THE MAXIMAL DENSITY OF PRODUCT-FREE SETS IN $\mathbb{Z}/n\mathbb{Z}$

PÄR KURLBERG, JEFFREY C. LAGARIAS, AND CARL POMERANCE

ABSTRACT. This paper studies the maximal size of product-free sets in $\mathbb{Z}/n\mathbb{Z}$. These are sets of residues for which there is no solution to $ab \equiv c \pmod{n}$ with a, b, c in the set. In a previous paper we constructed an infinite sequence of integers $(n_i)_{i\geq 1}$ and product-free sets $\mathcal{S}_i$ in $\mathbb{Z}/n_i\mathbb{Z}$ such that the density $|\mathcal{S}_i|/n_i \to 1$ as $i \to \infty$, where $|\mathcal{S}_i|$ denotes the cardinality of $\mathcal{S}_i$. Here we obtain matching, up to constants, upper and lower bounds on the maximal attainable density as $n \to \infty$.

1. INTRODUCTION

An important problem in combinatorial number theory is the study of sets of integers with additive restrictions. For example, a sum-free set $\mathcal{S}$ is one forbidding solutions to $a + b = c$ with $a, b, c \in \mathcal{S}$, and the condition of requiring no solutions to $a + c = 2b$ gives sets $\mathcal{S}$ containing no three-term arithmetic progression. For sum-free sets it is easy to show that such sets have upper density at most $\frac{1}{2}$, and the same holds for subsets of $\mathbb{Z}/n\mathbb{Z}$, and more generally for finite abelian groups. In fact, by the work of Green and Ruzsa [3] (building on partial results by Diananda and Yap [1]), the density attainable for any finite abelian group is known.

Similarly, it is also natural to consider sets with multiplicative restrictions. For example, Behrend, Besicovitch, Erdős and others (see Hall [5]) considered sets of integers with no member properly dividing another (known as *primitive* sets), and Erdős [2] considered sets where no member divides the product of two other members.

Here we consider a multiplicative version of the sum-free problem. We say a set of integers $\mathcal{S}$ is *product-free* if whenever $a, b, c \in \mathcal{S}$ we have $ab \neq c$. Similarly, if $\mathcal{S} \subset \mathbb{Z}/n\mathbb{Z}$, we say $\mathcal{S}$ is product-free if $ab \not\equiv c \pmod{n}$, whenever $a, b, c \in \mathcal{S}$. Clearly, if $\mathcal{S}$ is a product-free subset of $\mathbb{Z}/n\mathbb{Z}$, then the set of integers congruent modulo n to some member of $\mathcal{S}$ is a product-free set of integers. For a product-free subset $\mathcal{S}$ of $\mathbb{Z}/n\mathbb{Z}$, let $D(\mathcal{S}) = |\mathcal{S}|/n$, where $|\mathcal{S}|$ denotes the cardinality of $\mathcal{S}$. Further, let $D(n)$ denote the maximum of $D(\mathcal{S})$ over all product-free sets $\mathcal{S} \subset \mathbb{Z}/n\mathbb{Z}$.

The problem of product-free sets in $\mathbb{Z}/n\mathbb{Z}$ was studied in a recent paper by the third author and Schinzel [9]. One might initially think that this product-free problem has a similar answer to the sum-free case, where the density can never exceed $\frac{1}{2}$. In this direction, it was shown in [9] that $D(n) < \frac{1}{2}$ holds for the vast majority of numbers n; specifically for all n except possibly those divisible by some m^2 where m is the product of 6 distinct primes, and consequently the possible exceptional set has upper density smaller than 1.56×10^{-8}. However, somewhat surprisingly, there are numbers n for which $D(n)$ is arbitrarily close to 1; in [7] it was shown that there are infinitely many n such that

$$D(n) > 1 - \frac{C}{(\log\log n)^{1-\frac{1}{2}\mathrm{e}\log 2}} \tag{1.1}$$

Date: January 10, 2012.

2000 *Mathematics Subject Classification.* 11B05, 11B75.

for a suitable positive constant C. Here the exponent $1 - \frac{1}{2}\mathrm{e}\log 2 \approx 0.057915$. Some key features of the sets $\mathcal{S}$ of high density so constructed are that n is highly composite, divisible by the square of each of its prime factors, and each member of such a set has a large common divisor with n.

Our aim in this paper is to get an exact form for the rate at which $D(n)$ can approach 1. We begin with an upper bound that closely matches the lower bound (1.1).

Theorem 1.1. *There is a positive constant c such that for all $n \geq 20$,*

$$D(n) < 1 - \frac{c}{(\log\log n)^{1-\frac{1}{2}\mathrm{e}\log 2}\sqrt{\log\log\log n}}.$$

The restriction to $n \geq 20$ is made here so that the triple logarithm is defined and positive. Our second result is an improvement of the lower bound (1.1) which shows that, up to constants, Theorem 1.1 is sharp.

Theorem 1.2. *There is a positive constant C and infinitely many integers n with*

$$D(n) > 1 - \frac{C}{(\log\log n)^{1-\frac{1}{2}\mathrm{e}\log 2}\sqrt{\log\log\log n}}.$$

Before proceeding, we give a brief outline of the proof of our principal result, Theorem 1.1. To bound the maximum density from above, we introduce certain linear programming (LP) problems (P_n). The variables of (P_n) are $\{\alpha_u\}$ with u ranging over the divisors of n exceeding 1, with objective function $\sum \alpha_u/u$. Given a product-free set $\mathcal{S}$, the values

$$\alpha_u = |\{a \in \mathcal{S} : (a,n) = u\}|/|\{a \pmod n : (a,n) = u\}|,$$

for $u > 1$ give a feasible solution to (P_n). There is a mismatch between the objective function and $D(\mathcal{S})$, and to get around this we associate to each n a larger auxiliary number $N = N(n)$ which n divides (so that $D(n) \leq D(N)$), such that the optimal solution value of the linear program (P_N) can be used to give an upper bound on $D(N)$ (Theorem 4.1). To bound the new optimal solution value, we switch to the dual linear program (D_N), for which each feasible solution gives an upper bound on the optimal value of (P_N). A mechanism for finding a good feasible solution to the dual LP is the heart of the proof given in Section 5.

There remains the problem of obtaining tight optimal constants in these theorems. With some effort, numerical values for c and C in Theorems 1.1 and 1.2 are computable. However the linear program used to prove Theorem 1.1 relaxes the conditions of the problem and loses some information, and it is perhaps unlikely that the constants c and C so obtained will asymptotically match.

