Multiplicative decomposability of shifted sets

Christian Elsholtz

September 19, 2007

Abstract

The following two problems are open:
1) Do two sets of positive integers $\mathcal{A}$ and $\mathcal{B}$ exist, with at least two elements each, such that $\mathcal{A}+\mathcal{B}$ coincides with the set of primes $\mathcal{P}$, for sufficiently large elements?
2) Let $\mathcal{A}=\{6,12,18\}$. Is there an infinite set $\mathcal{B}$ of positive integers such that $\mathcal{A}\mathcal{B}+1\subset\mathcal{P}$? A positive answer would imply that there are infinitely many Carmichael numbers with 3 prime factors.

In this paper we prove the multiplicative analogue of the first problem, namely that there are no two sets $\mathcal{A}$ and $\mathcal{B}$, with at least two elements each, such that the product $\mathcal{A}\mathcal{B}$ coincides with any additively shifted copy $\mathcal{P}+c$ of the set of primes for sufficiently large elements. We also prove that shifted copies of sets of integers which are generated by certain subsets of the primes cannot be multiplicatively decomposed.

1 Introduction

Let $\mathcal{A}$ and $\mathcal{B}$ denote sets of positive integers. Let us define a sumset by

$$\mathcal{A}+\mathcal{B}=\{a+b : a\in\mathcal{A}, b\in\mathcal{B}\}$$

and similarly a product set by

$$\mathcal{A}\mathcal{B}=\{ab : a\in\mathcal{A}, b\in\mathcal{B}\}.$$

Sumsets have been extensively studied in the literature, see for example Ostmann [15], Nathanson [14], and Tao and Vu [19]. Some of the results on sumsets can be rewritten for product sets. Often, the right multiplicative analogue of problems on $\mathcal{A}+\mathcal{B}$ is to ask about sets of the form $\mathcal{A}\mathcal{B}+1$.

Usually the interaction of sums and products leads to very difficult problems. For example one would like to know whether the set of shifted primes $p+2$ or shifted squares n^2+1 contains infinitely many primes. Also, for a finite set of integers $\mathcal{A}$ it is an open problem if at least one of the sets $\mathcal{A}+\mathcal{A}$ and $\mathcal{A}\mathcal{A}$ has at least $|\mathcal{A}|^{2-\varepsilon}$ many distinct elements, as conjectured by Erdős and Szemerédi [5].

There are also many open problems on inverse questions, e.g., whether a given set can be additively or multiplicatively decomposed.

Let us start with some definitions.

Definition 1.1 (See Ostmann [15], vol. 1, p. 1)**.** *Let $\mathcal{S}_1$ and $\mathcal{S}_2$ denote sets of positive integers. We say that $\mathcal{S}_1$ and $\mathcal{S}_2$ are* asymptotically equal*, if there exists an integer N_0 such that $\mathcal{S}_1 \cap [N_0,\infty) = \mathcal{S}_2 \cap [N_0,\infty)$.*

Definition 1.2 (See [15], vol. 1, p. 5)**.** *Let $\mathcal{S}$ be a set of positive integers. We say that $\mathcal{S}$ is* additively irreducible *if there are no two sets of positive integers $\mathcal{A}$ and $\mathcal{B}$, with at least two elements each, such that $\mathcal{A}+\mathcal{B}=\mathcal{S}$.*

Definition 1.3 (See [15], vol. 1, p. 5)**.** *Let $\mathcal{S}$ be a set of positive integers. We say that $\mathcal{S}$ is* asymptotically additively irreducible *(or we say that* no asymptotic additive decomposition exists*) if there are no two sets of positive integers $\mathcal{A}$ and $\mathcal{B}$, with at least two elements each, such that $\mathcal{A}+\mathcal{B}$ is asymptotically equal to $\mathcal{S}$.*

Ostmann stated the following

Conjecture 1.4 ([15] vol. 1, p. 13)**.** *The set of primes $\mathcal{P}$ is asymptotically additively irreducible.*

This problem has attracted considerable attention, and several authors have proved that in a conceivable asymptotic additive decomposition of $\mathcal{P}$ both summands $\mathcal{A}$ and $\mathcal{B}$ would need to be infinite, (see Hornfeck [10], Mann [12], Laffer and Mann [11]). For further partial results see for example Pomerance, Sárközy and Stewart [16], Hofmann and Wolke [9], Puchta [17] or the present author [1], [2], [3] and [4]. In particular, the author proved in [2] that the set of primes is not asymptotically additively decomposable into *three* sets $\mathcal{A},\mathcal{B},\mathcal{C}$ containing at least two elements each.

We study some examples:

Example 1.5. There are "large" sets of integers which are sumsets but still have multiplicative properties, see also [4]. Let

$$\mathcal{A} = \{n^2 : n \in \mathbb{N} \text{ and } (p \mid n \Rightarrow p \equiv 1,3,5 \bmod 8)\},$$

$$\mathcal{B} = \{n^2 : n \in \mathbb{N} \text{ and } (p \mid n \Rightarrow p \equiv 1, 5, 7 \bmod 8)\}.$$

Then the set $\mathcal{C} = \mathcal{A} + \mathcal{B}$ has the two properties:
1) the elements of $\mathcal{C}$ consist of prime factors $p \not\equiv 3 \bmod 4$ only.
2) the set $\mathcal{C}$ can be additively decomposed.

