sequence.) In this case, we can write

$$|\mathcal{B}_d| = \frac{2^{\nu(d)}}{d} p_k^2 + R_d \quad (d|m_k, 2 \nmid d)$$

and

$$|\mathcal{B}_d| = \frac{2^{\nu(d)-1}}{d} p_k^2 + R_d \quad (d|m_k, 2 | d)$$

where R_d is the remainder term (see Subsection 1.5). Now, by the inclusion–exclusion principle,

$$T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k) = \sum_{d|m_k} \mu(d) |\mathcal{B}_d| = \frac{1}{2} \sum_{\substack{d|m_k \\ 2 \nmid d}} \mu(d) \frac{2^{\nu(d)}}{d} p_k^2 + \sum_{d|m_k} \mu(d) R_d,$$

thus, by means of (4), the number of permitted k -tuples in the interval $I[1, p_k^2]$ of the sequence of k -tuples associated to Sieve II is given by

$$T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k) = \frac{1}{2} p_k^2 \prod_{\substack{2 < p \leq p_k \\ p \in \mathcal{P}}} \left(1 - \frac{2}{p}\right) + \sum_{d|m_k} \mu(d) R_d, \quad (6)$$

for an specific choice of selected remainders. Note that the product

$$\left(1 - \frac{1}{p_1}\right) \prod_{1 < h \leq k} \left(1 - \frac{2}{p_h}\right) \quad (7)$$

appears in both formulas (5) and (6). In the formula (5) the factors (arranged in the order of primes) represent the precise fraction of permitted h -tuples that remain unsifted (as permitted $(h+1)$ -tuples) in the interval $I[1, m_k]$ after every stage of the sifting process from $h=1$ to $h=k$ (see the last paragraph in Subsection 1.6). On the other hand, the fraction of permitted h -tuples that remain unsifted in the interval $I[1, p_k^2]$ after every stage of the sifting process depends on the choice of the selected remainders in the sequence of k -tuples. For this reason, in the formula (6) the ‘true’ factors (corresponding to a given choice of the selected remainders) are replaced by the ‘average’ factors that appear in (7), and then an error term is added to the formula.

The usual approach in sieve theory consist in estimating $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$ by using (6) as starting point. However, the parity problem prevents us from attempting to establish a lower bound for $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$, as we have seen in Subsection 1.1. Note that the remainder sum in (6) has too many terms if k is sufficiently large, since $z = p_k$. Now, the limitation imposed by the parity problem appears when we apply to the formula in (6) the usual methods developed so far in sieve theory. In this paper, we proceed in a way quite different from that is usual in sieve theory.

As we have remarked in the last paragraph of Subsection 1.6 (and it is an obvious fact), after every stage of the sifting process from $h=1$ to $h=k$, the number of permitted h -tuples in $I[1, p_k^2]_h$ decreases. This fact makes very difficult (maybe impossible) to directly estimate a lower bound for the number of permitted k -tuples in $I[1, p_k^2]$ after the whole sifting process has ended. For this reason, in place of estimating a lower bound for $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$ using (6) we first estimate a lower bound for the density of permitted k -tuples in $I[1, p_k^2]$ using (5), and then we compute the lower bound for $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$ using the lower bound for the k -density (see the 3rd paragraph in this subsection). We explain briefly this idea in the following paragraphs.

Given k sufficiently large, let us consider again the interval $I[1, m_k]_h$ for every sequence of h -tuples from $h=1$ to $h=k$. Suppose that we rewrite (5) in the form

$$T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k) = m_k \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{2}{p_2}\right) \left(1 - \frac{2}{p_3}\right) \dots \left(1 - \frac{2}{p_k}\right).$$

Then, if we shift denominators to the right we obtain

$$T(\{n : 1 \leq n \leq m_k\}, \mathcal{P}, p_k) = \frac{m_k}{p_k} \left(\frac{p_2 - 2}{p_1}\right) \left(\frac{p_3 - 2}{p_2}\right) \left(\frac{p_4 - 2}{p_3}\right) \dots \left(\frac{p_k - 2}{p_{k-1}}\right).$$

Clearly, the quotient m_k/p_k is the number of subintervals of size p_k within the period of the sequence of k -tuples, and the product

$$\left(\frac{p_2-2}{p_1}\right)\left(\frac{p_3-2}{p_2}\right)\left(\frac{p_4-2}{p_3}\right)\cdots\left(\frac{p_k-2}{p_{k-1}}\right)$$

is the density of permitted k -tuples within the period of the sequence, which is denoted by δ_k . Furthermore, every partial product in the preceding formula is δ_h ($1 < h \leq k$); note that δ_h increases, as we have seen in the preceding subsection.

Now, let us consider the interval $I[1, p_k^2]_h$ for every sequence of h -tuples from $h = 1$ to $h = k$. We shall prove that the average density of permitted h -tuples (for all the choices of selected remainders) within the interval $I[1, p_k^2]_h$ of a given sequence of h -tuples ($1 \leq h \leq k$) is equal to δ_h . Thus, the average density of permitted h -tuples within the interval $I[1, p_k^2]_h$ increases as we go from $h = 1$ to $h = k$, despite that the number of permitted h -tuples decreases. From this fact we can obtain a lower bound for the density of permitted k -tuples within the interval $I[1, p_k^2]_k$, so, we can compute a lower bound for $T(\{n : 1 \leq n \leq p_k^2\}, \mathcal{P}, p_k)$, for sufficiently large k . This is the way to circumvent the parity problem in this paper, rather different than the usual methods in sieve theory.

2 Periodic sequences of k -tuples

General Notation. We write (a, b) for the greatest common divisor of a and b , if no confusion will arise. In addition, lcm is used as an abbreviation for the least common multiple. Given a set A , we denote by $|A|$ the cardinality of A . For each $a \in \mathbb{R}$, the symbol $\lfloor a \rfloor$ denotes the floor function, and the symbol $\lceil a \rceil$ denotes the ceiling function.

In the Introduction, we began by describing one type of sieve to address the Goldbach problem, which we call the Sieve associated with x (or Sieve I); then, we introduced the notion of a sequence of k tuples of remainders as a new formulation for sieves in general, and for this sieve in particular. The Sieve associated with x (Sieve I) is directly related to the Goldbach problem; we leave the formal definition of this sieve to Section 8. On the other hand, we have also described in the Introduction a second more general sieve, which we call Sieve II. As we have seen in the Introduction, the sequence of k -tuples corresponding to Sieve II is more homogeneous than that corresponding to Sieve I, in the sense that in every sequence of remainders modulo p_h ($1 < h \leq k$), there are always two selected remainders. This fact is very important for computing the minimum value of the sifting function of Sieve II.

Sieve II is not directly related to the Goldbach problem, but as we have seen in the Introduction, the minimum number of permitted k -tuples in the interval $I[1, p_k^2]$ of the sequence of k -tuples corresponding to Sieve II (the minimum value of the sifting function of Sieve II) is a lower bound for the number of permitted k -tuples in the interval $I[1, x]$ of the sequence corresponding to Sieve I (the sifting function of Sieve I), where $p_k^2 < x < p_{k+1}^2$. We shall prove this fact in Section 8. In this section, we formally define Sieve II; from here until the end of Section 7 we shall address the properties of this sieve.

We begin by defining the sequence of remainders, the sequence of k -tuples of remainders, and other associated concepts.

Definition 2.1. Let \mathcal{P} be the sequence of all primes, and consider the subset $\{p_1, p_2, p_3, \dots, p_k\}$ of the first k primes.

- (1) Given p_h ($1 \leq h \leq k$), we define the periodic sequence $\{r_n\}$, where r_n ($n \in \mathbb{Z}_+$) denotes the remainder of dividing n by the modulus p_h . We denote the sequence $\{r_n\}$ by the symbol s_h . The period of the sequence is equal to p_h .
- (2) We define the sequence $\{(r_1, r_2, r_3, \dots, r_k)_n\}$, the elements of which are k -tuples of the remainders obtained by dividing n by the moduli $p_1, p_2, p_3, \dots, p_k$. We arrange the sequence of k -tuples of remainders vertically; we usually omit the comma separators in the k -tuples. Then, the sequence of k -tuples can be seen as a matrix formed by k columns and infinitely many rows, where each column of the matrix is a periodic sequence s_h ($1 \leq h \leq k$). We call the index k the *level* of the sequence of k -tuples of remainders. See Example 2.1.

Example 2.1. Table 2 shows the first elements of the sequence of 5-tuples of the remainders of dividing n by $\{2, 3, 5, 7, 11\}$.

Definition 2.2. Given a sequence $\{r_n\}$ with prime modulus p_k , we assign to the remainders r_n one of the two following states: *selected state* or *not selected state*.

Definition 2.3. Given a sequence of k -tuples of remainders, we define a k -tuple to be *prohibited* if it has one or more selected remainders, and we define it to be *permitted* if it contains no selected remainders.

Definition 2.4. We denote by m_k the product $p_1 p_2 p_3 \cdots p_k$.

Table 2: Sequence of 5-tuples of remainders.

n	2	3	5	7	11
1	1	1	1	1	1
2	0	2	2	2	2
3	1	0	3	3	3
4	0	1	4	4	4
5	1	2	0	5	5
6	0	0	1	6	6
7	1	1	2	0	7
8	0	2	3	1	8
9	1	0	4	2	9
10	0	1	0	3	10
11	1	2	1	4	0
12	0	0	2	5	1
13	1	1	3	6	2
14	0	2	4	0	3
15	1	0	0	1	4
16	0	1	1	2	5
17	1	2	2	3	6
18	0	0	3	4	7
.

Proposition 2.1. *The sequence of k -tuples of remainders is periodic, and its fundamental period is equal to $m_k = p_1 p_2 p_3 \cdots p_k$.*

Proof. Let s_h ($1 \leq h \leq k$) be the sequences of remainders that form a given sequence of k -tuples. Let m' be a multiple of all the primes $p_1, p_2, p_3, \dots, p_k$. The period of every sequence s_h is equal to $p_h \in \{p_1, p_2, p_3, \dots, p_k\}$. Therefore, for every sequence s_h , the remainders are repeated for all the integer intervals of size m' , starting from the index $n = 1$ onward. Since $p_1, p_2, p_3, \dots, p_k$ are primes, the product m_k is the lcm. Consequently, the fundamental period of the sequence of k -tuples is equal to m_k . ■

Thus far, we have defined the sequence of k -tuples of remainders without defining any rules for selecting remainders, so, the sequence of k -tuples does not work as a sieve. Before defining these rules, we shall consider another important question concerning the sequence of k -tuples of remainders. As shown in the Introduction, in the case of Sieve II, the behaviour of the sequence of k -tuples as k increases indefinitely must be addressed. Consequently, we require two more definitions before defining the rules for selecting remainders.

Definition 2.5. Sum of sequences.

Let $\{p_1, p_2, p_3, \dots, p_k\}$ be the set of the first k primes. Let $\{(r_1 r_2 r_3 \dots r_k)_n\}$ be the sequence of k -tuples of the remainders of dividing n by the k prime moduli $\{p_1, p_2, p_3, \dots, p_k\}$, and let $\{(r_{k+1})_n\}$ be the sequence of the remainders of dividing n by the prime modulus p_{k+1} . We define the *sum* $\{(r_1 r_2 r_3 \dots r_k)_n\} + \{(r_{k+1})_n\}$ of the sequence $\{(r_1 r_2 r_3 \dots r_k)_n\}$ and the sequence $\{(r_{k+1})_n\}$ to be the sequence of $(k + 1)$ -tuples given by the equation

$$\{(r_1 r_2 r_3 \dots r_k)_n\} + \{(r_{k+1})_n\} = \{(r_1 r_2 r_3 \dots r_k r_{k+1})_n\},$$

and formed by the ordered juxtaposition of each k -tuple of the first sequence with each element (index n modulo p_{k+1}) of the second sequence.

Definition 2.6. Let \mathcal{P} be the sequence of all primes, and let $p_k \in \mathcal{P}$. Let s_k be the sequence of the remainders r_n of dividing n by the modulus p_k (see Definition 2.1). Let $\{s_k\}$ be the sequence of sequences s_k . We define the series denoted by $\sum s_k$ to be the sequence $\{S_k\}$, where S_k denotes the partial sum:

$$\begin{aligned}
S_1 &= s_1, \\
S_2 &= s_1 + s_2, \\
S_3 &= s_1 + s_2 + s_3, \\
&\vdots \\
S_k &= s_1 + s_2 + s_3 + s_4 + \cdots + s_k,
\end{aligned}$$

and the symbol \sum refers to the formal addition of sequences. In each partial sum S_k , the greatest prime modulus p_k is called the characteristic prime modulus of the partial sum S_k , and we say that S_k is the partial sum of level k .