The proof of Theorem 1.1 is given in Sections 2-5. In Section 6, we prove Theorem 1.2 by refining the method of [7].

Notation. For n a positive integer, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ denotes Euler's function at n, $\omega(n)$ denotes the number of distinct prime factors of n, $\Omega(n)$ denotes the total number of prime factors of n counted with multiplicity, $\sigma(n)$ denotes the sum of the positive divisors of n, and $\mathrm{rad}(n)$ denotes the largest squarefree divisor of n. We write $d \| n$ if $d \mid n$ and $\gcd(d, n/d) = 1$. We use the notation $A(x) \ll B(x)$ if $A(x) = O(B(x))$. This relation is uniform in other variables unless indicated by a subscript. We write $A(x) \asymp B(x)$ if $A(x) \ll B(x) \ll A(x)$. Finally, we always use the letter p to denote a prime variable.

2. Preliminaries: Properties of the Density Function

As noted in [7], we have the following simple result.

Lemma 2.1. *For all integers $m, n \geq 1$,*

$$D(n) \leq D(mn). \tag{2.1}$$

Proof. Given a product-free set $\mathcal{S} \pmod{n}$, the set $\tilde{\mathcal{S}} := \mathcal{S} + \{0, n, 2n, ..., (m-1)n\} \subset \mathbb{Z}/mn\mathbb{Z}$ has $|\tilde{\mathcal{S}}| = m|\tilde{\mathcal{S}}|$. Now $\tilde{\mathcal{S}}$ is product-free $\pmod{mn}$ since any product of elements in $\tilde{\mathcal{S}}$ falls in a congruence class $\pmod{n}$ that is not in $\mathcal{S}$. □

For a positive integer n and a divisor u of n, we let

$$\mathcal{T}_u := \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = u\}.$$

Clearly

$$|\mathcal{T}_u| = \varphi\left(\frac{n}{u}\right). \tag{2.2}$$

Given some subset $\mathcal{S}$ of $\mathbb{Z}/n\mathbb{Z}$, we let

$$\mathcal{S}_u := \{a \in \mathcal{S} : \gcd(a, n) = u\} = \mathcal{S} \cap \mathcal{T}_u.$$

It is natural to measure the size of $\mathcal{S}_u$ with respect to $\mathcal{T}_u$.

The following result is implicit in [9]; since it is central to our argument, we give complete details.

Lemma 2.2. *For any product-free set $\mathcal{S} \pmod{n}$ and $u \mid n$, let*

$$\alpha_u = \alpha_u(\mathcal{S}) := \frac{|\mathcal{S}_u|}{|\mathcal{T}_u|} = \frac{|\mathcal{S}_u|}{\varphi(n/u)}.$$

Then, for all $v \mid n$ such that $uv \mid n$, we have

$$0 \leq \alpha_u \leq 1 \tag{2.3}$$

and

$$\alpha_u + \alpha_v + \alpha_{uv} \leq 2 \tag{2.4}$$

Proof. Here (2.3) is immediate, holding in fact for any set $\mathcal{S} \subset \mathbb{Z}/n\mathbb{Z}$, whether or not it is product-free. If $\alpha_u = 0$, then (2.4) immediately follows from (2.3) applied to v and uv, so we may assume that $\alpha_u > 0$. Let $a \in \mathcal{S}_u$. In the ring $\mathbb{Z}/n\mathbb{Z}$, multiplication by a takes $\mathcal{T}_v$ onto $\mathcal{T}_{uv}$, where each member of $\mathcal{T}_{uv}$ has the same size pre-image in $\mathcal{T}_v$, namely $|\mathcal{T}_v|/|\mathcal{T}_{uv}| = \varphi(n/v)/\varphi(n/uv) = k$, say. Since $\mathcal{S}$ is product-free, each $b \in \mathcal{S}_{uv}$ is thus associated with k members of $\mathcal{T}_v$ that cannot lie in $\mathcal{S}_v$. Thus, $k|\mathcal{S}_{uv}| + |\mathcal{S}_v| \leq |\mathcal{T}_v| = \varphi(n/v)$. Dividing this inequality by $\varphi(n/v)$ and using the definition of k gives

$$\frac{|\mathcal{S}_{uv}|}{\varphi(n/uv)} + \frac{|\mathcal{S}_v|}{\varphi(n/v)} \leq 1,$$

which with (2.3) proves (2.4). □

Finally we recall (from [9]) a fact about product-free sets $\mathcal{S}$.

Lemma 2.3. *Given n, if $\mathcal{S}$ is product-free $\pmod{n}$ and $a \in \mathcal{S}$ has $\gcd(a, n) = 1$, then*

$$D(\mathcal{S}) < \frac{1}{2}.$$

Thus, if $D(\mathcal{S}) \geq \frac{1}{2}$ then $\alpha_1(\mathcal{S}) = 0$.

Proof. We may assume $0 \notin \mathcal{S}$. Suppose $a \in \mathcal{S}$ with $\gcd(a, n) = 1$. By the product-free property we have $a\mathcal{S} \cap \mathcal{S} = \emptyset$. Now the gcd condition gives $|a\mathcal{S}| = |\mathcal{S}|$, whence $|\mathcal{S}| + |a\mathcal{S}| = 2|\mathcal{S}| \leq n - 1$ gives the result. □

This simple result already yields an upper bound for $D(n)$: one has, for all $n \geq 8$,

$$D(n) \leq 1 - \frac{1}{3 \log \log n}. \tag{2.5}$$

To see this, if $\mathcal{S}$ is product-free (mod n) and $D(\mathcal{S}) \geq \frac{1}{2}$, then the lemma shows that the set contains no a with $(a, n) = 1$, whence $D(\mathcal{S}) \leq 1 - \varphi(n)/n$. The upper bound (2.5) then follows from estimates of Rosser and Schoenfeld [10, Theorem 15] valid for all $n \geq \mathrm{e}^{\mathrm{e}^2}$. For n with $8 \leq n \leq \mathrm{e}^{\mathrm{e}^2}$, we have from [9] that $D(n) < \frac{1}{2}$, which is stronger than (2.5). However, establishing the upper bound of Theorem 1.1 is more delicate.