This shows that "close" to Ostmann's conjecture there are examples that behave very differently.

Moreover, the set

$$\begin{aligned} \mathcal{C}_2 &= \{x^2 + y^2 : x, y \in \mathbb{N}\} \\ &= \{n = \prod_i p_i^{\alpha_i} : p_i \text{ prime}, \alpha_i \text{ nonnegative integers}, \alpha_i \text{ even if } p_i \equiv 3 \bmod 4\} \end{aligned}$$

has the following multiplicative and additive decomposition: Let

$$\mathcal{A}_2 = \{n \in \mathbb{N} : p \mid n \Rightarrow (p = 2 \text{ or } p \equiv 1 \bmod 4)\},$$

$$\mathcal{B}_2 = \{n^2 : n \in \mathbb{N} \text{ and } (p \mid n \Rightarrow p \equiv 3 \bmod 4)\} :$$

$$\mathcal{C}_2 = \mathcal{A}_2\mathcal{B}_2 = \{n^2 : n \in \mathbb{N}\} + \{n^2 : n \in \mathbb{N}\}.$$

Example 1.6. It is not known whether there is any set $\mathcal{A}$ of at least two elements a_1, a_2 and a set $\mathcal{B}$ with infinitely many elements such that all elements of the sumset are prime simultaneously: $\mathcal{A} + \mathcal{B} \subset \mathcal{P}$. The existence of such sets would imply that there are infinitely many pairs of primes with bounded gaps. The twin prime conjecture, and more generally the k-tuple conjectures, can be written in this notation: Let $\mathcal{A} = \{0, 2\}$. Does an infinite set $\mathcal{B}$ exist such that $\mathcal{A} + \mathcal{B} \subset \mathcal{P}$?

Example 1.7. If we study the analogue multiplicative questions we should study the multiplicative structure of primes shifted by an additive constant c. It is an open problem whether for any integer c and any set $\mathcal{A}$ of at least two integers a_1, a_2 there is a set $\mathcal{B}$ containing infinitely many elements such that all elements $a_i b_j + c$ are simultaneously prime: $\mathcal{AB} + c \subset \mathcal{P}$.

Famous open problems can be written as special cases of this question as follows:

- Sophie Germain primes are primes p with the property that $2p + 1$ is also a prime. It is not known whether there exist infinitely many of these prime pairs. This can be rephrased as follows: Let $\mathcal{A} = \{1, 2\}$. Determine whether there is an infinite set $\mathcal{B}$ such that $\mathcal{AB} - 1 \subset \mathcal{P}$. Note that in this example the elements in $\mathcal{B}$ would be shifted primes $p + 1$.

- Also, it is not known whether there are infinitely many Carmichael numbers with exactly 3 prime factors. This would follow if there are infinitely many prime triples $p_1 = 6k+1, p_2 = 12k+1, p_3 = 18k+1$; then $n = p_1p_2p_3$ is a Carmichael number. This can be written in terms of product sets as follows: Let $\mathcal{A} = \{6, 12, 18\}$. It is an open problem whether there is an infinite set $\mathcal{B}$ of integers such that $\mathcal{AB} + 1 \subset \mathcal{P}$. As Granville and Pomerance show (Theorem 1 of [8]) all Carmichael numbers come from a parametric form of a suitably generalized type.

Thus, these multiplicative decomposability problems of shifted primes are closely related to encryption protocols like RSA, i.e. to important questions in cryptography. (For references to Germain primes and Carmichael numbers see Ribenboim [18]).

In this paper we solve the multiplicative analogue of Ostmann's conjecture. In plain words, we prove that there are no *two* sets $\mathcal{A}, \mathcal{B}$, with at least two elements each, such that a shifted copy of the primes $\mathcal{P}+c$ can be asymptotically multiplicatively decomposed. A precise formulation follows below after some definitions.

Definition 1.8. *Let $\mathcal{S}$ be a set of positive integers. We say that $\mathcal{S}$ is* multiplicatively irreducible *if there are no two sets of positive integers $\mathcal{A}$ and $\mathcal{B}$, with at least two elements each, such that $\mathcal{AB} = \mathcal{S}$.*

Definition 1.9. *Let $\mathcal{S}$ be a set of positive integers. We say that $\mathcal{S}$ is* asymptotically multiplicatively irreducible (or cannot be asymptotically multiplicatively decomposed) *if there are no two sets of positive integers $\mathcal{A}, \mathcal{B}$, with at least two elements each, such that $\mathcal{AB}$ is asymptotically equal to $\mathcal{S}$.*

Definition 1.10. *Let $\mathcal{S}$ be a set of positive integers. We say that $\mathcal{S}$ is* asymptotically multiplicatively translation-irreducible *if there is no decomposition of the following type: $\mathcal{S}' = \mathcal{AB} + c$, where $\mathcal{A}, \mathcal{B}$ are sets of positive integers with at least two elements each, $c \neq 0$ an integer, and where $\mathcal{S}'$ is asymptotically equal to $\mathcal{S}$.*

In this paper we prove:

Theorem 1.11. *The set of primes is asymptotically multiplicatively translation-irreducible.*

Remark 1.12. The proof shows that the same holds for any set of primes $\mathcal{P}_1 \subset \mathcal{P}$ with a counting function $\mathcal{P}_1(N) \geq f(N)\frac{N}{(\log N)^2}$, where $f(N)$ tends to infinity.