Note . On the one hand, we can view a given partial sum S_k as a sequence, indexed by n , of the k -tuples of remainders obtained by dividing n by the moduli $p_1, p_2, p_3, \dots, p_k$. On the other hand, the partial sum S_k can be seen as a finite sequence, indexed by the set $\{1, \dots, k\}$ ($k \in \mathbb{Z}_+$), of sequences of remainders modulo $p_h \in \{p_1, p_2, p_3, \dots, p_k\}$, where the indices $\{1, \dots, k\}$ increase from left to right. Additionally, by definition, the series $\sum s_k$ is the sequence, indexed by k , of the partial sums S_k .

Example 2.2. Table 3 shows the partial sum S_4 and the formal addition of the sequence of remainders s_5 to obtain the partial sum S_5 .

Table 3: Partial sums S_4 and S_5 .

n	S_4				s_5	$+$	s_5	$=$	S_5					
	2	3	5	7	11				2	3	5	7	11	
1	1	1	1	1	1				1	1	1	1	1	1
2	0	2	2	2	2				0	2	2	2	2	2
3	1	0	3	3	3				1	0	3	3	3	3
4	0	1	4	4	4				0	1	4	4	4	4
5	1	2	0	5	5				1	2	0	5	5	5
6	0	0	1	6	6				0	0	1	6	6	6
7	1	1	2	0	7				1	1	2	0	7	7
8	0	2	3	1	8				0	2	3	1	8	8
9	1	0	4	2	9	$+$	9	$=$	1	0	4	2	9	9
10	0	1	0	3	10				0	1	0	3	10	10
11	1	2	1	4	0				1	2	1	4	0	0
12	0	0	2	5	1				0	0	2	5	1	1
13	1	1	3	6	2				1	1	3	6	2	2
14	0	2	4	0	3				0	2	4	0	3	3
15	1	0	0	1	4				1	0	0	1	4	4
16	0	1	1	2	5				0	1	1	2	5	5
17	1	2	2	3	6				1	2	2	3	6	6
18	0	0	3	4	7				0	0	3	4	7	7
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot				\cdot	\cdot	\cdot	\cdot	\cdot	\cdot

Now, we are ready to define the rules for selecting remainders in the sequences s_h ($1 \leq h \leq k$) that constitute every partial sum S_k of the series $\sum s_k$.

Definition 2.7. Let s_h ($1 \leq h \leq k$) be one of the sequences of remainders that form the partial sum S_k .

Rule 1. If $h = 1$, in the sequence of remainders s_1 , there will be selected one remainder, which is the same in every period of the sequence.

Rule 2. If $1 < h \leq k$, in every sequence of remainders s_h , there will be selected two remainders, which are the same two in every period of the sequence.

Example 2.3. Table 4 shows the partial sum of level $k = 4$, where the selected remainders are in square brackets []. Note that the 4-tuples 1 and 7 are permitted k -tuples.

A given partial sum S_k is a sequence of k -tuples of remainders. However, henceforth, when we refer to a given partial sum S_k , we mean S_k together with the selected remainders, unless we specifically state otherwise. Now, we are ready to formally define Sieve II.

Table 4: Partial sum S_4 with selected remainders.

n	2	3	5	7
1	1	1	1	1
2	[0]	[2]	2	2
3	1	[0]	[3]	[3]
4	[0]	1	4	4
5	1	[2]	[0]	[5]
6	[0]	[0]	1	6
7	1	1	2	0
8	[0]	[2]	[3]	1
9	1	[0]	4	2
10	[0]	1	[0]	[3]
11	1	[2]	1	4
12	[0]	[0]	2	[5]
13	1	1	[3]	6
14	[0]	[2]	4	0
15	1	[0]	[0]	1
16	[0]	1	1	2
·	·	·	·	·

Definition 2.8. Let \mathcal{P} be the sequence of all primes, and let p_k ($k \geq 4$) be a prime of the sequence. Let \mathcal{B} be the set consisting of the indices n of the partial sum S_k that lie in the interval $[1, y]$ (see note following Definition 2.6), where y is an integer that satisfies $y > p_k$. For each $p = p_h \in \mathcal{P}$ ($1 \leq h \leq k$), the subset \mathcal{B}_p of \mathcal{B} consists of the indices n whose remainder modulo $p = p_h$ is one of the selected remainders r or r' . The indices of the prohibited k -tuples lying in \mathcal{B} are sifted out, and the indices of the permitted k -tuples lying in \mathcal{B} remain unsifted. See Remark 1.2. The *sifting* function

$$T(\mathcal{B}, \mathcal{P}, p_k) = \left| \mathcal{B} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p \leq p_k}} \mathcal{B}_p \right|,$$

is given by the number of permitted k -tuples whose indices lie in the interval \mathcal{B} .

Hereafter, we take $\mathcal{B} = \{n : 1 \leq n \leq p_k^2\}$, that is $y = p_k^2$.

In the following theorems, we prove some additional properties of the partial sums of the series $\sum s_k$, which will be used throughout this paper.

Proposition 2.2. *Let S_k be a given partial sum. Let s_{k+1} be the sequence of remainders modulo p_{k+1} . Let r ($0 \leq r < p_{k+1}$) be one of the remainders modulo p_{k+1} of the sequence s_{k+1} . Let $n \in \mathbb{Z}_+$ be the index of a given k -tuple of S_k . Then, when we juxtapose the elements of the sequence s_{k+1} to each k -tuple of S_k , we obtain the following.*

- (1) *If the k -tuple at position n is prohibited, then the $(k+1)$ -tuple of S_{k+1} at position n will be prohibited as well.*
- (2) *If the k -tuple at position n is permitted and $n \equiv r \pmod{p_{k+1}}$, then:*
 - (a) *The $(k+1)$ -tuple of S_{k+1} at position n is prohibited if and only if r is a selected remainder;*
 - (b) *The $(k+1)$ -tuple of S_{k+1} at position n is permitted if and only if r is not a selected remainder.*

Proof. By definition, a given k -tuple is prohibited if it has one or more selected remainders; if it has no selected remainders, the k -tuple is permitted. The proof is immediate. ■

Definition 2.9. For a given partial sum S_k , we denote by c_k the number of permitted k -tuples within a period of S_k .

Proposition 2.3. *Let S_k be a given partial sum. We then have $c_k = (p_1 - 1)(p_2 - 2)(p_3 - 2) \cdots (p_k - 2)$.*

Proof. It follows from (5), by simplifying the expression. ■

Now, to obtain a period of the partial sum S_{k+1} , we first take p_{k+1} periods of the partial sum S_k ; next, we juxtapose the remainders of the sequence s_{k+1} to each k -tuple of S_k (that is, we perform the operation $S_k + s_{k+1}$). The following proposition shows that the distribution of the indices of permitted k -tuples within the p_{k+1} periods of the partial sum S_k over the residue classes modulo p_{k+1} is uniform.

Proposition 2.4. *The indices of permitted k -tuples within the first p_{k+1} periods of the partial sum S_k are uniformly distributed over the residue classes modulo p_{k+1} .*

Proof. Let c_k be the number of permitted k -tuples within a period of S_k . Let $[y] = [0], [1], [2], \dots, [p_{k+1} - 1]$ be the residue classes modulo p_{k+1} . Let $n \in \mathbb{Z}_+$ be the index of a given permitted k -tuple within the first period of the partial sum S_k . Thus, within p_{k+1} periods of the partial sum S_k , there are p_{k+1} permitted k -tuples with indices $n' = m_k x + n$, where $x = 0, 1, 2, 3, \dots, p_{k+1} - 1$ represents each period. Because $(m_k, p_{k+1}) = 1$, for each residue class $[y]$, the congruence $m_k x + n \equiv y \pmod{p_{k+1}}$ has a unique solution x . Therefore, since there are c_k permitted k -tuples within the period of S_k , it follows that there are c_k indices of permitted k -tuples within each residue class modulo p_{k+1} , and the resulting distribution is uniform. ■

Corollary 2.5. *If there are m' consecutive periods of the partial sum S_k (including the first), where m' is a multiple of p_{k+1} , the indices of permitted k -tuples within these m' periods are also uniformly distributed over the residue classes modulo p_{k+1} .*

3 Definition and properties of the density of permitted k -tuples

In this section, we formally define the concept of the density of permitted k -tuples, and we prove that the density of permitted k -tuples within a period of the partial sum S_k is increasing and tends to ∞ as $k \rightarrow \infty$.

Definition 3.1. If we write the index n of the sequences s_h from top to bottom and the level h from left to right (see Table 2), we say that the partial sum S_k is in the *vertical position*. Now, suppose that the partial sum S_k is in the vertical position, and we rotate it 90 degrees counterclockwise. Then, the index n of the sequences s_h increases from left to right, and the level h increases from the bottom up. In this case, we say that the partial sum S_k is in the *horizontal position*.

Hereafter, we consider that every partial sum S_k is in horizontal position, unless we specifically state otherwise.

Definition 3.2. Let S_k be a given partial sum of the series $\sum s_k$, and let $I[m, n]$ be a given interval of k -tuples. We denote by $c_k^{I[m, n]}$ the number of permitted k -tuples within $I[m, n]$.

Definition 3.3. Let S_k be a partial sum of the series $\sum s_k$, and let $I[m, n]$ be a given interval of k -tuples. The number of subintervals of size p_k in this interval is $|I[m, n]|/p_k$. We define the *density of permitted k -tuples* in the interval $I[m, n]$ (or simply the *k -density*) by

$$\delta_k^{I[m, n]} = \frac{c_k^{I[m, n]}}{|I[m, n]|/p_k}.$$

For the empty interval, we define $\delta_k^{I[\]} = 0$.

Definition 3.4. Let S_k be a given partial sum of the series $\sum s_k$, and let m_k be the period of S_k . Recall that we have used the notation $c_k = c_k^{I[1, m_k]}$ for the number of permitted k -tuples within the interval $I[1, m_k]$ (the first period of S_k). We normally use the notation $\delta_k = \delta_k^{I[1, m_k]}$ for the density of permitted k -tuples within the interval $I[1, m_k]$. Since m_k/p_k is the number of subintervals of size p_k within a period of S_k , by definition, we have

$$\delta_k = \frac{c_k}{m_k/p_k}.$$

By Proposition 2.3, the number of permitted k -tuples within the interval $I[1, m_k]$ (the first period of S_k) does not depend on the selected remainders in the sequences of remainders that form S_k . Therefore, we consider $I[1, m_k]$ to be a special interval, which explains why we use the special notation c_k for the number of permitted k -tuples within $I[1, m_k]$ and use δ_k for the density of permitted k -tuples within $I[1, m_k]$.

The following lemma gives a formula for computing δ_k .

Lemma 3.1. *We have*

$$\delta_k = \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 2}{p_2} \right) \left(\frac{p_3 - 2}{p_3} \right) \cdots \left(\frac{p_{k-1} - 2}{p_{k-1}} \right) (p_k - 2).$$

Proof. By definition and Proposition 2.3

$$\begin{aligned} \delta_k &= \frac{c_k}{m_k/p_k} = \frac{(p_1 - 1)(p_2 - 2)(p_3 - 2) \cdots (p_{k-1} - 2)(p_k - 2)}{p_1 p_2 p_3 p_4 \cdots p_{k-1}} = \\ &= \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 2}{p_2} \right) \left(\frac{p_3 - 2}{p_3} \right) \cdots \left(\frac{p_{k-1} - 2}{p_{k-1}} \right) (p_k - 2). \end{aligned}$$

■

The next lemma shows that δ_k is increasing if $k > 1$.

Lemma 3.2. *Let S_k and S_{k+1} be consecutive partial sums of the series $\sum s_k$. If δ_k denotes the density of permitted k -tuples within a period of S_k and δ_{k+1} denotes the density of permitted $(k+1)$ -tuples within a period of S_{k+1} , then*

$$\delta_{k+1} = \delta_k \left(\frac{p_{k+1} - 2}{p_k} \right).$$

Proof. Taking the quotient δ_{k+1}/δ_k and simplifying, the proof follows immediately.