3. Linear Programs and Linear Programming Duality

In this section, for each fixed positive integer n, we formulate a linear program (P_n), along with its associated dual linear program (D_n) which encodes product-free conditions given in Section 2; related linear programs were already suggested in [9, Question 3] as an approach to upper bounds. We term (P_n) a primal linear program and (D_n) its dual linear program, because (P_n) is given in a standard inequality form called in the literature *primal form* (alternatively, *canonical form*), and (D_n) takes the standard dual form as given in Schrijver [11, eqn. (19), p. 91], for example.

To label the variables in the primal linear program (P_n), we let u, v represent divisors of n which are larger than 1, and we let $\{u, v\}$ denote an unordered pair of divisors with both $u, v > 1$ and $uv \mid n$; we permit the equality $u = v$ if $u^2 \mid n$. The linear program (P_n) is as follows.

Primal LP : (P_n)

$$\begin{array}{lccl}
\text{MAXIMIZE} & \ell_P(\alpha) & = & \sum_{u|n, u>1} \quad \frac{1}{u}\, \alpha_u \\
\quad \textit{subject to} & & & \\
\text{nonnegativity constraints :} & \alpha_u & \geq & 0 \\
\quad \textit{and} & & & \\
\text{nontrivial constraints } C(\beta_u) : & \alpha_u & \leq & 1 \\
\text{nontrivial constraints } C(\beta_{\{u,v\}}) : & \alpha_u + \alpha_v + \alpha_{uv} & \leq & 2
\end{array}$$

This linear program has $\delta_1(n)$ variables α_u, where $\delta_1(n)$ denotes the number of divisors of n that exceed 1. These are the variables which appear in the linear *objective function* $\ell_P(\alpha)$, where α denotes the vector of variables $\alpha = (\alpha_u)_{u|n, u>1}$. We refer to the nonnegativity constraints as *trivial* constraints and call all the other constraints *nontrivial.* The nontrivial constraints of this linear program are named after the variables β_u and $\beta_{\{u,v\}}$ that occur in the dual linear program (D_n) described below. There are $\delta_1(n) + \delta_2(n)$ nontrivial constraints, where $\delta_2(n)$ counts the number of unordered pairs $\{u, v\}$ with $u, v > 1$ and $uv \mid n$.

We let $L_P^{opt}(n)$ denote the optimal objective function of this linear program, which is the maximum possible value given the constraints, explicitly noting its dependence on n. We note that Lemma 2.2 shows that the values of $\alpha_u(\mathcal{S})$ with $u > 1$ for any product-free set $\mathcal{S} \pmod{n}$ give a feasible solution to (P_n).

To a primal linear program (P_n) there is a canonically associated *dual linear program* (D_n). To label the dual variables, we let u, v, w represent divisors of n which are larger than 1. Some dual variables are labeled by unordered pairs of divisors e.g. $\{u, v\}$, and in this case we require $uv \mid n$, and again we allow $u = v$ when $u^2 \mid n$. The dual linear program (D_n) is as follows.

Dual LP: (D_n)

$$\begin{array}{lrcl}
\text{MINIMIZE} & \ell_D(\beta) & = & \sum_{u|n,u>1} \beta_u + 2\sum_{\{u,v\},\, uv|n,\, u,v>1} \beta_{\{u,v\}} \\
\quad subject\ to & & & \\
\text{nonnegativity constraints :} & \beta_u & \geq & 0 \\
\text{nonnegativity constraints :} & \beta_{\{u,v\}} & \geq & 0 \\
\quad and & & & \\
\text{nontrivial constraints } C(\alpha_u) : & \beta_u + \sum_{\{v,w\},\, vw=u} \beta_{\{v,w\}} + \sum^{*}_{v,\, uv|n} \beta_{\{u,v\}} & \geq & \frac{1}{u}.
\end{array}$$

The asterisk in $\sum^*$ signifies that the summand $\beta_{\{u,v\}}$ is counted twice in the case that $v = u$. (This corresponds to the primal LP constraint $C(\beta_{\{u,v\}})$ taking the form $2\alpha_u + \alpha_{uv} \leq 2$ when $u = v$.)

The nontrivial constraints $C(\alpha_u)$ in this linear program are named after the variables α_u in the primal linear program (D_n); there are $\delta_1(n)$ of them. The role of nontrivial constraints and variables interchanges between the primal and dual linear programs; one sees that (D_n) has $\delta_1(n) + \delta_2(n)$ variables and $\delta_1(n)$ nontrivial constraints. In addition the objective function coefficients and the constraint bound coefficients interchange in the two programs. We let $L_D^{opt}(n)$ denote the optimal value of the dual objective function $\ell_D(\beta)$, which is the minimal possible value given the constraints, explicitly noting its dependence on n.

Our results use only the following basic facts about LP duality.

Proposition 3.1. *For each $n \geq 2$, the linear programs (P_n) and (D_n) have equal optimal values: $L_P^{opt}(n) = L_D^{opt}(n)$. In particular, any feasible solution $\beta = (\beta_u, \beta_{\{v,w\}})$ of the dual linear program (D_n) has*

$$\ell_D(\beta) \geq L_P^{opt}(n). \tag{3.1}$$

Proof. These are standard results in linear programming duality, see Schrijver [11, Sec. 7.4, p. 90-91]. The equality of primal and dual optimal values holds whenever both linear programs in a dual pair have a feasible solution ([11, Corollary 7.1g, p. 90]). Here these conditions are satisfied by inspection, for (P_n) we have the feasible solution taking all $\alpha_u = 0$, and for (D_n) we have the feasible solution taking all $\beta_u = \frac{1}{u}$ and all $\beta_{\{u,v\}} = 0$.

The inequality (3.1) follows from *weak duality*, which asserts that any primal feasible solution α and dual feasible solution β satisfy $\ell_P(\alpha) \leq \ell_D(\beta)$. Here this is verifiable directly using the primal and dual constraints by noting that

$$\begin{aligned}
\ell_P(\alpha) = \sum_{u|n,u>1} \frac{1}{u}\alpha_u &\leq \sum_{u|n,u>1} \left(\beta_u + \sum_{\{v,w\},\, vw=u} \beta_{\{v,w\}} + \sum_{v,\, uv|n}{}^{*} \beta_{\{u,v\}} \right) \alpha_u \\
&= \sum_{\substack{u|n \\ u>1}} \beta_u \alpha_u + \sum_{\substack{\{v,w\} \\ v,\, w>1,\, vw|n}} \beta_{\{v,w\}} (\alpha_v + \alpha_w + \alpha_{vw}) \\
&\leq \sum_{\substack{u|n \\ u>1}} \beta_u + 2 \sum_{\substack{\{v,w\} \\ v,\, w>1,\, vw|n}} \beta_{\{v,w\}} = \ell_D(\beta),
\end{aligned}$$

as required. □

We first note the following easy lower bound on the optimal primal value $L_P^{opt}(n)$.