The following Theorem proves the corresponding result for sets of integers composed of certain prime factors only (i.e. for certain semigroups).

Theorem 1.13. *Let $\mathcal{T} \subset \mathcal{P}$ be a set of primes with the property that*

$$\sum_{p \leq N,\ p \in \mathcal{T}} 1 = \tau \frac{N}{\log N} + O\left(\frac{N}{(\log N)^2}\right), \tag{1}$$

for some constant $0 < \tau < 1$. Let

$$\mathcal{Q}(\mathcal{T}) = \{1\} \cup \{n \in \mathbb{N} : p \mid n \Rightarrow p \in \mathcal{T}\}.$$

Then $\mathcal{Q}(\mathcal{T})$ is asymptotically multiplicatively translation-irreducible.

Remark 1.14. Observe that Theorem 1.13 does not contain Theorem 1.11 as a special case. But even though, the proofs of both theorems are closely related which should be useful if one wants to adapt the method to other problems.

Remark 1.15. Observe that $\mathcal{Q}(\mathcal{T}) = \mathcal{Q}(\mathcal{T})\mathcal{Q}(\mathcal{T})$. So, we need $c \neq 0$ in Definition 1.10. In contrast to this, by the very definition of the primes, the set $\mathcal{P}$ is asymptotically multiplicatively irreducible, ($c = 0$).

Remark 1.16. The above choice of $\mathcal{T}$ contains important cases like $\mathcal{T}$ is the union of primes in certain arithmetic progressions.

2 Background from sieve theory

We shall use a combination of the large sieve, and of Gallagher's larger sieve. Let us state these sieves first.

Lemma 2.1 (Montgomery [13])**.** *Let $\mathcal{P}$ denote the set of primes. Let p be a prime. Let $\mathcal{A}$ denote a set of integers which avoids $\omega_{\mathcal{A}}(p)$ residue classes modulo p. Here $\omega_{\mathcal{A}} : \mathcal{P} \to \mathbb{N}$ with $0 \leq \omega(p) \leq p - 1$. Let $\mathcal{A}(N)$ denote the counting function $\mathcal{A}(N) = \sum_{a \leq N, a \in \mathcal{A}} 1$. Then the following upper bound on the counting function holds:*

$$\mathcal{A}(N) \leq \frac{N + Q^2}{L}, \text{ where } L = \sum_{q \leq Q} \mu^2(q) \prod_{p \mid q} \frac{\omega_{\mathcal{A}}(p)}{p - \omega_{\mathcal{A}}(p)}.$$

One typically chooses $Q = N^{\frac{1}{2}}$.

Vaughan has found a suitable lower bound of L if $\sum_{p \leq y} \dfrac{\omega(p)}{p}$ is known. We state a slight refinement of the original version.

Lemma 2.2 (Compare Vaughan [20])**.** *Let ε_m be positive constants with $0 < \varepsilon_m \leq e - 1$ that satisfy $m! \leq (\frac{m}{e-\varepsilon_m})^m$. For sufficiently large Q*

$$a) \qquad L \;\geq\; \sum_{m=1}^{\infty} \frac{1}{m!} \left(\sum_{p \leq Q^{\frac{1}{m}}} \frac{\omega(p)}{p} \right)^m .$$

$$b) \qquad L \;\geq\; \sum_{m=1}^{\infty} \exp\left(m \log \left(\frac{e-\varepsilon_m}{m} \sum_{p \leq Q^{\frac{1}{m}}} \frac{\omega(p)}{p} \right)\right),$$

It is always possible to have $e - \varepsilon_m = 1$. It follows from Stirling's formula that one can choose $\varepsilon_m \to 0$. The sum $\sum_{m=1}^{\infty}$ is in fact a finite sum only. The parameter m denotes the number of prime factors of q in the definition of L. Hence $1 \leq m \leq \dfrac{\log Q}{\log 2}$. There are at most $O(\log Q)$ summands. A lower bound on L can be found by choosing a suitable value of m.

Proof of Theorem 2.2. For the proof of a) see [20].