■

Corollary 3.3. *By Lemma 3.2,*

1. $p_{k+1} - p_k < 2 \implies \delta_{k+1} < \delta_k$.
2. $p_{k+1} - p_k = 2 \implies \delta_{k+1} = \delta_k$.
3. $p_{k+1} - p_k > 2 \implies \delta_{k+1} > \delta_k$.

Now, we prove that $\delta_k \rightarrow \infty$ as $k \rightarrow \infty$. First, we present a definition.

Definition 3.5. Let $p_k > 2$ and p_{k+1} be consecutive primes. We denote by θ_k the difference $p_{k+1} - p_k - 2$.

Theorem 3.4. *Let S_k be a given partial sum. Let δ_k be the density of permitted k -tuples within a period of S_k . As $k \rightarrow \infty$, we have $\delta_k \rightarrow \infty$.*

Proof. By Lemma 3.1,

$$\delta_k = \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 2}{p_2} \right) \left(\frac{p_3 - 2}{p_3} \right) \left(\frac{p_4 - 2}{p_4} \right) \left(\frac{p_5 - 2}{p_5} \right) \cdots \left(\frac{p_{k-1} - 2}{p_{k-1}} \right) (p_k - 2).$$

If we shift denominators to the right, we obtain

$$\delta_k = (p_1 - 1) \left(\frac{p_2 - 2}{p_1} \right) \left(\frac{p_3 - 2}{p_2} \right) \left(\frac{p_4 - 2}{p_3} \right) \left(\frac{p_5 - 2}{p_4} \right) \cdots \left(\frac{p_{k-1} - 2}{p_{k-2}} \right) \left(\frac{p_k - 2}{p_{k-1}} \right).$$

By definition, $\theta_k = p_{k+1} - p_k - 2 \implies p_{k+1} - 2 = p_k + \theta_k$. Consequently, we can write the expression of δ_k as

$$\begin{aligned} \delta_k &= \frac{1}{2} \left(\frac{p_2 + \theta_2}{p_2} \right) \left(\frac{p_3 + \theta_3}{p_3} \right) \left(\frac{p_4 + \theta_4}{p_4} \right) \cdots \left(\frac{p_{k-2} + \theta_{k-2}}{p_{k-2}} \right) \left(\frac{p_{k-1} + \theta_{k-1}}{p_{k-1}} \right) = \\ &= \frac{1}{2} \left(1 + \frac{\theta_2}{p_2} \right) \left(1 + \frac{\theta_3}{p_3} \right) \left(1 + \frac{\theta_4}{p_4} \right) \cdots \left(1 + \frac{\theta_{k-2}}{p_{k-2}} \right) \left(1 + \frac{\theta_{k-1}}{p_{k-1}} \right) = \\ &= \frac{1}{3} \left[\left(1 + \frac{1}{p_1} \right) \left(1 + \frac{\theta_2}{p_2} \right) \left(1 + \frac{\theta_3}{p_3} \right) \left(1 + \frac{\theta_4}{p_4} \right) \cdots \left(1 + \frac{\theta_{k-1}}{p_{k-1}} \right) \left(1 + \frac{\theta_k}{p_k} \right) \right] \frac{p_k}{p_k + \theta_k}. \end{aligned}$$

Then,

$$\lim_{k \rightarrow \infty} \delta_k = \frac{1}{3} \left[\left(1 + \frac{1}{p_1} \right) \prod_{k=2}^{\infty} \left(1 + \frac{\theta_k}{p_k} \right) \right] \lim_{k \rightarrow \infty} \frac{p_k}{p_k + \theta_k}. \quad (8)$$

The infinite product between square brackets diverges if the series

$$\frac{1}{p_1} + \sum_{k=2}^{\infty} \frac{\theta_k}{p_k} \quad (9)$$

diverges. In the series (9), if p_k is the first of a pair of twin primes, by definition, we have $\theta_k = 0$; otherwise, we have $\theta_k \geq 2$. Let $\sum_{j=1}^{\infty} 1/q_j$ denote the series where every prime q_j is the first of a pair of twin primes. Since the series of reciprocals of the twin primes converges [3], the series $\sum_{j=1}^{\infty} 1/q_j$ also converges. Therefore, the series $\sum_{k=1}^{\infty} 1/p_k - \sum_{j=1}^{\infty} 1/q_j$ diverges because $\sum_{k=1}^{\infty} 1/p_k$ diverges. By comparison with the series $\sum_{k=1}^{\infty} 1/p_k - \sum_{j=1}^{\infty} 1/q_j$, it follows that the series (9) diverges because $\theta_k/p_k > 1/p_k$ for the terms where $\theta_k > 0$. Thus, the infinite product in (8) tends to ∞ as well. On the other hand, by the Bertrand–Chebyshev theorem, $p_k < p_{k+1} < 2p_k \implies \theta_k < p_k \implies p_k/(p_k + \theta_k) > 1/2$. Consequently, $\delta_k \rightarrow \infty$ as $k \rightarrow \infty$. ■

4 The average density of permitted k -tuples within a given interval

$I[m, n]$

Let S_k be a given partial sum of the series $\sum s_k$. In Section 3 we showed that for the interval $I[1, m_k]$ of the partial sum S_k , the density of permitted k -tuples does not depend on the choice of the selected remainders in the sequences s_h ($1 \leq h \leq k$) that form the partial sum S_k (see Lemma 3.1). However, this assertion does not hold for all the intervals $I[m, n]$ of the partial sum S_k . In this section, we prove that within a given interval $I[m, n]$ of the partial sum S_k , the average of the values of the k -density for all the possible choices of the selected remainders is equal to δ_k . First, we present some definitions.

Definition 4.1. Let s_h ($1 \leq h \leq k$) be the sequences of remainders that form the partial sum S_k . A given choice of selected remainders within the period of one of the sequences s_h or within the periods of all the sequences s_h ($1 \leq h \leq k$) is called a *combination* of selected remainders. We denote by ν_h the number of combinations of selected remainders within the period of a given sequence s_h . Since, by definition, for the sequences s_h ($1 < h \leq k$) there are two selected remainders within the period p_h ,

$$\nu_h = \binom{p_h}{2}. \quad (10)$$

In the sequence s_1 , there is only one selected remainder within the period; then, $p_1 = 2 \implies \nu_1 = 2$.

Convention. Henceforth, when we refer to the average density of permitted k -tuples within a given interval $I[m, n]$ of the partial sum S_k , we mean that the average is computed taking into account all the combinations of selected remainders in the sequences s_h that form the partial sum S_k . We use the same convention when we refer to the average number of permitted k -tuples.

Definition 4.2. The operation of Type A.

Let s_h ($1 \leq h \leq k$) be the sequences of remainders that form the partial sum S_k . For $h > 1$, let r, r' (mod p_h) be the selected remainders within the period p_h of the sequence s_h . We define the operation that changes the selected remainders r, r' (mod p_h) to $r + 1, r' + 1$ (mod p_h) to be the *Type A* operation.

For the sequence s_1 , we also define the operation of changing the selected remainder r (mod p_1) to $r + 1$ (mod p_1) to be the Type A operation.

Example 4.1. Table 5 shows the first period of the sequence of remainders s_4 ($p_4 = 7$), where initially we select the remainders [1] and [3] and then successively apply the Type A operation.

Definition 4.3. The operation of Type B.

Let s_h ($1 < h \leq k$) be the sequences of remainders that form the partial sum S_k . Let r, r' (mod p_h) be the selected remainders (in that order), within the period p_h of the sequence s_h . We define the *Type B* operation as follows:

- 1) The remainder r remains selected.
- 2) We change the other selected remainder r' (mod p_h) to $r' + 1$ (mod p_h), $r \neq r' + 1$.

Table 5: First period of the sequence of remainders s_4 .

n							
1	[1]	1	1	1	1	[1]	1
2	2	[2]	2	2	2	2	[2]
3	[3]	3	[3]	3	3	3	3
4	4	[4]	4	[4]	4	4	4
5	5	5	[5]	5	[5]	5	5
6	6	6	6	[6]	6	[6]	6
7	0	0	0	0	[0]	0	[0]

Table 6: First period of the sequence of remainders s_4 .

n						
1	[1]	[1]	[1]	[1]	[1]	[1]
2	[2]	2	2	2	2	2
3	3	[3]	3	3	3	3
4	4	4	[4]	4	4	4
5	5	5	5	[5]	5	5
6	6	6	6	6	[6]	6
7	0	0	0	0	0	[0]

Example 4.2. Table 6 shows the first period of the sequence of remainders s_4 ($p_4 = 7$), where initially we selected the remainders [1] and [2] and then successively applied the Type B operation.

Definition 4.4. Let s_h ($1 \leq h \leq k$) be a given sequence of remainders modulo p_h . We define ν_h^A by $\nu_h^A = p_h$, and we define ν_h^B ($h > 1$) by $\nu_h^B = (p_h - 1)/2$.

Remark 4.1. Suppose that we choose two consecutive selected remainders r, r' within the period of the sequence s_h ($1 < h \leq k$). Thus, we have one of ν_h combinations of selected remainders. Repeating the Type A operation $\nu_h^A - 1$ times, we obtain $\nu_h^A = p_h$ different combinations of selected remainders. Now, if for each one of these combinations we leave unchanged the selected remainder r and then we repeat the Type B operation $\nu_h^B - 1$ times, we obtain all the ν_h combinations of selected remainders within the period of the sequence s_h . This process is expressed by the equation

$$\nu_h = \binom{p_h}{2} = \frac{p_h!}{2!(p_h - 2)!} = p_h \frac{p_h - 1}{2} = \nu_h^A \nu_h^B.$$

Definition 4.5. Let S_k and S_{k+1} be the partial sums of levels k and $k + 1$. Let s_{k+1} be the sequence of remainders of level $k + 1$. Let $I[m, n]_k$ be an interval of k -tuples of S_k , and let $I[m, n]_{k+1}$ be an interval of $(k + 1)$ -tuples of S_{k+1} , where the indices m, n are the same for both intervals. When we juxtapose the remainders of sequence s_{k+1} to each k -tuple of S_k , then, by Proposition 2.2, the permitted k -tuples of S_k , whose indices are congruent to a given selected remainder of s_{k+1} modulo p_{k+1} , are converted to prohibited $(k + 1)$ -tuples of S_{k+1} . We denote by f_{k+1} the fraction of the permitted k -tuples within the interval $I[m, n]_k$ that are converted to prohibited $(k + 1)$ -tuples within the interval $I[m, n]_{k+1}$. For the partial sum S_1 , let f_1 denote the fraction of the prohibited 1-tuples within the interval $I[m, n]_{k=1}$.

We denote by $\overline{f_{k+1}}$ the average of f_{k+1} for all the combinations of selected remainders in the sequence s_{k+1} ($k \geq 1$). For the partial sum S_1 , let $\overline{f_1}$ denote the average of f_1 for the 2 combinations of selected remainders in the sequence s_1 .

The following lemma gives a formula for computing the average fraction $\overline{f_{k+1}}$.

Lemma 4.1. For $k \geq 1$, we have $\overline{f_{k+1}} = 2/p_{k+1}$. For S_1 , we have $\overline{f_1} = 1/p_1$.

Proof. Let $[0], [1], [2], \dots, [p_{k+1} - 1]$ be the residue classes modulo p_{k+1} . Let $c_k^{I[m, n]}$ be the number of permitted k -tuples within $I[m, n]_k$. We denote by $\eta_0, \eta_1, \eta_2, \dots, \eta_{p_{k+1} - 1}$ the number of permitted k -tuples within $I[m, n]_k$ whose indices belong to the residue classes $[0], [1], [2], \dots, [p_{k+1} - 1]$, respectively. Therefore, $c_k^{I[m, n]} = \eta_0 + \eta_1 + \eta_2 + \dots + \eta_{p_{k+1} - 1}$.

We wish to compute the average fraction of the permitted k -tuples within the interval $I[m, n]_k$ that are converted to prohibited $(k + 1)$ -tuples within the interval $I[m, n]_{k+1}$ for all ν_{k+1} combinations of selected remainders in the sequence s_{k+1} ($k \geq 1$). Now,

$$\nu_{k+1} = \nu_{k+1}^A \nu_{k+1}^B = p_{k+1} \frac{(p_{k+1} - 1)}{2},$$

by Remark 4.1. Consequently, we begin by taking the average over the ν_{k+1}^A combinations obtained by the Type A operations, and then we take the average of the previous averages over the ν_{k+1}^B combinations obtained by the Type B operations.