Proposition 3.2. *For every $n \geq 2$ there holds*

$$L_P^{opt}(n) \geq \frac{2}{3} \sum_{u|n, u>1} \frac{1}{u}.$$

Proof. We take all $\alpha_u = \frac{2}{3}$. This is obviously a feasible solution to the linear program (P_n) and its objective function value $\ell_P(\alpha) = \frac{2}{3} \sum_{u|n,u>1} \frac{1}{u}$. This value can be no larger than $L_P^{opt}(n)$, giving the result. □

For later use, we restate the dual objective function in the special case of a dual feasible solution that attains equality in all the nontrivial constraints.

Proposition 3.3. *In the dual linear program (D_n) if a feasible solution β attains equality in all the nontrivial constraints $C(\alpha_u)$, then*

$$\ell_D(\beta) = \sum_{\substack{u|n \\ u>1}} \frac{1}{u} - \sum_{\substack{\{v,w\} \\ vw|n,\ v,w>1}} \beta_{\{v,w\}}.$$

Proof. Assume that equality holds in all the nontrivial constraints of (D_n). Adding them together yields

$$\sum_{u|n,\ u>1} \beta_u + 3 \sum_{\substack{\{v,w\} \\ vw|n,\ v,w>1}} \beta_{\{v,w\}} = \sum_{u|n,\ u>1} \frac{1}{u}.$$

(One checks here that each $\beta_{\{v,w\}}$ occurs exactly three times across all the constraints.) Therefore, using the definition of $\ell_D(\beta)$, we have

$$\ell_D(\beta) = \sum_{u|n,\ u>1} \beta_u + 2 \sum_{\substack{\{v,w\} \\ vw|n,\ v,w>1}} \beta_{\{v,w\}} = \sum_{u|n,\ u>1} \frac{1}{u} - \sum_{\substack{\{v,w\} \\ vw|n,\ v,w>1}} \beta_{\{v,w\}},$$

as asserted. □

4. Primal Linear Program Bound

Our object is to relate the bound for the primal linear program (P_n) to the density function $D(n)$. We establish such a relation for integers of a special form.

Given a product-free set $\mathcal{S} \pmod{n}$, note that $\mathcal{S}$ is the disjoint union of the sets $\mathcal{S}_u$ for $u \mid n$, so that $|\mathcal{S}| = \sum_{u|n} |\mathcal{S}_u| = \sum_{u|n} |\mathcal{T}_u| \alpha_u = \sum_{u|n} \varphi\left(\frac{n}{u}\right) \alpha_u$, and hence

$$D(\mathcal{S}) = \frac{1}{n}|\mathcal{S}| = \sum_{u|n} \frac{1}{n} \varphi\left(\frac{n}{u}\right) \alpha_u.$$

On the other hand, the linear program (P_n) has the objective function

$$\ell_P(\alpha) = \sum_{u|n,u>1} \frac{1}{u} \alpha_u.$$

These two functions assign different weights to the variables α_u. These weights are related by the inequality

$$\frac{1}{n}\varphi\left(\frac{n}{u}\right) \geq \frac{\varphi(n)}{n}\frac{1}{u},$$

which goes in the wrong direction for obtaining an upper bound, but has the positive feature that equality holds for those divisors u of n such that each prime factor of u divides n/u. The equality case gives exactly those u such that each prime divisor of u divides n to a non-maximal power, and in this case the coefficient of these variables α_u in $\ell_P(\alpha)$ is exactly $\frac{n}{\varphi(n)}$ times that of the same variable appearing in $D(\mathcal{S})$. This suggests that $D(n)$ be compared with $\frac{\varphi(n)}{n}L_P^{opt}(n)$, and that this be done in cases when all primes dividing n do so to a high power. We obtain the following result, which controls the loss from the inequality above.

Theorem 4.1. *Let n be an arbitrary positive integer and set*

$$X = X(n) = \lfloor \log n \rfloor, \quad N = N(n) = \left(n\prod_{p\leq X} p\right)^X.$$

Then $n \mid N$ and

$$D(N) \leq \frac{\varphi(N)}{N}\left(1 + L_P^{opt}(N)\right). \tag{4.1}$$

Proof. We first note that the theorem holds for all cases where $X = 0$ or 1, which correspond to $n \leq 7$. If $X = 0$, then $N = 1$ and $D(N) = 0$, so the inequality holds. If $X = 1$, then $N = n$. In each case up to $n = 7$ we have $D(N) < \frac{1}{2} \leq \varphi(N)/N$ except for $n = N = 6$, in which case it is easy to see that $D(N) = \frac{1}{3} = \varphi(N)/N$. Thus we may assume that $n \geq 8$, and hence $X \geq 2$.

We next show that if $X \geq 2$ and $D(N) \leq \frac{1}{2}$ then (4.1) holds. This would follow if we show that $\frac{\varphi(N)}{N}\left(1 + L_P^{opt}(N)\right) > \frac{1}{2}$ holds when $X \geq 2$. We observe that

$$\sum_{u|N}\frac{1}{u} \geq \prod_{p|N}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^X}\right) \geq \prod_{p|N}\left(1 + \frac{1}{p} + \frac{1}{p^2}\right).$$

Using this fact together with Proposition 3.2 and $X \geq 2$ we obtain

$$\begin{aligned}\frac{\varphi(N)}{N}\left(1 + L_P^{opt}(N)\right) &\geq \frac{\varphi(N)}{N}\left(1 + \frac{2}{3}\sum_{u|N,u>1}\frac{1}{u}\right) > \frac{\varphi(N)}{N}\cdot\frac{2}{3}\sum_{u|N}\frac{1}{u}\\ &\geq \frac{2}{3}\prod_{p|N}\left(1-\frac{1}{p}\right)\left(1+\frac{1}{p}+\frac{1}{p^2}\right) = \frac{2}{3}\prod_{p|N}\left(1-\frac{1}{p^3}\right) > \frac{2}{3\zeta(3)} > \frac{1}{2}.\end{aligned}$$

It remains to treat the cases where $X \geq 2$ and $D(N) > \frac{1}{2}$. From [9], this implies that we may assume that $\omega(N) \geq 6$. Note that if $X \leq 5$, then $n < \mathrm{e}^6 < 403$, so that there are at most two different primes greater than 5 dividing n, and so $\omega(N) \leq 5$. Hence we may assume that $X \geq 6$.