Proof of b)

With $\left(\frac{m}{e-\varepsilon_m}\right)^m \geq m!$ the following inequalities hold:

$$\begin{aligned}\sum_{m=1}^{\infty} \frac{1}{m!} \left(\sum_{p \leq Q^{\frac{1}{m}}} \frac{\omega(p)}{p} \right)^m &\geq \sum_{m=1}^{\infty} \left(\sum_{p \leq Q^{\frac{1}{m}}} \frac{(e-\varepsilon_m)\omega(p)}{mp} \right)^m \\ &= \sum_{m=1}^{\infty} \exp\left(m \log \left(\frac{e-\varepsilon_m}{m} \sum_{p \leq Q^{\frac{1}{m}}} \frac{\omega(p)}{p} \right)\right).\end{aligned}$$

□

Lemma 2.3 (Gallagher's larger sieve, [6])**.** *Let $\mathcal{S}$ denote a set of primes such that $\mathcal{B}$ lies modulo p (for $p \in \mathcal{S}$) in at most $\nu_{\mathcal{B}}(p)$ residue classes. Then the following bound holds, provided the denominator is positive:*

$$\mathcal{B}(N) \leq \frac{-\log N + \sum_{p \in \mathcal{S}} \log p}{-\log N + \sum_{p \in \mathcal{S}} \dfrac{\log p}{\nu_{\mathcal{B}}(p)}}.$$

3 Proof of Theorem 1.11

Proposition 3.1. *Let $\mathcal{A}, \mathcal{B}$ be sets of positive integers with at least two elements each. Suppose that $\mathcal{P}' = \mathcal{A}\mathcal{B} + c$, where $\mathcal{P}' \cap [N_0, \infty) = \mathcal{P} \cap [N_0, \infty)$. Then for arbitrary $\varepsilon > 0$:*

$$N^{\frac{1}{2}-\varepsilon} \ll_\varepsilon \mathcal{A}(N) \ll_\varepsilon N^{\frac{1}{2}+\varepsilon}.$$

The same holds for $\mathcal{B}(N)$.

Proof. Suppose that $\mathcal{P}' = \mathcal{A}\mathcal{B} + c$, where $\mathcal{P}' \cap [N_0, \infty) = \mathcal{P} \cap [N_0, \infty)$. Let $b_1 < b_2$ be the least two elements of $\mathcal{B}$. Without loss of generality we may assume that $N_0 > \max(b_2, c)$; otherwise, we just increase N_0. Let $N > N_0^3$ be a large integer. We begin by showing that for any prime $q \in [N_0, N^{1/2}]$ the set $\mathcal{A}_1 = \mathcal{A} \cap [N^{1/2}, N]$ avoids at least two residue classes modulo q. If $a \in \mathcal{A}_1$, then $ab_1 + c = p$ is a prime with $b_1 < N_0 < q < N^{1/2} < p$. Now $b_1 \not\equiv 0 \bmod q$, so $b_1^{-1} \bmod q$ exists and $a \not\equiv -b_1^{-1}c \bmod q$. Similarly $a \not\equiv -b_2^{-1}c \bmod q$. It follows that $a \in \mathcal{A}_1$ avoids the two residue classes $-b_1^{-1}c$ and $-b_2^{-1}c$ modulo q. These are distinct since $0 < b_1 < b_2 < q$ and $0 < c < q$.

Lemma 2.1 applied with $\omega(q) = 2$ gives the upper bound $\mathcal{A}_1(N) \ll \frac{N}{(\log N)^2}$, so $\mathcal{A}(N) \leq \sqrt{N} + \mathcal{A}_1(N) \ll \frac{N}{(\log N)^2}$. Because $\mathcal{P}(N) \gg \frac{N}{\log N}$ we must have $\mathcal{B}(N) \gg \log N$. This trivially implies that $\mathcal{B}(N) \to \infty$, as $N \to \infty$. Observe that this argument (and those below) also holds for a subset $\mathcal{P}_1$ of the primes, if $\mathcal{P}_1(N) \geq \frac{N}{(\log N)^2} f(N)$ where $f(N) \to \infty$ as $N \to \infty$.

Let $b_1 < b_2 < \ldots < b_k$ be the first k elements of $\mathcal{B}$. We adapt the argument above with the change that $N_0 > b_k$. A sieve with $\omega(q) = k$, for $q \in [N_0, N^{\frac{1}{2}}]$ implies that $\mathcal{A}(N) \ll_k \frac{N}{(\log N)^k}$ and therefore $\mathcal{B}(N) \gg_k (\log N)^{k-1}$. This holds for all k, so we have $\mathcal{B}(N) \geq c_k (\log N)^k$.

To iterate this further we need a lower bound on $\omega(q)$ on average. Since a residue class $b \mod q$ forbids a class $a \bmod q$ for $\mathcal{A}$ we actually count those classes modulo primes that occur in $\mathcal{B}$.

Let $\nu_{\mathcal{B}}(p) = |\mathcal{B} \mod p|$; i.e., $\nu_{\mathcal{B}}(p)$ is the number of residue classes modulo p that contain at least one element of $\mathcal{B}$.