Step 1. Suppose that we choose two selected remainders r, r' within the period of the sequence s_{k+1} . By Proposition 2.2, the indices of the permitted k -tuples within the interval $I[m, n]_k$ of S_k that are converted to prohibited $(k+1)$ -tuples within the interval $I[m, n]_{k+1}$ of S_{k+1} belong to one of the residue classes $[r]$ or $[r']$. It follows that the fraction of the $c_k^{I[m, n]}$ permitted k -tuples within the interval $I[m, n]_k$ of S_k that are converted to prohibited $(k+1)$ -tuples within the interval $I[m, n]_{k+1}$ of S_{k+1} is equal to $(\eta_r + \eta_{r'})/c_k^{I[m, n]}$. Taking the average over the ν_{k+1}^A combinations of selected remainders obtained by repeated Type A operations, we obtain

$$\frac{\sum_{i=1}^{\nu_{k+1}^A} \frac{\eta_r + \eta_{r'}}{c_k^{I[m, n]}}}{\nu_{k+1}^A} = \frac{\sum_{i=1}^{p_{k+1}} \frac{\eta_r + \eta_{r'}}{c_k^{I[m, n]}}}{p_{k+1}} = \frac{\left(1/c_k^{I[m, n]}\right) \left(\sum_{r=0}^{p_{k+1}-1} \eta_r + \sum_{r'=0}^{p_{k+1}-1} \eta_{r'}\right)}{p_{k+1}} = \frac{\left(1/c_k^{I[m, n]}\right) \left(c_k^{I[m, n]} + c_k^{I[m, n]}\right)}{p_{k+1}} = \frac{2}{p_{k+1}}.$$

Step 2. Now, if we take the average over the $\nu_{k+1}^B = (p_{k+1} - 1)/2$ combinations of selected remainders obtained by repeated Type B operations from each one of the combinations obtained before, we obtain

$$\overline{f_{k+1}} = \frac{\sum_{j=1}^{\nu_{k+1}^B} \frac{2}{p_{k+1}}}{\nu_{k+1}^B} = \frac{2}{p_{k+1}},$$

because p_{k+1} does not depend on the index j ($1 \leq j \leq \nu_{k+1}^B$).

For the partial sum S_1 , there are two residue classes modulo $p_1 = 2$ and one selected remainder. Therefore, $\overline{f_1} = 1/p_1$. ■

Definition 4.6. It follows from Proposition 2.2 that when we juxtapose the remainders of the sequence s_{k+1} to each k -tuple of S_k , the permitted k -tuples of S_k whose indices are not congruent to any of the two selected remainders of s_{k+1} modulo p_{k+1} are, as $(k+1)$ -tuples of S_{k+1} , still permitted. We denote by f'_{k+1} the fraction of permitted k -tuples within the interval $I[m, n]_k$ of S_k that are transferred to the interval $I[m, n]_{k+1}$ of S_{k+1} as permitted $(k+1)$ -tuples. For the partial sum S_1 , let f'_1 denote the fraction of the permitted 1-tuples within the interval $I[m, n]_{k=1}$.

We denote by $\overline{f'_{k+1}}$ the average of f'_{k+1} for all combinations of selected remainders in sequence s_{k+1} . For the partial sum S_1 , let $\overline{f'_1}$ denote the average of f'_1 for the 2 combinations of selected remainders in sequence s_1 .

Now, using the preceding lemma, we can calculate the average fraction $\overline{f'_{k+1}}$.

Lemma 4.2. We have $\overline{f'_{k+1}} = (p_{k+1} - 2)/p_{k+1}$. For S_1 , we have $\overline{f'_1} = (p_1 - 1)/p_1$.

Proof. By Proposition 2.2, a given permitted k -tuple within the interval $I[m, n]_k$ of S_k can be transferred to the interval $I[m, n]_{k+1}$ of S_{k+1} either as a permitted $(k+1)$ -tuple or as a prohibited $(k+1)$ -tuple. Consequently, $f_{k+1} + f'_{k+1} = 1$, so $\overline{f_{k+1}} + \overline{f'_{k+1}} = 1$. Therefore, using Lemma 4.1, we obtain $\overline{f'_{k+1}} = 1 - \overline{f_{k+1}} = 1 - 2/p_{k+1} = (p_{k+1} - 2)/p_{k+1}$.

For the partial sum S_1 , we have $\overline{f_1} = 1/p_1 \implies \overline{f'_1} = (p_1 - 1)/p_1$. ■

Definition 4.7. Let S_k be the partial sum of level k . Let $I[m, n]$ be an interval of k -tuples of S_k . We denote by $\overline{c_k^{I[m, n]}}$ the average number of permitted k -tuples within the interval $I[m, n]$. We denote by $\overline{\delta_k^{I[m, n]}}$ the average density of permitted k -tuples within the interval $I[m, n]$.

Finally, using the preceding lemmas, we calculate the average k -density within a given interval $I[m, n]$ and show that it is equal to the k -density within the period of S_k .

Theorem 4.3. Let δ_k be the density of permitted k -tuples within a period of the partial sum S_k . Then, $\overline{\delta_k^{I[m, n]}} = \delta_k$.

Proof. Let s_h ($1 \leq h \leq k$) be the sequences of remainders that form S_k . If there are no selected remainders within the sequences s_h , all the k -tuples within the interval $I[m, n]$ are permitted k -tuples, and $\overline{c_k^{I[m, n]}} = |I[m, n]|$, where $|I[m, n]|$ is the size of the interval $I[m, n]$. However, since we have selected remainders in every sequence s_h ($1 \leq h \leq k$), using Lemma 4.2 at each level transition from $h = 1$ to $h = k$, we can write

$$\overline{c_k^{I[m, n]}} = |I[m, n]| \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 2}{p_2} \right) \left(\frac{p_3 - 2}{p_3} \right) \cdots \left(\frac{p_k - 2}{p_k} \right). \quad (11)$$

Now, the number of intervals of size p_k within the interval $I[m, n]$ is equal to $|I[m, n]|/p_k$. Consequently, by definition,

$$\delta_k^{I[m, n]} = \frac{\overline{c_k^{I[m, n]}}}{\frac{|I[m, n]|}{p_k}} = \frac{p_k}{|I[m, n]|} \overline{c_k^{I[m, n]}}. \quad (12)$$

Therefore, substituting (11) for $\overline{c_k^{I[m, n]}}$ in (12) and using Lemma 3.1, we obtain

$$\begin{aligned} \delta_k^{I[m, n]} &= \frac{p_k}{|I[m, n]|} \left(|I[m, n]| \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 2}{p_2} \right) \left(\frac{p_3 - 2}{p_3} \right) \cdots \left(\frac{p_k - 2}{p_k} \right) \right) = \\ &= \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 2}{p_2} \right) \left(\frac{p_3 - 2}{p_3} \right) \cdots (p_k - 2) = \delta_k. \end{aligned}$$

■

5 The density of permitted k -tuples within the interval $I[1, n]$ as $n \rightarrow \infty$

Let S_k ($k > 2$) be a partial sum of the series $\sum s_k$. Let p_k be its characteristic prime modulus, and let m_k be its period. Let δ_k be the density of permitted k -tuples within the period of S_k . Let $I[1, n]$ ($n \geq m_k$) be a given interval of k -tuples of the partial sum S_k . Recall the notation $c_k^{I[1, n]}$ for the number of permitted k -tuples and $\delta_k^{I[1, n]}$ for the k -density in $I[1, n]$. In this section, we shall show that $\delta_k^{I[1, n]}$ converges to δ_k as $n \rightarrow \infty$. First, we present a definition.

Definition 5.1. Let $\lfloor n/m_k \rfloor$ denote the integer part of n/m_k ($n \geq m_k$). We denote by c_η the number of permitted k -tuples within the interval $I[1, \lfloor n/m_k \rfloor m_k] \subseteq I[1, n]$. If n is not a multiple of m_k , we denote by c_ϵ the number of permitted k -tuples within the interval $I[\lfloor n/m_k \rfloor m_k + 1, n] \subset I[1, n]$; otherwise, $c_\epsilon = 0$. We call the interval $I[\lfloor n/m_k \rfloor m_k + 1, n]$ the *incomplete period* of the interval $I[1, n]$.

The following lemma gives us a formula for the k -density in the interval $I[1, n]$.

Lemma 5.1. *We have*

$$\delta_k^{I[1, n]} = \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{n} \delta_k + \frac{p_k c_\epsilon}{n}.$$

Proof. By definition,

$$\delta_k^{I[1, n]} = \frac{c_k^{I[1, n]}}{\frac{n}{p_k}}.$$

Since $\lfloor n/m_k \rfloor$ is the number of times that the period of S_k fits in the interval $I[1, n]$, the interval $I[1, \lfloor n/m_k \rfloor m_k]$ is that part of $I[1, n]$ whose size is a multiple of m_k . Thus, $\lfloor n/m_k \rfloor m_k/p_k$ is the number of subintervals of size p_k within this part of the interval $I[1, n]$. Consequently, multiplying by the k -density in the period of S_k , we obtain

$$c_\eta = \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{p_k} \delta_k.$$

Since $c_k^{I[1, n]}$ is the number of permitted k -tuples within $I[1, n]$, we have $c_k^{I[1, n]} = c_\eta + c_\epsilon$. Then,

$$\delta_k^{I[1,n]} = \frac{c_k^{I[1,n]}}{\frac{n}{p_k}} = \frac{c_\eta + c_\epsilon}{\frac{n}{p_k}} = \frac{\lfloor \frac{n}{m_k} \rfloor m_k \delta_k + c_\epsilon}{\frac{n}{p_k}} = \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{n} \delta_k + \frac{p_k c_\epsilon}{n}.$$

■

Now, using the formula from the preceding lemma, we find lower and upper bounds for the k -density within the interval $I[1, n]$.

Lemma 5.2. *Let $I[1, n]$ ($n \geq m_k$) be an interval of k -tuples of a given partial sum S_k . Recall the notation c_k for the number of permitted k -tuples within the period of S_k . For $k > 2$,*

$$\frac{\lfloor \frac{n}{m_k} \rfloor m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + (m_k - 1)} \delta_k < \delta_k^{I[1,n]} < \frac{\left(\lfloor \frac{n}{m_k} \rfloor + 1 \right) m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + 1} \delta_k. \quad (13)$$

Proof. Step 1. We first consider the case where n is not a multiple of m_k . By Lemma 5.1,

$$\delta_k^{I[1,n]} = \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{n} \delta_k + \frac{p_k c_\epsilon}{n}. \quad (14)$$

To obtain bounds for $\delta_k^{I[1,n]}$, we proceed as follows. We begin by obtaining bounds for c_ϵ . By definition $\delta_k = c_k / (m_k / p_k)$, so, $c_k = \delta_k m_k / p_k$. Since, by assumption, n is not a multiple of m_k , it is easy to see that

$$0 \leq c_\epsilon \leq c_k = \delta_k m_k / p_k. \quad (15)$$

Next, we obtain bounds for the denominator in (14). Since n is not a multiple of m_k ,

$$\lfloor n/m_k \rfloor m_k + 1 \leq n \leq \lfloor n/m_k \rfloor m_k + (m_k - 1). \quad (16)$$

Step 2. We obtain a lower bound for $\delta_k^{I[1,n]}$. If we replace the denominator in (14) with the upper bound in (16),

$$\frac{\lfloor \frac{n}{m_k} \rfloor m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + (m_k - 1)} \delta_k + \frac{p_k c_\epsilon}{\lfloor \frac{n}{m_k} \rfloor m_k + (m_k - 1)} \leq \delta_k^{I[1,n]}. \quad (17)$$

Note that if n is equal to the upper bound in (16), the size of the incomplete period differs from period m_k by one. On the other hand, it is easy to check, using Proposition 2.3, that within the period of the partial sum S_k ($k > 2$), there is more than one permitted k -tuple. It follows that if n is equal to the upper bound in (16), then there is at least one permitted k -tuple within the incomplete period of $I[1, n]$; thus, $c_\epsilon > 0$. Therefore, if we replace c_ϵ in (17) with the lower bound in (15),

$$\frac{\lfloor \frac{n}{m_k} \rfloor m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + (m_k - 1)} \delta_k < \delta_k^{I[1,n]}. \quad (18)$$

Step 3. We now obtain an upper bound for $\delta_k^{I[1,n]}$. If we replace the denominator in (14) with the lower bound in (16),

$$\delta_k^{I[1,n]} \leq \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + 1} \delta_k + \frac{p_k c_\epsilon}{\lfloor \frac{n}{m_k} \rfloor m_k + 1}. \quad (19)$$

Note that if n is equal to the lower bound in (16), the size of the incomplete period is equal to 1, so there cannot be more than one permitted k -tuple within the incomplete period of $I[1, n]$. On the other hand, we saw in Step 2 that for a level $k > 2$, there is more than one permitted k -tuple within the period of the partial sum S_k . It follows that if n is equal to the lower bound in (16), then $c_\epsilon \leq 1 < \delta_k m_k / p_k$. Therefore, if we replace c_ϵ in (19) with the upper bound in (15),

$$\delta_k^{I[1, n]} < \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + 1} \delta_k + \frac{p_k \frac{\delta_k m_k}{p_k}}{\lfloor \frac{n}{m_k} \rfloor m_k + 1} = \frac{\left(\lfloor \frac{n}{m_k} \rfloor + 1 \right) m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + 1} \delta_k. \quad (20)$$

Step 4. Now we complete the proof. Suppose that n is a multiple of m_k . Then, clearly the density of permitted k -tuples within the interval $I[1, n]$ is equal to the density within the period of S_k ; that is, $\delta_k^{I[1, n]} = \delta_k$. Since the lower bound in (18) is less than δ_k and the upper bound in (20) is greater than δ_k , we conclude that for every interval $I[1, n]$ of the partial sum S_k ($k > 2$), the inequalities (18) and (20) are always satisfied, and the lemma is proved. \blacksquare

Remark 5.1. It is easy to check that in (13) the upper bound is decreasing and the lower bound is increasing as $n \rightarrow \infty$.