Now suppose $\mathcal{S}$ is a product-free subset of $\mathbb{Z}/N\mathbb{Z}$ having $D(\mathcal{S}) > \frac{1}{2}$. We take $\alpha_u := \alpha_u(\mathcal{S})$, as in Lemma 2.2, whose values for $u|N, u > 1$ give a feasible solution to (P_N), and Lemma 2.3 gives $\alpha_1 = 0$. Every $u \mid N$ is uniquely factorable as $u = bv$, where $b\|N$ and $v \mid (N/b)/\mathrm{rad}(N/b)$. We have $\varphi(N/u) = \varphi(N)/(\varphi(b)v)$. Thus,

$$|\mathcal{S}| = \sum_{\substack{u|N\\u>1}} |\mathcal{S}_u| = \sum_{\substack{u|N\\u>1}} \alpha_u \varphi\left(\frac{N}{u}\right) = \varphi(N) \sum_{v|\frac{N}{\mathrm{rad}(N)}} \frac{\alpha_v}{v} + \varphi(N) \sum_{\substack{b\|N\\b>1}} \frac{b}{\varphi(b)} \sum_{v|\frac{N/b}{\mathrm{rad}(N/b)}} \frac{\alpha_{vb}}{vb}.$$

Using $\alpha_{vb} \leq 1$, the second expression on the right is at most

$$\varphi(N) \sum_{\substack{b\|N\\b>1}} \frac{1}{\varphi(b)} \cdot \frac{\sigma(N/b)}{N/b} \leq \varphi(N) \sum_{\substack{b\|N\\b>1}} \frac{1}{\varphi(b)} \cdot \frac{N/b}{\varphi(N/b)} = N \sum_{\substack{b\|N\\b>1}} \frac{1}{b},$$

using $\sigma(m)/m \leq m/\varphi(m)$ (see [6, Theorem 329]). Hence

$$\frac{1}{N}|\mathcal{S}| \leq \frac{\varphi(N)}{N} \sum_{\substack{u|N\\u>1}} \frac{\alpha_u}{u} + \sum_{\substack{b\|N\\b>1}} \frac{1}{b}. \tag{4.2}$$

We now claim that

$$\sum_{\substack{b\|N\\b>1}} \frac{1}{b} \leq \frac{\varphi(N)}{N}. \tag{4.3}$$

We defer its proof. Using (4.2) and the claim (4.3) we deduce that

$$\frac{1}{N}|\mathcal{S}| \leq \frac{\varphi(N)}{N}\left(1 + \sum_{u|N, u>1} \frac{\alpha_u}{u}\right) \leq \frac{\varphi(N)}{N}\left(1 + L_P^{opt}(N)\right).$$

Since this holds for all product-free sets $\mathcal{S} \subset \mathbb{Z}/n\mathbb{Z}$ with $D(\mathcal{S}) > \frac{1}{2}$, we conclude that the bound (4.1) holds for $D(N)$, completing the argument.

It remains to prove the claim (4.3). Since each number b with $b\|N$ is an Xth power, we have

$$\sum_{\substack{b\|N\\b>1}} \frac{1}{b} < \sum_{m=2}^{\infty} \frac{1}{m^X} < \frac{1}{2^X} + \int_2^{\infty} \frac{\mathrm{d}t}{t^X} \leq \frac{1.4}{2^X}, \tag{4.4}$$

using $X \geq 6$. Since the number of distinct primes dividing n that exceed X is at most $\log n/\log X < (X+1)/\log X < X$ for $X \geq 6$, we have

$$\frac{\varphi(N)}{N} = \prod_{\substack{p|n\\p>X}} \left(1 - \frac{1}{p}\right) \prod_{p \leq X} \left(1 - \frac{1}{p}\right) > \left(1 - \frac{1}{X}\right)^X \prod_{p \leq X} \left(1 - \frac{1}{p}\right) > \frac{1}{3} \prod_{p \leq X} \left(1 - \frac{1}{p}\right). \tag{4.5}$$

Using an explicit estimate of Rosser and Schoenfeld [10, Corollary to Theorem 7] and (4.5), we see that

$$\frac{\varphi(N)}{N} > \frac{1}{3\mathrm{e}^{\gamma} \log X}\left(1 - \frac{1}{\log^2 X}\right) \tag{4.6}$$

and so (4.4) and (4.6) imply that (4.3) holds when $X \geq 6$. □

5. Proof of Theorem 1.1

Let n be a large integer, let $X = \lfloor \log n \rfloor$, and let

$$N = N(n) = \left(n \prod_{p \le X} p \right)^X,$$

as in Theorem 4.1. Lemma 2.3 implies that any product-free set $\mathcal{S}$ having $D(\mathcal{S}) \ge \frac{1}{2}$ necessarily has $\alpha_1 = 0$, and for these, Lemma 2.2 shows that the remaining α_u with $u > 1$ give a feasible solution to (P_N).

To bound the primal LP objective function from above, we investigate the dual linear program (D_N). A trivial choice for the variables β, in which all the nontrivial constraints hold with equality, is to have each $\beta_u = 1/u$ and each $\beta_{\{u,v\}} = 0$. This gives $L_D^{opt}(N) \le \sum_{u|N, u>1} \frac{1}{u} = \frac{\sigma(N)}{N} - 1$. Using Theorem 4.1 and Proposition 3.1, we obtain

$$D(N) \le \frac{\varphi(N)}{N}(1 + L_P^{opt}(N)) = \frac{\varphi(N)}{N}(1 + L_D^{opt}(N)) \le \frac{\varphi(N)}{N}\frac{\sigma(N)}{N} < 1, \tag{5.1}$$

when $N > 1$. Using Theorem 4.1, (5.1) leads to an estimate of the shape $D(n) < 1 - c/n^{\log 2}$, which is much worse than our estimate (2.5). However we will improve on this upper bound by deforming this solution via "mass shifting" from some of the variables β_u to the other variables $\beta_{\{v,w\}}$, while keeping all the nontrivial constraints tight.