Let

$$y = c_k (\log N)^{k+1} \tag{2}$$

and $\mathcal{S} = \{p : N_0 < p \leq y\}$. If $\sum_{p \in \mathcal{S}} \frac{\log p}{\nu_{\mathcal{B}}(p)} > 3 \log N$, then we apply Gallagher's larger sieve. Using (2) and Chebyshev's bound $\sum_{p \leq y} \log p < 2y$ we obtain a contradiction:

$$c_k (\log N)^k \leq \mathcal{B}(N) \leq \frac{-\log N + \sum_{p \in \mathcal{S}} \log p}{-\log N + \sum_{p \in \mathcal{S}} \frac{\log p}{\nu_{\mathcal{B}}(p)}} < \frac{2y}{-\log N + \sum_{p \in \mathcal{S}} \frac{\log p}{\nu_{\mathcal{B}}(p)}} < c_k (\log N)^k.$$

Consequently

$$\sum_{p\in\mathcal{S}} \frac{\log p}{\nu_{\mathcal{B}}(p)} \leq 3\log N.$$

From the Cauchy-Schwarz inequality and by partial summation from Chebyshev's inequality $\pi(y) \gg \frac{y}{\log y}$ we find that:

$$\left(\sum_{N_0<p\leq y} \frac{\log p}{\nu_{\mathcal{B}}(p)}\right)\left(\sum_{N_0<p\leq y} \frac{\nu_{\mathcal{B}}(p)}{p}\right) \geq \left(\sum_{p\leq y}\left(\frac{\log p}{p}\right)^{1/2}\right)^2 \gg \frac{y}{\log y}. \tag{3}$$

We combine these two inequalities to obtain

$$\sum_{p\in\mathcal{S}} \frac{\nu_{\mathcal{B}}(p)}{p} \gg \frac{y}{(\log y)(3\log N)} \gg \frac{(\log N)^k}{\log\log N}.$$

It then follows by Montgomery's large sieve and by Vaughan's Lemma 2.2 that $\mathcal{A}_1(N) \leq \frac{2N}{L}$, where

$$\begin{aligned} L &= \sum_{q\leq N^{1/2}} \mu^2(q)\prod_{p|q}\frac{\omega_{\mathcal{A}}(p)}{p-\omega_{\mathcal{A}}(p)} \\ &\geq \max_{m\in\mathbb{N}} \exp\left(m\log\left(\frac{1}{m}\sum_{p\leq N^{1/(2m)}}\frac{\omega_{\mathcal{A}}(p)}{p}\right)\right). \end{aligned}$$

We choose the integer m such that $N^{1/(2m)}$ is close to y. Hence

$$m = \frac{1}{2(k+1)}\frac{\log N}{\log\log N} + O(1).$$

We may choose

$$\omega_{\mathcal{A}}(p) = \begin{cases} \nu_{\mathcal{B}}(p) & \text{for } p\in\mathcal{S} \\ 0 & \text{otherwise.}\end{cases}$$

Therefore we find that for all $\varepsilon' > 0$:

$$\begin{aligned} \log L &\geq \frac{\log N}{2(k+1)\log\log N}\log\left(\frac{2(k+1)\log\log N}{\log N}\frac{c(\log N)^k}{\log\log N}\right) + O(1) \\ &\geq \left(\frac{1}{2} - \frac{1}{k+1} - \varepsilon'\right)\log N. \end{aligned}$$

So, for any given $\varepsilon > 0$, we choose $\varepsilon' = \frac{\varepsilon}{2}$, and so, for sufficiently large k, we find that

$$\mathcal{A}(N) \leq \mathcal{A}_1(N) + N^{\frac{1}{2}} \leq \frac{2N}{L} + N^{\frac{1}{2}} \ll_{\varepsilon} N^{\frac{1}{2}+\frac{1}{k+1}+\varepsilon'} \ll_{\varepsilon} N^{\frac{1}{2}+\frac{3}{4}\varepsilon}.$$

The same upper bound holds for $\mathcal{B}(N)$, by symmetry. The lower bound $\mathcal{A}(N) \gg N^{\frac{1}{2}-\varepsilon}$, for all $\varepsilon > 0$, follows since $\mathcal{A}(N)\mathcal{B}(N) \gg \pi(N) \gg \frac{N}{\log N}$ must hold. So, the proposition follows. □

Proof of Theorem 1.11. If $ab + c = p \leq N$, then at least one of $a \ll \sqrt{N}$ or $b \ll \sqrt{N}$ must hold. Since all $\pi(N) + O(1) \gg \frac{N}{\log N}$ primes in $[N_0, N]$ have at least one presentation as $ab + c$, we not only have $\mathcal{A}(N)\mathcal{B}(N) \gg \frac{N}{\log N}$ but also

$$\mathcal{A}(N)\mathcal{B}(\sqrt{N}) + \mathcal{A}(\sqrt{N})\mathcal{B}(N) \gg \frac{N}{\log N}.$$

Applying our proposition, once with $N_1 = \sqrt{N}$, a second time with $N_2 = N$ gives

$$\mathcal{A}(N)\mathcal{B}(\sqrt{N}) + \mathcal{A}(\sqrt{N})\mathcal{B}(N) \ll N^{\frac{3}{4}+\varepsilon},$$

which proves the theorem. □

4 Proof of Theorem 1.13

This proof follows along the same lines.