Finally, we show that the k -density in the interval $I[1, n]$ of a given partial sum S_k tends to δ_k as the size n of the interval increases.

Proposition 5.3. *Let S_k ($k > 2$) be a given partial sum of the series $\sum s_k$. As $n \rightarrow \infty$, the density $\delta_k^{I[1, n]}$ converges to δ_k , regardless of the combination of selected remainders in the sequences s_h that form the partial sum S_k .*

Proof. Using the inequalities of Lemma 5.2, if we take the limits as $n \rightarrow \infty$,

$$\lim_{n \rightarrow \infty} \frac{\lfloor \frac{n}{m_k} \rfloor m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + (m_k - 1)} \delta_k < \lim_{n \rightarrow \infty} \delta_k^{I[1, n]} < \lim_{n \rightarrow \infty} \frac{\left(\lfloor \frac{n}{m_k} \rfloor + 1 \right) m_k}{\lfloor \frac{n}{m_k} \rfloor m_k + 1} \delta_k.$$

Now, dividing the numerator and denominator by $\lfloor n/m_k \rfloor$, we obtain

$$\lim_{n \rightarrow \infty} \frac{m_k}{m_k + \frac{(m_k - 1)}{\lfloor \frac{n}{m_k} \rfloor}} \delta_k < \lim_{n \rightarrow \infty} \delta_k^{I[1, n]} < \lim_{n \rightarrow \infty} \frac{\left(1 + \frac{1}{\lfloor \frac{n}{m_k} \rfloor} \right) m_k}{m_k + \frac{1}{\lfloor \frac{n}{m_k} \rfloor}} \delta_k.$$

Since for a given level k , the values m_k and δ_k are constant, as $n \rightarrow \infty$, we have $\lfloor n/m_k \rfloor \rightarrow \infty$, and the lower and upper bounds tend to δ_k . Thus $\delta_k^{I[1, n]}$ converges to δ_k as $n \rightarrow \infty$. \blacksquare

6 The k -density within the intervals $I[1, p_k^2]$ and $I[p_k^2 + 1, m_k]$

Let S_k ($k \geq 4$) be a given partial sum of the series $\sum s_k$. In this section, we shall subdivide the interval $I[1, m_k]$ of S_k into two parts and establish the relationship between the density of permitted k -tuples within one part and the density of permitted k -tuples within the other part. We begin by introducing some terminology and notation.

Definition 6.1. Let S_k and S_{k+1} be consecutive partial sums of the series $\sum s_k$. We use the notation $p_k \rightarrow p_{k+1}$, or alternatively $k \rightarrow k + 1$, to denote the transition from level k to level $k + 1$. For the level transition $p_k \rightarrow p_{k+1}$, we call the difference $p_{k+1} - p_k$ the *order* of the transition.

Definition 6.2. When we juxtapose the remainders of the sequence s_{k+1} to each k -tuple of S_k , by Proposition 2.2, a given permitted k -tuple of S_k , whose index is congruent to a selected remainder of s_{k+1} modulo p_{k+1} , is converted to a prohibited $(k + 1)$ -tuple of S_{k+1} . In that case, we say that at the level transition $k \rightarrow k + 1$, one permitted k -tuple is *removed*.

Let s_h ($1 \leq h \leq k$) be the periodic sequences of remainders that form the partial sum S_k . Recall the notation m_h for the period of the partial sum S_h ; recall the notation c_h for the number of permitted h -tuples and δ_h for the h -density within the period of the partial sum S_h ($1 \leq h \leq k$). For every partial sum S_h from level $h = 1$ to level $h = k$ in the horizontal position, let us consider the interval $I[1, m_k]_h$, whose size is the period m_k of S_k .

Remark 6.1. Using Proposition 2.1, it is easy to check that the period of the partial sum S_1 is equal to $m_1 = p_1 = 2$. On the other hand, by Proposition 2.3, within every period of S_1 we have only one permitted 1-tuple. Therefore, the interval $I[1, m_k]_1$ of the partial sum S_1 is divided into subintervals of size $m_1 = 2$, each containing one permitted 1-tuple. The position of the permitted 1-tuple is the same within every subinterval and is determined by the selected remainder in the sequence s_1 .

Remark 6.2. According to the preceding remark, the positions of the permitted 1-tuples show a regular pattern along the interval $I[1, m_k]_1$ of the partial sum S_1 . However, when we add the sequences s_h from level $h = 2$ to level $h = k$, the selected remainders in each sequence s_h remove permitted $(h-1)$ -tuples from the partial sum S_{h-1} . Consequently, we obtain an interval $I[1, m_k]_k$ where the permitted k -tuples are spread along the interval in positions that show an irregular pattern. Note that if we change the combination of selected remainders in the sequences s_h ($1 \leq h \leq k$), within the interval $I[1, m_k]_k$, some permitted k -tuples ‘disappear’, and other permitted k -tuples ‘appear’, although the number of permitted k -tuples within the interval $I[1, m_k]_k$ of the partial sum S_k does not change (see Proposition 2.3).

The following lemma gives us the number of permitted h -tuples within the interval $I[1, m_k]_h$ of every partial sum S_h where $h < k$.

Lemma 6.1. *Let S_k ($k \geq 4$) be a given partial sum of the series $\sum s_k$. For any given partial sum S_h ($h < k$), the number of permitted h -tuples within the interval $I[1, m_k]_h$ is equal to $c_h p_{h+1} p_{h+2} \cdots p_k$.*

Proof. Choose a level $h < k$. By definition, we have $m_k = p_1 p_2 p_3 \cdots p_h p_{h+1} p_{h+2} \cdots p_k = m_h p_{h+1} p_{h+2} \cdots p_k$. That is, the size of the interval $I[1, m_k]_h$ of the partial sum S_h is equal to $p_{h+1} p_{h+2} \cdots p_k$ times the period m_h of the partial sum S_h . Consequently, it is easy to see that the number of permitted h -tuples within the interval $I[1, m_k]_h$ is equal to $c_h p_{h+1} p_{h+2} \cdots p_k$. ■

Now, let us denote by c'_h the number of permitted h -tuples within the interval $I[1, m_k]_h$ of every partial sum S_h ($1 \leq h \leq k$), which is computed using Proposition 2.3 and Lemma 6.1. We have a question at this point: What is the behaviour of c'_h as h goes from level 1 to level k ? This behaviour is given by the following lemma.

Lemma 6.2. *Let h and $h + 1$ be consecutive levels, where $1 \leq h < k$. We have*

$$c'_{h+1} = c'_h \left(\frac{p_{h+1} - 2}{p_{h+1}} \right).$$

Proof. Given the partial sum S_h ($1 \leq h < k$), suppose that we juxtapose the remainders of the sequence s_{h+1} to each h -tuple of S_h . By Proposition 2.2, the permitted h -tuples within the interval $I[1, m_k]_h$ whose indices are included in two residue classes modulo p_{h+1} are removed by the selected remainders within the sequence s_{h+1} , and the permitted h -tuples whose indices are not included in these residue classes are transferred to level $h + 1$ as permitted $(h + 1)$ -tuples within the interval $I[1, m_k]_{h+1}$ of the partial sum S_{h+1} , regardless of the combination of selected remainders in the sequence s_{h+1} . Since for every level $h < k$, the size of the interval $I[1, m_k]_h$ is a multiple of p_{h+1} , by Proposition 2.4 and Corollary 2.5, the indices of permitted h -tuples within the interval $I[1, m_k]_h$ of S_h are distributed uniformly over the residue classes modulo p_{h+1} . Therefore, a $2/p_{h+1}$ fraction of the permitted h -tuples within the interval $I[1, m_k]_h$ of S_h have been removed, and a $(p_{h+1} - 2)/p_{h+1}$ fraction have been transferred to level $h + 1$ as permitted $(h + 1)$ -tuples within the interval $I[1, m_k]_{h+1}$ of S_{h+1} , regardless of the combination of selected remainders in the sequence s_{h+1} . From this result, the lemma follows. ■

Remark 6.3. By Proposition 2.3 and Lemma 6.1, the number of permitted h -tuples within the interval $I[1, m_k]_h$ ($1 \leq h \leq k$) does not depend on the combination of selected remainders in the sequences s_h that form the partial sum S_h , therefore, neither does the density of permitted h -tuples within this interval. Furthermore, since the size of $I[1, m_k]_h$ is a multiple of m_h , the density of permitted h -tuples within the interval $I[1, m_k]_h$ is equal to δ_h (the density of permitted h -tuples within the period m_h of the partial sum S_h).

Let us now examine the behaviour of δ_h as h goes from level 1 to level k . Since the selected remainders of the sequences s_{h+1} remove permitted h -tuples within the interval $I[1, m_k]_h$ of the partial sum S_h , at each level transition $h \rightarrow h + 1$, the number of permitted h -tuples decreases as the level increases from $h = 1$ to $h = k$ (the factor by which we must multiply c'_h to obtain c'_{h+1} is given by Lemma 6.2). However, by Lemma 3.2 and Corollary 3.3, the h -density within the interval $I[1, m_k]_h$ of the partial sum S_h grows at each transition $p_h \rightarrow p_{h+1}$ of order greater than 2; and if $p_h \rightarrow p_{h+1}$ is a level transition of order 2, the h -density within $I[1, m_k]_h$ does not change.

Remark 6.4. Note that if $p_h \rightarrow p_{h+1}$ is a level transition of order greater than 2, δ_h increases because to compute the h -density we count the permitted h -tuples within subintervals of size p_h , which grow by more than 2, overcompensating for the removed permitted h -tuples. On the other hand, if $p_h \rightarrow p_{h+1}$ is a level transition of order 2, δ_h does not change because the increase in the size p_h is compensated for by the removed permitted h -tuples. (Observe that $p_1 \rightarrow p_2$ is the only level transition where δ_h decreases.) Note that the result from Lemma 3.2 can be written in the form

$$\delta_{h+1} = \delta_h \left(\frac{p_{h+1} - 2}{p_{h+1}} \right) \left(\frac{p_{h+1}}{p_h} \right),$$

where the factor $(p_{h+1} - 2)/p_{h+1}$ is related to the permitted h -tuples removed from $I[1, m_k]_h$ (see Lemma 6.2), and the factor p_{h+1}/p_h is related to the increase of the size of the subintervals.

Now, if we ‘cut’ the first period of S_k into two parts between the indices p_k^2 and $p_k^2 + 1$, we obtain a left-hand subinterval and a right-hand subinterval.

Definition 6.3. Let S_k ($k \geq 4$) be a given partial sum in the horizontal position. We subdivide the interval $I[1, m_k]$ (its first period) into two intervals: $I[1, p_k^2]$, which we call the *Left interval*, and $I[p_k^2 + 1, m_k]$, which we call the *Right interval*. We often denote the Left interval $I[1, p_k^2]$ by the symbol L_k and the Right interval $I[p_k^2 + 1, m_k]$ by the symbol R_k . For every partial sum S_h from level $h = 1$ to level $h = k - 1$, there is also a Left interval $I[1, p_k^2]_h$ and a Right interval $I[p_k^2 + 1, m_k]_h$. See Figure 4.