To maximize the gain, Proposition 3.3 suggests that one should move as much "mass" as possible onto the variables $\beta_{\{u,v\}}$. As a critical parameter for the mass-shifting, we introduce

$$k = k(X) = \left\lfloor \frac{\mathrm{e}}{4} \log\log X \right\rfloor. \tag{5.2}$$

We discuss this parameter choice in Remark 5.2 after the proof.

Lemma 5.1. *With the value of k just defined, we have*

$$\binom{2k}{k} \asymp \frac{4^k}{\sqrt{k}} \asymp \frac{(\log X)^{\frac{\mathrm{e}}{2}\log 2}}{\sqrt{\log\log X}} \asymp \frac{(\log\log X)^k}{k!} \asymp \sum_{\substack{m \le X \\ \Omega(m)=k}} \frac{1}{m}.$$

Proof. The first three relations are clear from Stirling's formula and the definition of k. The last relation can be derived using a famous theorem of Sathe and Selberg [12] (see also [8, Theorem 7.19]). We use only the somewhat weaker version: for all $x \ge 20$ and $\epsilon > 0$, over the range of integers j with $1 \le j \le (2-\epsilon)\log\log x$ the estimate

$$\sum_{\substack{m \le x \\ \Omega(m)=j}} 1 \asymp \frac{x}{\log x}\frac{(\log\log x)^{j-1}}{(j-1)!} \tag{5.3}$$

holds uniformly, the implied constants depending only on ϵ. By partial summation, we have

$$\sum_{\substack{m\le X\\ \Omega(m)=k}}\frac{1}{m}=\frac{1}{X}\sum_{\substack{m\le X\\ \Omega(m)=k}}1+\int_1^X\frac{1}{t^2}\sum_{\substack{m\le t\\ \Omega(m)=k}}1\,\mathrm{d}t$$

$$=\int_1^X\frac{1}{t^2}\sum_{\substack{m\le t\\ \Omega(m)=k}}1\,\mathrm{d}t+O(1)=\int_{\mathrm{e}^{\sqrt{\log X}}}^X\frac{1}{t^2}\sum_{\substack{m\le t\\ \Omega(m)=k}}1\,\mathrm{d}t+O\left(\sqrt{\log X}\right).$$

Using (5.3) and the already proved third relation,

$$\int_{\mathrm{e}^{\sqrt{\log X}}}^X\frac{1}{t^2}\sum_{\substack{m\le t\\ \Omega(m)=k}}1\,\mathrm{d}t\asymp\int_{\mathrm{e}^{\sqrt{\log X}}}^X\frac{1}{t\log t}\frac{(\log\log t)^{k-1}}{(k-1)!}\,\mathrm{d}t$$

$$=\left(1-2^{-k}\right)\frac{(\log\log X)^k}{k!}\asymp\frac{(\log X)^{\frac{\mathrm{e}}{2}\log 2}}{\sqrt{\log\log X}}.$$

Since $\frac{\mathrm{e}}{2}\log 2>\frac{1}{2}$, the error $O(\sqrt{\log x})$ is negligible, and so the last relation in the lemma follows. □

Based on Lemma 5.1 we choose as a weight parameter

$$A=A(X):=c_0(\log X)^{\frac{\mathrm{e}}{2}\log 2}/\sqrt{\log\log X}.$$

where c_0 is chosen large enough to assure that for all large n we have both

$$A\ge\binom{2k}{k},\quad \frac{1}{2}A\ge\sum_{\substack{m\le X\\ \Omega(m)=k}}\frac{1}{m}. \tag{5.4}$$

We now define the variable values for a better feasible solution to the dual linear program (D_N). If $uv\mid N$, $u,v>1$, we set

$$\beta_{\{u,v\}}:=\begin{cases}\frac{1}{uvA}, & \text{when } u,v\le X \text{ and } \Omega(u)=\Omega(v)=k,\\ 0 & \text{otherwise.}\end{cases}$$

We then choose the variables β_u by the rule

$$\beta_u:=\frac{1}{u}-\sum_{\substack{v\\ uv|N}}{}^{*}\,\beta_{\{u,v\}}-\sum_{\substack{\{v,w\}\\ vw=u}}\beta_{\{v,w\}},$$

where we continue to understand that u,v,w run over divisors of N that exceed 1. That is, these variables are obtained from the β_u in the "trivial" solution by subtracting off exactly the amount required by the new $\beta_{\{u,v\}}$ needed to keep the constraints $C(\alpha_u)$ tight. The parameter A in the definition of $\beta_{\{u,v\}}$ serves as a weight chosen (approximately) optimally so that the new β_u will remain nonnegative.

Thus, we have equality in the constraints $C(\alpha_u)$, and we next show that we have nonnegativity for our variables β_u, so that we have a dual feasible solution. First note that if $\Omega(u)\ne k,2k$, then

$\beta_u = 1/u > 0$. Now suppose that $\Omega(u) = k$. Then,

$$\beta_u = \frac{1}{u} - {\sum_{\substack{v \\ uv|N}}}^{*} \beta_{\{u,v\}} \geq \frac{1}{u} - \frac{2}{uA} \sum_{\substack{v \leq X \\ \Omega(v)=k}} \frac{1}{v} \geq 0,$$

by (5.4). Finally suppose that $\Omega(u) = 2k$. Then,

$$\beta_u = \frac{1}{u} - \frac{1}{uA} \sum_{\substack{\{v,w\} \\ vw=u \\ \Omega(v)=\Omega(w)=k}} 1 \geq 0.$$

The inequality holds because the number of summands here is at most the number of partitions of a $2k$-element set into two k-element sets, which is $\frac{1}{2}\binom{2k}{k} < A$, by (5.4).

Thus, β is feasible for (D_N), and so $\ell_D(\beta) \geq L_P^{opt}(N)$, by Proposition 3.1. We now get an upper bound for $\ell_D(\beta)$ using Proposition 3.3:

$$\ell_D(\beta) = \sum_{\substack{u|N \\ u>1}} \frac{1}{u} - \sum_{\{u,v\}} \beta_{\{u,v\}} \leq \sum_{\substack{u|N \\ u>1}} \frac{1}{u} - \frac{1}{2} \sum_{\substack{u,v \\ u,v \leq X \\ \Omega(u)=\Omega(v)=k}} \beta_{\{u,v\}} = \Big(\frac{\sigma(N)}{N} - 1\Big) - \frac{1}{2A} \left(\sum_{\substack{u \leq X \\ \Omega(u)=k}} \frac{1}{u} \right)^2 .$$

By Lemma 5.1, the sum here is of order $(\log X)^{\frac{\mathrm{e}}{2}\log 2}/\sqrt{\log\log X}$, and A is of this order as well. Since $\sigma(N)/N \leq N/\varphi(N)$, we obtain

$$\ell_D(\beta) \leq \Big(\frac{N}{\varphi(N)} - 1\Big) - c_1 \frac{(\log X)^{\frac{\mathrm{e}}{2}\log 2}}{\sqrt{\log\log X}} \tag{5.5}$$

for some absolute constant $c_1 > 0$ and all sufficiently large n.