Let us state some consequences of the density condition of $\mathcal{T}$.

Lemma 4.1.

$$\sum_{p \leq y, p \notin \mathcal{T}} \frac{1}{p} = (1 - \tau) \log\log y + C + o(1).$$

Proof. This follows by partial summation from the density assumption in equation (1). Actually, a somewhat weaker density assumption would suffice. □

Lemma 4.2.

$$\sum_{p \leq y, p \notin \mathcal{T}} \left(\frac{\log p}{p}\right)^{\frac{1}{2}} \gg_\tau \frac{y^{\frac{1}{2}}}{(\log y)^{\frac{1}{2}}}.$$

This follows again by partial summation. The following argument may be easier: Let p_n denotes the n-th prime which is not in $\mathcal{T}$. Equation (1) implies that $p_n \sim \frac{1}{1-\tau} n \log n$. Then

$$\begin{aligned} \textstyle\sum_{p \leq y, p \notin \mathcal{T}} \left(\frac{\log p}{p}\right)^{\frac{1}{2}} &\sim \textstyle\sum_{n \leq \frac{(1-\tau+o(1))y}{\log y}} \left(\frac{(1-\tau)(\log n + \log\log n + O(1))}{n \log n}\right)^{\frac{1}{2}} \\ &\gg_\tau \textstyle\sum_{n \leq \frac{(1-\tau+o(1))y}{\log y}} \frac{1}{n^{\frac{1}{2}}} \gg_\tau \frac{y^{\frac{1}{2}}}{(\log y)^{\frac{1}{2}}}. \end{aligned}$$

Lemma 4.3.

$$\mathcal{Q}(\mathcal{T})(N) \sim C_\tau \frac{N}{(\log N)^{1-\tau}}.$$

$$\mathcal{Q}(\mathcal{P}\backslash\mathcal{T})(N) \sim C_{1-\tau} \frac{N}{(\log N)^{\tau}}.$$

This follows from the following result.

Lemma 4.4 (Wirsing, [21]). *Let $\mathcal{T}$ denote a set of primes and $0 < \tau \leq 1$. If*

$$\sum_{\substack{p \leq x \\ p \in \mathcal{T}}} \frac{1}{p} = \tau \log\log x + C + o(1),$$

then

$$|\{n \leq N, p \mid n \Rightarrow p \in \mathcal{T}\}| \sim C_{\mathcal{T}} \frac{N}{(\log N)^{1-\tau}}.$$

Proposition 4.5. *Suppose that $\mathcal{Q}(\mathcal{T})' = \mathcal{AB} + c$, where $\min(|\mathcal{A}|, |\mathcal{B}|) \geq 2$, $\mathcal{Q}(\mathcal{T})' \cap [N_0, \infty) = \mathcal{Q}(\mathcal{T}) \cap [N_0, \infty)$. Then for arbitrary $\varepsilon > 0$:*

$$N^{\frac{1}{2}-\varepsilon} \ll_\varepsilon \mathcal{A}(N) \ll_\varepsilon N^{\frac{1}{2}+\varepsilon}.$$

The same holds for $\mathcal{B}(N)$.

Proof. Suppose for a contradiction that $\mathcal{Q}(\mathcal{T})' = \mathcal{AB} + c$, where $\mathcal{Q}(\mathcal{T})' \cap [N_0, \infty) = \mathcal{Q}(\mathcal{T}) \cap [N_0, \infty)$. Let $b_1 < b_2$ be the two smallest elements of $\mathcal{B}$, and without loss of generality we can assume that $N_0 > \max(b_2, c)$; (otherwise just increase N_0). Observe that $ab + c \not\equiv 0 \bmod q$ for primes $q \notin \mathcal{T}$. A class $b \bmod q$ that occurs in $\mathcal{B}$ induces a forbidden class $-c\, b^{-1} \bmod q$ for $\mathcal{A}$: let $N > N_0^3$ be any large integer. Let $\overline{\mathcal{T}} = \mathcal{P}\backslash\mathcal{T}$. Let $q \in \overline{\mathcal{T}}$ be a prime in $[N_0, N^{1/2}]$. Let $\mathcal{A}_1 = \mathcal{A} \cap [N^{1/2}, N]$, and let $a \in \mathcal{A}_1$. Let $N > ab + c = p > N^{1/2} > q > N_0$. Since $b_1 < b_2 < q$ it is clear that $b_1^{-1} \bmod q$ and $b_2^{-1} \bmod q$ exist and are distinct. Also recall that $c \neq 0$ and $q > c$. Therefore the set $\mathcal{A}_1$ avoids modulo all primes $q \in [N_0, N^{1/2}]$ at least two distinct residue classes. An application of Vaughan's lemma 2.2 applied with

$$\omega(q) = \begin{cases} 2 & \text{if } q \in \overline{\mathcal{T}} \cap [N_0, N^{\frac{1}{2}}] \\ 0 & \text{otherwise.} \end{cases}$$

gives an upper bound of

$$\mathcal{A}_1(N) \ll \frac{N}{\max_m \left(\exp\left(m \log\left(\frac{e-\varepsilon_m}{m} \sum_{p \leq N^{1/(2m)}} \frac{\omega(p)}{p}\right)\right)\right)}.$$