As shown in the Introduction, the first period of the sequence of k -tuples can be seen as a matrix with m_k columns and k rows. In addition, this matrix has been partitioned into two blocks: the *Left block* formed by the columns from $n = 1$ to $n = p_k^2$ and the *Right block* formed by the columns from $n = p_k^2 + 1$ to $n = m_k$. Each row of the Left block is formed by the remainders of dividing the integers from $n = 1$ to $n = p_k^2$ by the modulus p_h , and each row of the Right block is formed by the remainders of dividing the integers from $n = p_k^2 + 1$ to $n = m_k$ by the modulus p_h .

$$\begin{array}{ccccc} \text{Level } h = k & I[1, p_k^2]_{h=k} & \cup & I[p_k^2 + 1, m_k]_{h=k} & = & I[1, m_k]_{h=k} \\ \vdots & \vdots & & \vdots & & \vdots \\ \text{Level } h = h' & I[1, p_k^2]_{h=h'} & \cup & I[p_k^2 + 1, m_k]_{h=h'} & = & I[1, m_k]_{h=h'} \\ \vdots & \vdots & & \vdots & & \vdots \\ \text{Level } h = 1 & I[1, p_k^2]_{h=1} & \cup & I[p_k^2 + 1, m_k]_{h=1} & = & I[1, m_k]_{h=1} \end{array}$$

Figure 4: Left and Right intervals

Definition 6.4. For a given partial sum S_h ($1 \leq h \leq k$), we use the notation $c_h^{L_k}$ to denote the number of permitted h -tuples within the Left interval $I[1, p_k^2]_h$, and we use the notation $c_h^{R_k}$ to denote the number of permitted h -tuples within the Right interval $I[p_k^2 + 1, m_k]_h$.

Although the number of permitted h -tuples within the interval $I[1, m_k]_h$ of every partial sum S_h ($1 \leq h \leq k$) does not change if we choose another set of selected remainders, the positions of the permitted h -tuples along the period of S_h do change. Thus, it appears reasonable to expect that some permitted h -tuples will be transferred from the Left interval $I[1, p_k^2]_h$ to the Right interval $I[p_k^2 + 1, m_k]_h$, or vice versa. Hence, the number of permitted h -tuples within the Left interval $I[1, p_k^2]_h$ and within the Right interval $I[p_k^2 + 1, m_k]_h$ is determined by the combination of the selected remainders in the sequences s_h that form the partial sum S_h .

Definition 6.5. For a given partial sum S_h ($1 \leq h \leq k$), we use the notation $\delta_h^{L_k}$ to denote the density of permitted h -tuples within the Left interval $I[1, p_k^2]_h$, and we use the notation $\delta_h^{R_k}$ to denote the density of permitted h -tuples within the Right interval $I[p_k^2 + 1, m_k]_h$.

According to Remark 6.3, the h -density within the interval $I[1, m_k]_h$ does not depend on the combination of selected remainders in the sequences s_h that form the partial sum S_h . However, the transfer of some permitted h -tuples from the Left interval $I[1, p_k^2]_h$ to the Right interval $I[p_k^2 + 1, m_k]_h$, or in the opposite direction, when we change the combination of selected remainders, changes the h -density within both intervals. The crossing of some permitted h -tuples from $I[1, p_k^2]_h$ to $I[p_k^2 + 1, m_k]_h$ decreases $\delta_h^{L_k}$ and increases $\delta_h^{R_k}$, and vice versa. By Theorem 4.3, the average of $\delta_h^{L_k}$ within $I[1, p_k^2]_h$ is equal to δ_h , and the average of $\delta_h^{R_k}$ within $I[p_k^2 + 1, m_k]_h$ is also equal to δ_h . Hence,

$$\begin{aligned} \delta_h^{L_k} > \delta_h &\iff \delta_h^{R_k} < \delta_h, \\ \delta_h^{L_k} < \delta_h &\iff \delta_h^{R_k} > \delta_h. \end{aligned} \tag{21}$$

7 A lower bound for the sifting function of the Sieve II

For every partial sum S_h from level $h = 1$ to level $h = k$ ($k \geq 4$), let us consider the interval $I[1, m_k]_h$, the Left interval $I[1, p_k^2]_h$ and the Right interval $I[p_k^2 + 1, m_k]_h$. Recall the notation δ_h for the density of permitted h -tuples within the period of S_h , and recall the notation $\delta_h^{L_k}$ and $\delta_h^{R_k}$ for the density of permitted h -tuples within the intervals $I[1, p_k^2]_h$ and $I[p_k^2 + 1, m_k]_h$, respectively.

In this section, we shall prove that there exists a sufficiently large integer $K_\alpha > 4$ such that the number of permitted k -tuples within the Left interval $I[1, p_k^2]$ of the partial sum S_k (the sifting function of Sieve II) is greater than $p_k/2$ for every $k > K_\alpha$, regardless of the combination of selected remainders in the sequences s_h that form the partial sum S_k .

Given the partial sum S_k and a particular combination of selected remainders in S_k , we begin by asking whether it can occur that there are no permitted k -tuples within a given interval $I[1, n]_k$ ($n > 1$) of S_k . Consider the interval $I[1, n]_h$ of every partial sum S_h from $h = 1$ to $h = k$. Assume that there are some permitted 1-tuples within the interval $I[1, n]_1$ of the partial sum S_1 (see Remark 6.1). We know that when the sequences s_h from level $h = 2$ to level $h = k$ are added, the selected remainders in every sequence s_h remove permitted $(h - 1)$ -tuples from the partial sum S_{h-1} (see Remark 6.2). Clearly, it can happen that there are no permitted k -tuples within the interval $I[1, n]_k$ of S_k if k is sufficiently large. On the other hand, for a given k there must be permitted k -tuples within the interval $I[1, n]_k$ of S_k if n is sufficiently large, since the density of permitted k -tuples within this interval converges to δ_k as $n \rightarrow \infty$, by Proposition 5.3.

We can see that the quantity of permitted k -tuples within the interval $I[1, n]_k$ of S_k depends on the level k and the size n of this interval. Thus, as $k \rightarrow \infty$, the chance that there are permitted k -tuples within $I[1, n]_k$ is given by the relationship between k and the size of $I[1, n]_k$. In the case of the Left interval $n = p_k^2$, so the relationship between k and the size of $I[1, n]_k$ follows from the sequence of the primes.

As we have seen in Section 6, the density of permitted h -tuples within every interval $I[1, m_k]_h$ ($1 \leq h \leq k$), denoted by δ_h , does not depend on the combination of selected remainders in the sequences s_h that form the partial sum S_h (see Remark 6.3). Furthermore, δ_h increases between $h = 1$ and $h = k$, by Lemma 3.2 and Corollary 3.3, for sufficiently large k .

Now, the density of permitted h -tuples within every Left interval $I[1, p_k^2]_h$ ($1 \leq h \leq k$), denoted by $\delta_h^{L_k}$, clearly depends on the combination of selected remainders in S_k . However, it seems reasonable to conjecture that, for sufficiently large k the behaviour of $\delta_h^{L_k}$ as h goes from level 1 to level k is similar to the behaviour of δ_h . Thus, for sufficiently large k it should be $\delta_k^{L_k} > \delta_4$ (see Introduction, Subsection 1.8). Before proving this, we need the following remarks.

Remark 7.1. Let S_k be a given partial sum of the series $\sum s_k$ with a particular combination of selected remainders in the sequences s_h ($1 \leq h \leq k$) that form S_k . Given a partial sum S_h ($1 \leq h \leq k$), when the interval $I[1, m_k]_h$ is subdivided into the Left interval $I[1, p_k^2]_h$ and the Right interval $I[p_k^2 + 1, m_k]_h$, the proportion of permitted h -tuples within the Left interval $I[1, p_k^2]_h$ will be greater than the proportion of permitted h -tuples within the Right interval $I[p_k^2 + 1, m_k]_h$, or vice versa, since p_k^2 is not a multiple of m_h .

Remark 7.2. From the preceding remark, it follows that when the interval $I[1, m_k]_h$ of S_h ($1 \leq h \leq k$) is subdivided into the Left interval $I[1, p_k^2]_h$ and the Right interval $I[p_k^2 + 1, m_k]_h$, the h -density within the Left interval $I[1, p_k^2]_h$ will be greater than the h -density within the Right interval $I[p_k^2 + 1, m_k]_h$; or vice versa (see (21) and the paragraph preceding these inequalities). Therefore, considering the Left intervals $I[1, p_k^2]_h$ from $h = 1$ to $h = k$ (left block of the partition of the first period of S_k), there must be levels for which $\delta_h^{L_k} < \delta_h$ mixed with levels for which $\delta_h^{L_k} > \delta_h$, for k sufficiently large.

Definition 7.1. Let S_k be a given partial sum of the series $\sum s_k$, where there is a particular combination of selected remainders. Given the level transition $p_h \rightarrow p_{h+1}$ ($1 \leq h < k$), we denote by $F_{h, h+1}^{L_k}$ the fraction of the permitted h -tuples within the Left interval $I[1, p_k^2]_h$ of S_h that are transferred to the Left interval $I[1, p_k^2]_{h+1}$ of S_{h+1} as permitted $(h + 1)$ -tuples. Note that by Lemma 6.2, the average of $F_{h, h+1}^{L_k}$ is equal to $(p_{h+1} - 2)/p_{h+1}$.

Remark 7.3. Let S_k be a given partial sum of the series $\sum s_k$. Given a particular combination of selected remainders in S_k , suppose that in every level transition $p_h \rightarrow p_{h+1}$ ($1 \leq h < k$), the value of $F_{h, h+1}^{L_k}$ is very close to the average fraction $(p_{h+1} - 2)/p_{h+1}$, given by Lemma 6.2. In this case, if k is sufficiently large, $\delta_h^{L_k}$ must increase between $h = 1$ and $h = k$, by the arguments given in Remark 6.4 for the average δ_h .

Now, suppose that there exists a level $h = h'$ ($1 < h' < k$), where the difference $k - h'$ is sufficiently large, such that $\delta_h^{L_k}$ does not increase between $h = h'$ and $h = k$. Clearly, this can only happen if there are level transitions $p_h \rightarrow p_{h+1}$ between $h = h'$ and $h = k$ for which $F_{h, h+1}^{L_k}$ is much less than the average fraction $(p_{h+1} - 2)/p_{h+1}$ given by Lemma 6.2.

Remark 7.4. Let S_k be a partial sum of the series $\sum s_k$, and consider a given level $h = h'$ ($1 < h' < k$). Given consecutive primes p_h and p_{h+1} , we denote $g_h = p_{h+1} - p_h$. Assume that in each period (of size p_h) of every sequence s_h from $h = h' + 1$ to $h = k$ of S_k there are g_h selected remainders (the same in every period of the sequence). As we have seen in Remark 6.2, the selected remainders in every sequence s_h ($h' < h \leq k$) remove permitted $(h - 1)$ -tuples from the partial sum S_{h-1} . However, in this case the fraction of permitted h -tuples within the interval $I[1, m_k]_h$ of

S_h that are transferred to the interval $I[1, m_k]_{h+1}$ of S_{h+1} as permitted $(h+1)$ -tuples is equal to $(p_{h+1} - g_h)/p_{h+1}$, where $h' \leq h < k$, regardless of the combination of selected remainders in S_k (see the proof of Lemma 6.2). So, for sufficiently large k , the whole number of permitted h -tuples removed between $h = h'$ and $h = k$ is rather greater than in the case where there are only two selected remainders in the sequences s_h ($h' < h \leq k$). Furthermore, in every level transition $p_h \rightarrow p_{h+1}$ ($h' \leq h < k$), the increase of δ_h in this case would be given by

$$\delta_{h+1} = \delta_h \left(\frac{p_{h+1} - g_h}{p_{h+1}} \right) \left(\frac{p_{h+1}}{p_h} \right) = \delta_h,$$

(see Remark 6.4). This means that under the preceding assumption, the h -density within the interval $I[1, m_k]_h$ of S_h does not increase between $h = h'$ and $h = k$.