We next obtain an upper bound for $D(N)$. Theorem 4.1 and Proposition 3.1 combine with (5.5) to yield

$$D(N) \leq \frac{\varphi(N)}{N}\Big(1 + L_P^{opt}(N)\Big) \leq \frac{\varphi(N)}{N}\Big(1 + \ell_D(\beta)\Big) \leq \frac{\varphi(N)}{N}\left(\frac{N}{\varphi(N)} - c_1 \frac{(\log X)^{\frac{\mathrm{e}}{2}\log 2}}{\sqrt{\log\log X}}\right).$$

Now the lower bound (4.6) yields

$$D(N) \leq 1 - \frac{c}{(\log X)^{1-\frac{\mathrm{e}}{2}\log 2}\sqrt{\log\log X}}$$

for some positive constant c and for all n sufficiently large.

Finally, since $D(n) \leq D(N)$ by Lemma 2.1, this bound applies to $D(n)$ as well. But $\log X \leq \log\log n$, so

$$D(n) \leq 1 - \frac{c}{(\log\log n)^{1-\frac{\mathrm{e}}{2}\log 2}\sqrt{\log\log\log n}}$$

holds for n sufficiently large. Since $D(n) < 1$ for all n, by adjusting c if necessary, we have the inequality holding for all $n \geq 20$. This completes the proof of Theorem 1.1.

Remark 5.2. The choice of the critical parameter (5.2) in the argument is based on specific features of the dual LP. Each dual variable $\beta_{\{u,v\}}$ appears with weight 1 in three nontrivial dual LP constraints, namely in $C(\alpha_u)$, $C(\alpha_v)$ and $C(\alpha_{uv})$. (If $u = v$ it appears in $C(\alpha_u)$ with weight 2.) If some mass is assigned to the variable $\beta_{\{u,v\}}$ this mass counts towards the constraint masses $\frac{1}{u}, \frac{1}{v}, \frac{1}{uv}$ (i.e., the right hand sides of the dual nontrivial constraints for which $\beta_{\{u,v\}}$ appears.) Now, for any fixed value of the parameter k, at least one of $w = u, v, uv$ will satisfy either $\Omega(w) \le k$ or $\Omega(w) > 2k$. This, together with the condition of equality of all dual constraints (note that the contribution from the β_u-terms is positive), gives that

$$\sum_{\{u,v\}} \beta_{\{u,v\}} \le \sum_{u:\Omega(u)\notin[k+1,2k]} \left(\sum_{v:uv|N}{}^{*} \beta_{\{u,v\}} + \sum_{\{v,w\}:vw=u} \beta_{\{v,w\}} \right) \le \sum_{u:\Omega(u)\notin[k+1,2k]} \frac{1}{u}, \tag{5.6}$$

which imposes an upper bound on the total mass shifting. The value (5.2) for k minimizes the right side, and establishes the strongest upper limit of this kind on the mass that can be moved. Since a positive fraction of the mass on the right side occurs at level k, this suggests attempting to move mass on exactly this level. The proof then shows that this upper limit can be attained, up to a constant factor. Finally the restriction in the definition of $\beta_{\{u,v\}}$ to $u, v \le X$ is convenient and does not appreciably alter the situation.

6. Proof of Theorem 1.2

This result is proved by a modification of the proof of Theorem 1 in [7].

Let ℓ_x denote the least common multiple of the integers in $[1, x]$, and let $n_x = \ell_x^2$. As in the previous section, let $k = k(x) = \lfloor \frac{e}{4} \log\log x \rfloor$. Instead of the specific values k and $2k$ which occurred in the previous section, the key now is the interval $(k, 2k)$. In the proof of Theorem 2.1 in [7], we showed that

$$D(n_x) \ge 1 - \frac{\pi(x)}{x} - \frac{\varphi(n_x)}{n_x} \sum_{\substack{d|\ell_x \\ \Omega(d)\notin(k,2k)}} \frac{1}{d} \ge 1 - \frac{\pi(x)}{x} - \frac{\varphi(n_x)}{n_x} \sum_{\substack{P(d)\le x \\ \Omega(d)\notin(k,2k)}} \frac{1}{d},$$

where $P(d)$ denotes the largest prime factor of $d > 1$ (and $P(1) = 1$). Our result then followed from the bounds $\varphi(n_x)/n_x \asymp 1/\log x$ and $\log x \asymp \log\log n_x$, and from the estimate

$$\sum_{\substack{P(d)\le x \\ \Omega(d)\notin(k,2k)}} \frac{1}{d} \ll (\log x)^{\frac{e}{2}\log 2}. \tag{6.1}$$

Our objective here is to improve on the estimate (6.1) and show that

$$\sum_{\substack{P(d)\le x \\ \Omega(d)\notin(k,2k)}} \frac{1}{d} \ll \frac{(\log x)^{\frac{e}{2}\log 2}}{\sqrt{\log\log x}}, \tag{6.2}$$

from which Theorem 1.2 follows directly. Towards doing this, we prove the following lemma.

Lemma 6.1. *Let $\epsilon > 0$ be arbitrary but fixed. Let $\mathcal{P}$ be a non-empty set of prime numbers and assume $s := \sum_{p\in\mathcal{P}} 1/p < \infty$. Let $\mathcal{N}_{\mathcal{P}}$ denote the set of integers all of whose prime factors come from $\mathcal{P}$. Then*

$$\frac{s^j}{j!} \le \sum_{\substack{n\in\mathcal{N}_{\mathcal{P}} \\ \Omega(n)=j}} \frac{1}{n} \ll_\epsilon \frac{s^j}{j!}$$

for every integer $0 \le j \le (2-\epsilon)s$.

Remark 6.2. If the least prime in $\mathcal{P}$ is p_0, then this result can be extended to the range $j \le (p_0 - \epsilon)s$, with the implied constant then depending on both p_0 and ϵ.