Choosing $m = \lfloor 2(1-\tau)\log\log N \rfloor$ gives

$$\begin{aligned} \mathcal{A}_1(N) &\ll \frac{N}{\exp\left(m \log \frac{2e(1-\varepsilon)(1-\tau)(\log\log N - \log(2m))}{2(1-\tau)\log\log N}\right)} \\ &\ll \frac{N}{(\log N)^{2(1-\tau)(1-2\varepsilon)}}, \end{aligned}$$

which implies $\mathcal{A}(N) \leq \sqrt{N} + \mathcal{A}_1(N) \ll \frac{N}{(\log N)^{2(1-\tau)(1-2\varepsilon)}}$. Since

$$\mathcal{Q}(\mathcal{T})(N) \gg \frac{N}{(\log N)^{1-\tau}}$$

one necessarily has $\mathcal{B}(N) \geq k$, for each fixed k. Let $b_1 < b_2 < \ldots < b_k$ be the first k elements of $\mathcal{B}$. We iterate this procedure. Let $N_0 > b_k$. An application of Vaughan's lemma applied with

$$\omega(q) = \begin{cases} k & \text{if } q \in \overline{\mathcal{T}} \cap [N_0, N^{\frac{1}{2}}] \\ 0 & \text{otherwise.} \end{cases}$$

and $m = \lfloor k(1-\tau)\log\log N \rfloor$ gives an upper bound of $\mathcal{A}(N) \ll \frac{N}{(\log N)^{k(1-\tau)(1-\varepsilon')}}$. Since this holds for all k we also have $\mathcal{B}(N) \geq c_k (\log N)^k$. Let $\overline{\mathcal{T}}(y) = \{p \in \overline{\mathcal{T}}, p \leq y\}$. By Lemma 4.2 above we find that:

$$\left(\sum_{p \in \overline{\mathcal{T}}(y)} \frac{\log p}{\nu_{\mathcal{B}}(p)}\right) \left(\sum_{p \in \overline{\mathcal{T}}(y)} \frac{\nu_{\mathcal{B}}(p)}{p}\right) \geq \left(\sum_{p \in \overline{\mathcal{T}}(y)} \left(\frac{\log p}{p}\right)^{1/2}\right)^2 \gg_\tau \frac{y}{\log y}.$$

Choose $y = c_k (\log N)^{k+1}$. Let us assume that

$$\sum_{p \in \overline{\mathcal{T}}(y)} \frac{\log p}{\nu_{\mathcal{B}}(p)} > 3 \log N.$$

Then we arrive at a contradiction, by Gallagher's larger sieve:

$$\mathcal{B}(N) \leq \frac{-\log N + \sum_{p \in \overline{\mathcal{T}}(y)} \log p}{-\log N + \sum_{p \in \overline{\mathcal{T}}(y)} \frac{\log p}{\nu_{\mathcal{B}}(p)}} < \frac{y}{2\log N} < c_k (\log N)^k.$$

Therefore we have that

$$\sum_{p \in \overline{\mathcal{T}}(y)} \frac{\log p}{\nu_{\mathcal{B}}(p)} \leq 3 \log N$$

which implies that

$$\sum_{p \in \overline{\mathcal{T}}(y)} \frac{\nu_{\mathcal{B}}(p)}{p} \gg \frac{y}{(\log y)(3 \log N)} \gg \frac{(\log N)^k}{\log\log N}.$$

We apply again Montgomery's large sieve and Vaughan's Lemma . We choose the integer m such that $N^{1/(2m)}$ is close to y. Hence $m = \frac{1}{2(k+1)} \frac{\log N}{\log\log N} + O(1)$. We may choose $\omega_{\mathcal{A}}(p) = \begin{cases} \nu_{\mathcal{B}}(p) & \text{for } p \in \overline{\mathcal{T}}(y) \\ 0 & \text{otherwise.} \end{cases}$

Therefore we find that

$$\begin{aligned} \log L &\geq \frac{\log N}{2(k+1)\log\log N} \log\left(\frac{2(k+1)\log\log N}{\log N}\frac{c(\log N)^k}{\log\log N}\right) + O(1) \\ &\geq \left(\frac{1}{2} - \frac{1}{k+1} - \varepsilon'\right)\log N. \end{aligned}$$

And so we have that $\mathcal{A}(N) \leq \frac{2N}{L} + N^{\frac{1}{2}} \ll N^{\frac{1}{2}+\frac{1}{k+1}+\varepsilon'} \ll N^{\frac{1}{2}+\frac{3}{4}\varepsilon}$. The upper bound on $\mathcal{B}(N)$ is the same, by symmetry. The lower bounds follow again from $\mathcal{A}(N)\mathcal{B}(N) \gg \frac{N}{(\log N)^{1-\tau}}$, which completes the proof of the Proposition. □

The proof of Theorem 1.13 is as before. Assuming a decomposition $\mathcal{Q}(\mathcal{T})' = \mathcal{A}\mathcal{B} + c$ exists, then for some constant c'

$$\frac{N}{(\log N)^{1-\tau}} \ll \mathcal{Q}(\mathcal{T})(N) \ll \mathcal{A}(N)\mathcal{B}(c'\sqrt{N}) + \mathcal{A}(c'\sqrt{N})\mathcal{B}(N) \ll N^{\frac{3}{4}+\varepsilon},$$

which is a contradiction.