Lemma 7.1. *Let S_k ($k > 4$) be a partial sum of the series $\sum s_k$. Let $I[1, p_k^2]_h$ be the Left interval for every partial sum S_h from $h = 1$ to $h = k$, and let $\delta_h^{L_k}$ be the density of permitted h -tuples within every interval $I[1, p_k^2]_h$.*

For every real number $M > 0$ there is a positive integer K (not depending on the combination of selected remainders in S_k) such that $\delta_k^{L_k} > M$ for every $k > K$.

Proof. Step 1. The average of the h -density within every Left interval $I[1, p_k^2]_h$ from $h = 1$ to $h = k$ is equal to δ_h , by Theorem 4.3. Recall that, as the level increases from $h = 1$ to $h = k$, the average δ_h increases at each level transition $p_h \rightarrow p_{h+1}$ of order greater than 2, and, if $p_h \rightarrow p_{h+1}$ is a level transition of order 2, δ_h does not change, as we have seen in the paragraph below Remark 6.3 and in Remark 6.4. Therefore, for sufficiently large k , the average of the h -density within every Left interval $I[1, p_k^2]_h$ increases between $h = 1$ and $h = k$ (see Lemma 3.2).

The fact that the average of the h -density within every Left interval $I[1, p_k^2]_h$ ($1 \leq h \leq k$) is δ_h , together with Remark 7.2 suggest that for every h ($1 \leq h \leq k$) the value of $\delta_h^{L_k}$ is relatively close to δ_h , if k is sufficiently large. Assuming this, it follows that $\delta_k^{L_k} > M$ for every k sufficiently large (no matter the combination of selected remainders in S_k), since $\delta_k \rightarrow \infty$ as $k \rightarrow \infty$ by Theorem 3.4.

Step 2. Consider a partial sum S_k with a particular combination of selected remainders. Let us examine the behaviour of the h -density within every Left interval $I[1, p_k^2]_h$, denoted by $\delta_h^{L_k}$, as h goes from level 1 to level k . For sufficiently large k , the positions of the permitted 1-tuples show a regular pattern along the Left interval $I[1, p_k^2]_1$ of the partial sum S_1 (see Remark 6.1). As we have seen in Remark 6.2, when we add the sequences s_h from level $h = 2$ to level $h = k$, the selected remainders in every sequence s_h remove permitted $(h-1)$ -tuples from the partial sum S_{h-1} . Thus, the number and proportion of permitted h -tuples within the Left interval $I[1, p_k^2]_h$ decrease slowly as the level increases from $h = 1$ to $h = k$.

Now, assume that for every level transition $p_h \rightarrow p_{h+1}$ ($1 \leq h < k$) the value of $F_{h, h+1}^{L_k}$ is sufficiently close to the average fraction $(p_{h+1} - 2)/p_{h+1}$, given by Lemma 6.2. In this case, for k sufficiently large $\delta_h^{L_k}$ must increase as h goes from level 1 to level k , by the same arguments given in Remark 6.4 for the average δ_h (see Remark 7.3).

Step 3. Consider S_k ($k > 5$) with a particular combination of selected remainders. Choose a fixed level $h = h'$ ($4 < h' < k$). As $k \rightarrow \infty$, the following two things occur at the same time:

- (a) For the fixed level h' , the size of the Left interval $I[1, p_k^2]_{h'}$ increases, so $\delta_{h'}^{L_k}$ converges uniformly to $\delta_{h'}$, by Proposition 5.3. Thus, given any small number $\varepsilon > 0$, for a level k sufficiently large it must be

$$\delta_{h'} - \varepsilon < \delta_{h'}^{L_k} < \delta_{h'} + \varepsilon,$$

regardless of the combination of selected remainders in S_k .

- (b) The number and proportion of the level transitions $h \rightarrow h+1$ of order greater than 2 increase between $h = h'$ and $h = k$.

Step 4. Now, given any fixed level h such that $1 \leq h < h'$, as the size of the Left interval $I[1, p_k^2]_h$ increases (as $k \rightarrow \infty$), $\delta_h^{L_k}$ also converges uniformly to δ_h , by Proposition 5.3. Note that, as the size of the Left interval $I[1, p_k^2]_h$ increases, the number of times that m_h (the period of S_h) fits in $I[1, p_k^2]_h$ increases more and more, and this fact is underlying the result $\delta_h^{L_k} \rightarrow \delta_h$. Therefore, for a level k sufficiently large, if $\delta_{h'} - \varepsilon < \delta_{h'}^{L_k} < \delta_{h'} + \varepsilon$ (see Step 3 (a)), then $\delta_h - \varepsilon < \delta_h^{L_k} < \delta_h + \varepsilon$ for every h ($1 \leq h < h'$), since $m_{h+1} = m_h p_{h+1}$, regardless of the combination of selected remainders in S_k . Thus, $\delta_h^{L_k}$ will be very close to δ_h for every level from $h = 1$ to $h = h'$, if ε is sufficiently small and k sufficiently large. This means that the behaviour of $\delta_h^{L_k}$ is very similar to the behaviour of δ_h , so, $\delta_h^{L_k}$ increases between $h = 1$ and $h = h'$.

Step 5. Consider the interval $I[1, m_k]_h$ in every partial sum S_h ($h' \leq h \leq k$). Under the condition assumed in Remark 7.4 (with regard to the selected remainders in the sequences s_h), for every level transition $p_h \rightarrow p_{h+1}$ from $h = h'$ to $h = k - 1$, the fraction of permitted h -tuples within the interval $I[1, m_k]_h$ of S_h that are transferred to the interval $I[1, m_k]_{h+1}$ of S_{h+1} as permitted $(h+1)$ -tuples is $(p_{h+1} - g_h)/p_{h+1}$. Hence, for every level transition $p_h \rightarrow p_{h+1}$ ($h' \leq h < k$) of order greater than 2 (that is $g_h > 2$), the number of permitted h -tuples removed from $I[1, m_k]_h$ is rather greater than in the case where there are only two selected remainders in the sequences s_h ($h' < h \leq k$), so, the density of permitted h -tuples within $I[1, m_k]_h$ does not increase as h goes from level h' to level k .

In our case the condition assumed in Remark 7.4 is not present (see Definition 2.7), so, for every level transition $p_h \rightarrow p_{h+1}$ ($h' \leq h < k$), the fraction of permitted h -tuples within the interval $I[1, m_k]_h$ of S_h that are transferred to the interval $I[1, m_k]_{h+1}$ of S_{h+1} as permitted $(h+1)$ -tuples is $(p_{h+1} - 2)/p_{h+1}$, by Lemma 6.2. Thus, for sufficiently large k , the density of permitted h -tuples within $I[1, m_k]_h$ increases between $h = h'$ and $h = k$, as we have seen in Section 6. Undoubtedly, in the case of the Left intervals $I[1, p_k^2]_h$ ($h' \leq h \leq k$), for every level transition $p_h \rightarrow p_{h+1}$ ($h' \leq h < k$) the fraction $F_{h, h+1}^{L_k}$ must be much closer to $(p_{h+1} - 2)/p_{h+1}$ than to $(p_{h+1} - g_h)/p_{h+1}$. Thus, in view of Step 3 (b), it follows that $\delta_h^{L_k}$ must increase between $h = h'$ and $h = k$ for sufficiently large k (see the second paragraph in Step 2).

Step 6. However, one can ask the following question: Could there be a particular combination of selected remainders in S_k such that $\delta_k^{L_k} \leq \delta_{h'} + \varepsilon$ for sufficiently large k ?

Suppose we choose another fixed level $h = h^*$ ($h' < h^* < k$), such that the average density δ_{h^*} is much larger than $\delta_{h'}$. By Step 3 (a) and Step 4, for every sufficiently large k we have

$$\delta_h - \varepsilon < \delta_h^{L_k} < \delta_h + \varepsilon \quad (1 \leq h \leq h^*), \quad (22)$$

where ε is sufficiently small that $\delta_h^{L_k}$ is very close to δ_h . If we assume that the answer to the above question is affirmative, this implies that $\delta_h^{L_k}$ increases first between $h = 1$ and $h = h^*$, and then decreases between $h = h^*$ and $h = k$ to a value less than or equal to $\delta_{h'} + \varepsilon$. In order for $\delta_h^{L_k}$ to decrease between $h = h^*$ and $h = k$ it is necessary $F_{h, h+1}^{L_k}$ ($h^* \leq h < k$) to be much less than the average fraction $(p_{h+1} - 2)/p_{h+1}$ given by Lemma 6.2 (see Remark 7.3). That is, the number of permitted h -tuples removed from every Left interval $I[1, p_k^2]_h$ between $h = h^*$ and $h = k$ must be much greater than the average number.

Now, suppose that the condition assumed in Remark 7.4 is satisfied for every level from $h = h^* + 1$ to $h = k$. In this case, as we have seen in the preceding step, the number of permitted h -tuples removed from every interval $I[1, m_k]_h$ is rather greater than in the case given by Definition 2.7, thus, the density of permitted h -tuples within $I[1, m_k]_h$ cannot increase as h goes from level h^* to level k . Clearly, δ_k will be equal to δ_{h^*} and $\delta_k^{L_k}$ will be rather close to δ_{h^*} , so, $\delta_k^{L_k}$ will be rather close to δ_{h^*} by (22). Thus, since δ_{h^*} is much greater than $\delta_{h'}$, it follows that the condition assumed in Remark 7.4 is not sufficient for $\delta_h^{L_k}$ to decrease between $h = h^*$ and $h = k$ to a value less than or equal to $\delta_{h'} + \varepsilon$, for sufficiently large h^* and sufficiently large k . Then clearly the stipulation established by Definition 2.7 is not sufficient either. Therefore, we answer the above question in the negative, thus, $\delta_k^{L_k} > \delta_{h'} + \varepsilon$ for every sufficiently large k and every combination of selected remainders in S_k .

Step 7. From Step 4, Step 5 and Step 6 we see that $\delta_h^{L_k}$ increases between $h = 1$ and $h = k$ for sufficiently large k , regardless of the combination of selected remainders in S_k , as we have assumed in the second paragraph of Step 2.

Now, given M , suppose we choose a level $h = h'$ such that $\delta_{h'} > M$ (see Theorem 3.4). By the arguments given in Step 3 (a), as k increases $\delta_{h'}^{L_k}$ tends to $\delta_{h'}$, thus, since $\delta_{h'} > M$ there must exist K' such that $\delta_{h'}^{L_k} > M$ for every $k > K'$, no matter the combination of selected remainders in S_k .

On the other hand, by steps 5 and 6 there must exist $K > K'$ such that $\delta_k^{L_k} > \delta_{h'}^{L_k}$ for every $k > K$, so, $\delta_k^{L_k} > M$ by the preceding paragraph, regardless of the combination of selected remainders in S_k . The lemma is proved. ■

Corollary 7.2. *There exists an integer $K_\alpha > 4$ such that $\delta_k^{L_k} > \delta_4$ for every $k > K_\alpha$, regardless of the combination of selected remainders in S_k .*

Proof. This follows immediately taking $M = \delta_4$. ■

Definition 7.2. Let S_k be the partial sum associated to Sieve II. Recall that in Section 2, we have taken $\mathcal{B} = \{n : 1 \leq n \leq p_k^2\}$. Let $T(\mathcal{B}, \mathcal{P}, p_k)$ be the sifting function of Sieve II. We denote by $\{T(\mathcal{B}, \mathcal{P}, p_k)\}$ the set of values of $T(\mathcal{B}, \mathcal{P}, p_k)$ for all combinations of selected remainders in the sequences that form the partial sum S_k .

Now, we can obtain a lower bound for the sifting function of Sieve II (that is, a lower bound for the number of permitted k -tuples within the Left interval $I[1, p_k^2]$ of S_k) for sufficiently large k .

Lemma 7.3. *Let K_α be the number whose existence is established in Corollary 7.2. For level $k > K_\alpha$, we have $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\} > p_k/2$.*

Proof. Step 1. Let S_k be the partial sum associated to Sieve II. We use the notation $\{\delta_k^{L_k}\}$ to denote the set of values of $\delta_k^{L_k}$ for all the combinations of selected remainders in the sequences that form the partial sum S_k . Since there are p_k subintervals of size p_k in the Left interval $I[1, p_k^2]$ of S_k , the minimum number of permitted k -tuples within $I[1, p_k^2]$ is $p_k \min\{\delta_k^{L_k}\}$. Then, by definition, $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\} = p_k \min\{\delta_k^{L_k}\}$.