Proof. The lower bound is almost immediate and it holds for all j. Indeed, expanding s^j by the multinomial theorem, each term is of the form b_n/n where b_n is a multinomial coefficient, $n \in \mathcal{N}_{\mathcal{P}}$, and $\Omega(n) = j$. Since $b_n \le j!$, the lower bound follows. We note that this argument also shows that $s^j/j!$ stands as an upper bound for the sum over *squarefree* n in the lemma.

For $n \in \mathcal{N}_{\mathcal{P}}$, write $n = m^2 u$, where u is squarefree. Since $\Omega(m^2) = 2\Omega(m)$, we have by the observation above about squarefree numbers,

$$W_j := \sum_{\substack{n \in \mathcal{N}_{\mathcal{P}} \\ \Omega(n)=j}} \frac{1}{n} \le \sum_{\substack{m \in \mathcal{N}_{\mathcal{P}} \\ \Omega(m) \le j/2}} \frac{1}{m^2} \cdot \frac{s^{j-2\Omega(m)}}{(j-2\Omega(m))!}.$$

This, together with $j!/(j-2\Omega(m))! \le j^{2\Omega(m)}$, gives that

$$\begin{aligned} W_j &\le \frac{s^j}{j!} \sum_{\substack{m \in \mathcal{N}_{\mathcal{P}} \\ \Omega(m) \le j/2}} \frac{1}{m^2} \cdot \frac{j!}{(j-2\Omega(m))!} s^{-2\Omega(m)} \le \frac{s^j}{j!} \sum_{\substack{m \in \mathcal{N}_{\mathcal{P}} \\ \Omega(m) \le j/2}} \frac{1}{m^2} \cdot \left(\frac{j}{s}\right)^{2\Omega(m)} \\ &\le \frac{s^j}{j!} \sum_{\substack{m \in \mathcal{N}_{\mathcal{P}} \\ \Omega(m) \le j/2}} \frac{(2-\epsilon)^{2\Omega(m)}}{m^2} \le \frac{s^j}{j!} \prod_{p \in \mathcal{P}} \left(1 + \sum_{i=1}^{\infty} \frac{(2-\epsilon)^{2i}}{p^{2i}}\right) \\ &= \frac{s^j}{j!} \prod_{p \in \mathcal{P}} \left(1 - \left(\frac{2-\epsilon}{p}\right)^2\right)^{-1} \ll_\epsilon \frac{s^j}{j!}, \end{aligned}$$

and the proof of the lemma is complete. □

We now prove (6.2), which as we have seen, is sufficient for the proof of Theorem 1.2. We may assume that x is large. Let $\mathcal{P}$ be the set of primes in $[1, x]$, so that $\mathcal{N}_{\mathcal{P}}$ consists of the integers n with $P(n) \le x$ and $s = \log\log x + O(1)$. Let $a_j = s^j/j!$ and note that if $j < k$, then a_j/a_{j+1} is bounded below 1. Thus, by Lemma 6.1 and Lemma 5.1, we have

$$\sum_{\substack{P(n) \le x \\ \Omega(n) \le k}} \frac{1}{n} \ll \sum_{j \le k} a_j \ll a_k \ll \frac{(\log x)^{\frac{\mathrm{e}}{2}\log 2}}{\sqrt{\log\log x}}.$$

Similarly, a_{j+1}/a_j is bounded below 1 when $j \ge 2k$, so that by Lemma 6.1 applied for $2k \le j \le 2.5k$ ($< 1.7 \log\log x$),

$$\sum_{\substack{P(n) \le x \\ 2k \le \Omega(n) \le 2.5k}} \frac{1}{n} \ll \sum_{2k \le j \le 2.5k} a_j \ll a_{2k} \ll \frac{(\log x)^{\frac{\mathrm{e}}{2}\log 2}}{\sqrt{\log\log x}},$$

the last inequality holding as in the third relation in Lemma 5.1. It remains to consider those n with $\Omega(n) > 2.5k$. Using [7, Corollary 2.5], we have that

$$\sum_{\substack{P(n) \le x \\ \Omega(n) \ge (2.5\mathrm{e}/4)\log\log x}} \frac{1}{n} \ll (\log x)^{-(2.5\mathrm{e}/4)\log(2.5/4)} < (\log x)^{0.8},$$

which is negligible. This then proves (6.2) and Theorem 1.2.

Acknowledgments

Part of this work was done while the three authors visited MSRI, as part of the semester program "Arithmetic Statistics." They thank MSRI for support, funded through the NSF. The first author was supported in part by grants from the Göran Gustafsson Foundation, and the Swedish Research Council. The second author was supported in part by NSF grants DMS-0801029 and DMS-1101373. The third author was supported in part by NSF grant DMS-1001180.

References

[1] P. H. Diananda and H. P. Yap, Maximal sum-free sets of elements of finite groups, *Proc. Japan Acad.* **45** (1969), No. 1, 1–5.

[2] P. Erdős, On sequences of integers no one of which divides the product of two others and on some related problems, *Mitt. Forsch.-Inst. Math. Mech. Univ. Tomsk* **2** (1938), 74–82.

[3] B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math.* **147** (2005), 157–188.

[4] L. Hajdu, A. Schinzel, and M. Skalba, Multiplicative properties of sets of positive integers, *Arch. Math. (Basel)* **93** (2009), 269–276.

[5] R. R. Hall, *Sets of multiples*, Cambridge University Press, 1996.

[6] G. H. Hardy and E. M. Wright, *The theory of numbers, 4th ed.*, Oxford University Press, London, 1968.

[7] P. Kurlberg, J. C. Lagarias and C. Pomerance, Product-free sets with high density, *Acta Arith.,* to appear.

[8] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory I. Classical theory* Cambridge University Press, 2007.

[9] C. Pomerance and A. Schinzel, Multiplicative properties of sets of residues, *Moscow J. Combinatorics and Number Theory* **1** (2011), 52–66.

[10] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[11] A. Schrijver, *Theory of Linear and Integer Programming,* Wiley-Interscience: New York 1986.

[12] A. Selberg, Note on a paper of L. G. Sathe, *J. Indian Math. Soc.***18** (1954), 83–87. (*Collected Papers,* Vol. I. Berlin: Springer-Verlag: New York 1989.)

Department of Mathematics, KTH, SE-10044, Stockholm, Sweden
E-mail address: kurlberg@math.kth.se

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: lagarias@umich.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755, USA
E-mail address: carl.pomerance@dartmouth.edu