Remark 4.6. An alternative proof of Theorem 1.11 is as follows: By a theorem of Goldfeld [7] it is known that for $\gg \frac{N}{(\log N)}$ of the primes $p \leq N$ the largest prime factor of $p+c$ satisfies $P(p+c) \gg p^{0.5}$. This means that a multiplicative decomposition of $\mathcal{P} + c$ would need $\gg \frac{N}{\log N}$ large elements in $\mathcal{A}$ or $\mathcal{B}$, which is impossible by relatively simple sieve bounds. In order to prove Theorem 1.13 one would need to prove suitable results on the largest prime factor of sequences like $\mathcal{Q}(\mathcal{T}) + c$ first. This approach would not seem to be any simpler than the one chosen in this paper.

This paper was written while the author was enjoying a research stay at the Mathematical Institute of the Hungarian Academy of Sciences. The author was supported by the Finite Structures project, in the framework of the European Community's "Structuring the European Research Area" programme. The author is also grateful to the referee for a careful reading of the manuscript.

References

[1] C. Elsholtz, *A Remark on Hofmann and Wolke's Additive Decompositions of the Set of Prime*, Arch. Math. **76** (2001), 30-33.

[2] C. Elsholtz, *The Inverse Goldbach Problem*, Mathematika **48** (2001), 151-158.

[3] C. Elsholtz, *Some remarks on the additive structure of the set of primes*, Number theory for the millennium, I (Urbana, IL, 2000), 419–427, (Proceedings of the Millennial Conference on Number Theory (Bennett et.al.), AK Peters, 2002).

[4] C. Elsholtz, *Additive decomposability of multiplicatively defined sets.* Funct. Approx. Comment. Math. **35** (2006), 61–77.

[5] P. Erdős, E. Szemerédi, *On sums and products of integers*, Studies in pure mathematics, Mem. of P. Turan, 213-218 (1983).

[6] P.X. Gallagher, *A Larger Sieve*, Acta Arith. **18** (1971), 77-81.

[7] M. Goldfeld, *On the number of primes p for which $p + a$ has a large prime factor*, Mathematika **16** (1969), 23- 27.

[8] A. Granville, C. Pomerance, *Two contradictory conjectures concerning Carmichael numbers*, Math. Comp. **71** (2002), 883-908.

[9] A. Hofmann, D. Wolke, *On Additive Decompositions of the Set of Primes*, Arch. Math. **67** (1996), 379-382.

[10] B. Hornfeck, *Ein Satz über die Primzahlmenge*, Math. Z. **60** (1954), 271–273, see also the Zentralblatt review by Erdős and the correction in Math. Z. 62, (1955), page 502.

[11] W.B. Laffer, H.B. Mann, *Decomposition of sets of group elements*, Pacific J. Math. **14** (1964) 547–558.

[12] H.B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Wiley Interscience, New York-London-Sydney, 1965.

[13] H. Montgomery, *The Analytic Principle of the Large Sieve*, Bull. Amer. Math Soc. **84** (1978), 547-567.

[14] M. Nathanson, *Additive Number Theory, Inverse problems and the geometry of sumsets.* Graduate Texts in Mathematics, 165. Springer-Verlag, New York, 1996.

[15] H.-H. Ostmann, *Additive Zahlentheorie*, 2 volumes, Springer-Verlag, Berlin-Heidelberg-New York, 1956, reprint 1968.

[16] C. Pomerance, C.L. Stewart, A. Sárközy, *On Divisors of Sums of Integers, III*, Pacific J. Math. **133** (1988), 363-379.

[17] J.-P. Puchta, *On additive decompositions of the set of primes.* Arch. Math. **78** (2002), 24–25.

[18] P. Ribenboim, *The new book of prime number records*, 3rd edition, Springer-Verlag, New York, 1995.

[19] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.

[20] R.C. Vaughan, *Some Applications of Montgomery's Sieve*, J. Number Theory **5** (1973), 64-79.

[21] E. Wirsing, *Über die Zahlen, deren Primteiler einer gegebenen Menge angehören.* Arch. Math. **7**, 263–272, 1956.

Christian Elsholtz
Department of Mathematics
Royal Holloway
Egham
Surrey TW20 0EX
UK
christian.elsholtz@rhul.ac.uk

2000 Mathematics Subject Classification:
Primary:11N25, 11N36