Step 2. Now, by Lemma 7.1 and Corollary 7.2, if $k > K_\alpha$, then $\min\{\delta_k^{L_k}\} > \delta_4$. From this result and Step 1, it follows that $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\} > p_k \delta_4$, whenever $k > K_\alpha$. Using Lemma 3.1, it is easy to check that $\delta_4 = 1/2$ (see Table 1), so $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\} > p_k/2$ if $k > K_\alpha$. ■

8 Proof of the Main Theorem

In this section, we prove the main theorem. We begin by defining formally the sequence of k -tuples of the Sieve associated with x (Sieve I).

Definition 8.1. Let $x > 49$ be an even number, and let k be the index of the greatest prime less than \sqrt{x} . Let $\{b_1, b_2, b_3, \dots, b_k\}$ be the ordered set of the remainders of dividing x by $p_1, p_2, p_3, \dots, p_k$. We define the sequence of k -tuples of remainders of level k , where the following rules for selecting remainders are applied in the sequences of remainders modulo p_h ($1 \leq h \leq k$) that form this sequence of k -tuples.

Rule 1. Within every period of size p_h of the sequence s_h ($1 \leq h \leq k$), the remainder 0 is selected.

Rule 2. Within every period of size p_h of the sequence s_h ($1 \leq h \leq k$), the remainder b_h is selected.

Now, we can formally define the formulation of Sieve I based on a sequence of k -tuples, as follows.

Definition 8.2. Let \mathcal{P} be the sequence of primes, let $z = \sqrt{x}$, and let p_k be the greatest prime less than z . Let \mathcal{A} be the set consisting of the indices n of the sequence of k -tuples of the preceding definition that lie in the interval $[1, x]$. For each $p = p_h \in \mathcal{P}$ ($1 \leq h \leq k$), the subset \mathcal{A}_p of \mathcal{A} consists of the indices n of the sequence of k -tuples such that the remainder of dividing n by the modulus p_h is a selected remainder. Then, the indices of the prohibited k -tuples lying in \mathcal{A} are sifted out, and the indices of the permitted k -tuples lying in \mathcal{A} remain unsifted. See Remark 1.1. The sifting function

$$S(\mathcal{A}, \mathcal{P}, z) = \left| \mathcal{A} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p < z}} \mathcal{A}_p \right|,$$

is given by the number of permitted k -tuples whose indices lie in the set \mathcal{A} .

Remark 8.1. Every sequence s_h ($1 \leq h \leq k$) that forms the sequence of k -tuples associated to Sieve I consists of the remainders of dividing n by p_h . If a remainder is equal to 0, it is always a selected remainder. If a remainder is equal to b_h , it is also a selected remainder. If x is divisible by p_h , then $b_h = 0$; therefore, in every period p_h of s_h , there is only one selected remainder.

The following theorem shows that if n is the index of a permitted k -tuple belonging to the set \mathcal{A} and $1 < n < x$, then n is a prime such that either $x - n = 1$ or $x - n$ is also a prime.

Theorem 8.1. *Let $x > 49$ be an even number, and let k be the index of the greatest prime less than $z = \sqrt{x}$. Let us consider Sieve I and its associated sequence of k -tuples. If n ($1 < n < x$) is an unsifted element of the set \mathcal{A} , then n is a prime such that either $x - n = 1$ or $x - n$ is also a prime.*

Proof. Step 1. By definition, the set \mathcal{A} consists of the indices of the sequence of k -tuples associated to Sieve I that lie in $[1, x]$. Since n is an unsifted element of the set \mathcal{A} , by definition, n is the index of a permitted k -tuple. In the sequences of remainders modulo p_h ($1 \leq h \leq k$) that form this sequence of k -tuples, if a remainder is equal to 0, then it is a selected remainder; thus, by definition, a permitted k -tuple in this sequence has no element equal to 0 (see Remark 1.1). Therefore, n is not divisible by any prime p_h ($1 \leq h \leq k$), so, n is a prime. ■

Step 2. Let $\{b_1, b_2, b_3, \dots, b_k\}$ be the ordered set of the remainders of dividing x by $p_1, p_2, p_3, \dots, p_k$. Let r_h ($1 \leq h \leq k$) be the elements of the permitted k -tuple whose index is n . In the sequences of remainders modulo p_h ($1 \leq h \leq k$) that form this sequence of k -tuples, by definition, if a remainder is equal to $b_h \in \{b_1, b_2, b_3, \dots, b_k\}$, then it is a selected remainder. Consequently, by definition, for the permitted k -tuple whose index is n , we have $r_h \neq b_h$ ($1 \leq h \leq k$). This result implies $n \not\equiv x \pmod{p_h}$ for every prime p_h ($1 \leq h \leq k$) (see Remark 1.1).

Step 3. By Step 1, n is a prime; furthermore $x - n$ is not divisible by any prime $p < \sqrt{x}$, by Step 2. Since $\sqrt{x - n} < \sqrt{x}$, it follows that either $x - n = 1$ or $x - n$ is also a prime. ■

Note that, given k and an even integer x such that $p_k^2 < x < p_{k+1}^2$, there is a sequence of k -tuples associated to Sieve I that has specific selected remainders for this particular x . On the other hand, given k , there is a partial sum S_k associated to Sieve II, where there are multiple choices for selecting remainders allowed by the rules defined in Section 2. Both are sequences of k -tuples of remainders, but they differ in terms of the rules for selecting remainders. The following lemma gives the relationship between the number of permitted k -tuples within the interval $I[1, p_k^2]$ of the partial sum S_k (the sifting function of Sieve II) and the number of permitted k -tuples within the interval $I[1, x]$ of the sequence of k -tuples associated to Sieve I (the sifting function of Sieve I).

Recall that we denote by $\{T(\mathcal{B}, \mathcal{P}, p_k)\}$ the set of values of $T(\mathcal{B}, \mathcal{P}, p_k)$ for all combinations of selected remainders in the sequences that form the partial sum S_k associated to Sieve II.

Lemma 8.2. *Let \mathcal{P} be the sequence of primes. Let $x > 49$ be an even number, and let k be the index of the greatest prime less than $z = \sqrt{x}$; that is, $p_k^2 < x < p_{k+1}^2$. Consider Sieve I, Sieve II, and their associated sequences of k -tuples. We have $S(\mathcal{A}, \mathcal{P}, z) \geq \min\{T(\mathcal{B}, \mathcal{P}, p_k)\}$.*

Proof. By definition, the sequences of remainders modulo p_h ($1 < h \leq k$) that form the sequence of k -tuples associated to Sieve I can have one or two selected remainders in every period (see Remark 8.1). However, the sequences s_h ($1 < h \leq k$) that form the partial sum S_k associated to Sieve II, by definition, always have two selected remainders in every period. Suppose that we perform the following operation on the sequence of k -tuples associated to Sieve I: in each sequence of remainders modulo p_h ($1 < h \leq k$) that have only one selected remainder in every period, we choose an arbitrary second selected remainder (the same element in every period of the sequence). We obtain a partial sum S_k with a particular combination of selected remainders, where the number of permitted k -tuples within the interval $I[1, p_k^2]$ is greater than or equal to $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\}$. Clearly, in the interval $I[1, p_k^2]$ of the sequence of k -tuples associated to Sieve I before performing the operation, the number of permitted k -tuples is also greater than or equal to $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\}$. Since $I[1, p_k^2] \subset I[1, x]$, it follows that $S(\mathcal{A}, \mathcal{P}, z) \geq \min\{T(\mathcal{B}, \mathcal{P}, p_k)\}$. ■

Finally, we prove the main theorem.

Theorem 8.3. *The Main Theorem*

Let $x > 49$ be an even number, and let k be the index of the greatest prime less than $z = \sqrt{x}$. Furthermore, let K_α be the number whose existence is established in Corollary 7.2. Every even integer $x > p_k^2$ ($k > K_\alpha$) is the sum of two primes.

Remark 8.2. Assume that x is of the form $q + 1$, where q is a prime. Clearly, in the sequence of k -tuples associated to Sieve I there is a permitted k -tuple at position $n = 1$, since $1 \not\equiv 0 \pmod{p_h}$, and furthermore $x - 1 = q \implies 1 \not\equiv x \pmod{p_h}$, for every prime p_h ($1 \leq h \leq k$). (See Remark 1.1.) On the other hand, there is a permitted k -tuple at position $n = x - 1$, since $x - 1 = q \implies x - 1 \not\equiv 0 \pmod{p_h}$, and furthermore $x - 1 \not\equiv x \pmod{p_h}$, for every prime p_h ($1 \leq h \leq k$).

Proof. Step 1. Recall that $S(\mathcal{A}, \mathcal{P}, z)$ denotes the sifting function of Sieve I. Assume that $S(\mathcal{A}, \mathcal{P}, z) \geq 3$. By Remark 8.2, among the unsifted members of the set \mathcal{A} might appear 1 and $x - 1$. Therefore, we can see that there are at least $S(\mathcal{A}, \mathcal{P}, z) - 2$ integers n in \mathcal{A} such that n is a prime and $x - n$ is also a prime, by Theorem 8.1.

Step 2. By Lemma 7.3, for every level $k > K_\alpha$ we have $\min\{T(\mathcal{B}, \mathcal{P}, p_k)\} > p_k/2$. On the other hand, $S(\mathcal{A}, \mathcal{P}, z) \geq \min\{T(\mathcal{B}, \mathcal{P}, p_k)\}$ for every even number $x > 49$ such that $p_k^2 < x < p_{k+1}^2$, by Lemma 8.2. It follows that $S(\mathcal{A}, \mathcal{P}, z) > p_k/2$ for every even number $x > p_k^2$, where $k > K_\alpha$ (note that $K_\alpha > 4$ by definition). Then, by Step 1, if $x > p_k^2$ ($k > K_\alpha$), there must be at least one unsifted member $n < x$ of \mathcal{A} that is a prime such that $x - n$ is also a prime. The theorem is proved.

On the basis of the main theorem, we can assert that every even integer $x > p_k^2$, where $k > K_\alpha$, is the sum of two primes. On the other hand, the strong Goldbach conjecture has already been verified for all even numbers less than a certain bound N , whose value is updated frequently [8]. We believe that the next step towards the proof of the binary Goldbach conjecture is to obtain a suitable estimate for K_α ; if this estimate is sufficiently small, the Goldbach conjecture would be true.

Acknowledgements

The author wants to thank Dra. Patricia Quattrini (Departamento de Matemáticas, FCEyN, Universidad de Buenos Aires) for helpful conversations and Dr. Hendrik W. Lenstra (Universiteit Leiden, The Netherlands) for his extremely useful suggestions.

References

- [1] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
- [2] A. C. Cojocaru and M. Ram Murty, *An Introduction to Sieve Methods and Their Applications*, Cambridge University Press, London, 2005.
- [3] V. Brun, La série $1/5+1/7+1/11+1/13+1/17+1/19+1/29+1/31+1/41+1/43+1/59+1/61+\dots$, où les dénominateurs sont nombres premiers jumeaux est convergente où finie, *Bull. Sci. Math.*, **43**, (1919), 124–128.
- [4] V. Brun, Le crible d’Eratosthène et le théorème de Goldbach, *C. R. Acad. Sci. Paris*, **168**, (1919), 544–546.
- [5] J. R. Chen, On the representation of a large even integer as the sum of a prime and the product of at most two primes. II, *Sci. Sinica* **21** (1978), no. 4, 421–430. MR0511293 (80e:10037)
- [6] R. K. Guy, *Unsolved Problems in Number Theory*, third edition, Springer-Verlag, Berlin, 2004. MR2076335 (2005h:11003).
- [7] H. L. Montgomery and R. C. Vaughan, The exceptional set in Goldbach’s problem, *Acta Arith.* **27** (1975), 353–370. MR0374063 (51 #10263).
- [8] T. Oliveira e Silva, Goldbach conjecture verification, <http://www.ieeta.pt/~tos/goldbach.html>.
- [9] I.M. Vinogradov, The Representation of an Odd Number as the Sum of Three Primes, *Dokl. Akad. Nauk SSSR* **16** (1937), 139–142.
- [10] H. Helfgott, The ternary Goldbach conjecture is true, <http://www.arXiv.org/abs/1312.7748>.
- [11] Terence Tao, Open question: The parity problem in sieve theory, <https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/>.
- [12] A. Selberg, The general sieve method and its place in prime number theory, *Proc. Int. Congress of Mathematicians Cambridge*, MA (Providence, RI. American Mathematical Society), **1** (1950), 262–289.

Ricardo G. Barca
 Universidad Tecnológica Nacional
 Buenos Aires (Argentina)
E-mail address: rbarca@frba.utn.edu.ar