

SIEVING BY LARGE INTEGERS AND COVERING SYSTEMS OF CONGRUENCES

Michael Filaseta

Department of Mathematics
University of South Carolina
Columbia, SC 29208
filaseta@math.sc.edu

Kevin Ford

Department of Mathematics
University of Illinois
Urbana, IL 61801
ford@math.uiuc.edu

Sergei Konyagin

Department of Mathematics
Moscow State University
Moscow, Russia 119992
konyagin@ok.ru

Carl Pomerance

Department of Mathematics
Dartmouth College
Hanover, NH 03755-3551
carl.pomerance@dartmouth.edu

Gang Yu

Department of Mathematics
University of South Carolina
Columbia, SC 29208
yu@math.sc.edu

May 25, 2005

2000 Mathematics Subject Classification: 11B25, 11A07, 11N35 *Key words and phrases:* covering system.

The first author was supported by NSF grant DMS-0207302 and NSA grant H98230-05-1-0038. The second author was supported by NSF grant DMS-0301083. Much of the research for this paper was accomplished while the third author was visiting the University of South Carolina, Columbia in January 2004 (supported by NSF grant DMS-0200187) and the University of Illinois at Urbana-Champaign in February 2004 (supported by NSF grant DMS-0301083). The fourth author was supported by NSF grant DMS-0401422.

Abstract

An old question of Erdős asks if there exists, for each number N , a finite set S of integers greater than N and residue classes $r(n) \pmod{n}$ for $n \in S$ whose union is \mathbb{Z} . We prove that if $\sum_{n \in S} 1/n$ is bounded for such a covering of the integers, then the least member of S is also bounded, thus confirming a conjecture of Erdős and Selfridge. We also prove a conjecture of Erdős and Graham, that, for each fixed number $K > 1$, the complement in \mathbb{Z} of any union of residue classes $r(n) \pmod{n}$, for distinct $n \in (N, KN]$, has density at least d_K for N sufficiently large. Here d_K is a positive number depending only on K . Either of these new results implies another conjecture of Erdős and Graham, that if S is a finite set of moduli greater than N , with a choice for residue classes $r(n) \pmod{n}$ for $n \in S$ which covers \mathbb{Z} , then the largest member of S cannot be $O(N)$. We further obtain stronger forms of these results and establish other information, including an improvement of a related theorem of Haight.

1 Introduction

Notice that every integer n satisfies at least one of the congruences

$$n \equiv 0 \pmod{2}, \quad n \equiv 0 \pmod{3}, \quad n \equiv 1 \pmod{4}, \quad n \equiv 1 \pmod{6}, \quad n \equiv 11 \pmod{12}.$$

Such a collection of congruences, where each integer satisfies at least one them, is called a *covering system*. A famous problem of Erdős from 1950 [3] is to determine whether for every N , there is a covering system with distinct moduli greater than N . In other words, can the minimum modulus in a covering system with distinct moduli be arbitrarily large? In regards to this problem, Erdős writes in [5], “This is perhaps my favourite problem.”

There are various other problems that have been posed aiming at a better understanding of what must happen when the minimum modulus in a covering is large. In a covering system with distinct moduli which have a reciprocal sum that is $O(1)$, must the least modulus also be $O(1)$? Erdős and Selfridge ([4]; also see [8], §F13) have conjectured that the answer is yes. Restated, their conjecture is as follows.

Conjecture 1. *For any number B , there is a number N_B , such that in a covering system with distinct moduli greater than N_B , the sum of reciprocals of these moduli is greater than B .*

A version of Conjecture 1 also appears in [6]. Even with $B = 1.001$, this is an intriguing question which apparently is difficult to answer. (The conjecture is trivial for $B < 1$.)

Whether or not one can cover all of \mathbb{Z} , it is interesting to consider how much of \mathbb{Z} one can cover with residue classes $r(n) \pmod{n}$, where the moduli n come from an interval $(N, KN]$ and are distinct. In this regard, Erdős and Graham [6] have formulated the following conjecture.

Conjecture 2. For each number $K > 1$ there is a positive number d_K such that if N is sufficiently large, depending on K , and we choose arbitrary integers $r(n)$ for each $n \in (N, KN]$, then the complement in \mathbb{Z} of the union of the residue classes $r(n) \pmod{n}$ has density at least d_K .

In [5], Erdős writes with respect to establishing such a lower bound d_K for the density, “I am not sure at all if this is possible and I give \$100 for an answer.”

A corollary of either Conjecture 1 or Conjecture 2 is the following conjecture also raised by Erdős and Graham in [6].

Conjecture 3. For any number $K > 1$ and N sufficiently large, depending on K , there is no covering system using distinct moduli from the interval $(N, KN]$.

In this paper we prove strong forms of Conjectures 1, 2, and 3.

Despite the age and fame of the minimum modulus problem, there are still many more questions than answers. We mention a few results. According to [13], the largest known minimum modulus of a covering system with distinct moduli is 24, a result of Morikawa from 1981. If $r_i \pmod{n_i}$ for $i = 1, 2, \dots, l$ is a covering system, then $\sum 1/n_i \geq 1$. Indeed, each residue class $r_i \pmod{n_i}$ covers density $1/n_i$ of the integers, and as the density of the union of these residue classes is at most the sum of the individual densities, we have the inequality. Assuming that the moduli n_i are distinct and larger than 1, it is possible to show that equality cannot occur, that is, $\sum 1/n_i > 1$. The following proof (of M. Newman) is a gem. Suppose that $\sum 1/n_i = 1$. If the system then covers, a density argument shows that there cannot be any overlap between the residue classes, that is, we have an *exact covering system*. We suppose, as we may, that $n_1 < n_2 < \dots < n_l$ and each $r_i \in [0, n_i - 1]$. Then

$$\frac{1}{1-z} = 1 + z + z^2 + \dots = \sum_{i=1}^l (z^{r_i} + z^{r_i+n_i} + z^{r_i+2n_i} + \dots) = \sum_{i=1}^l \frac{z^{r_i}}{1-z^{n_i}}.$$

The right side of this equation has poles at the primitive n_i -th roots of 1, which is not true of the left side. Thus, there cannot be an exact covering system with distinct moduli greater than 1 (in fact, the largest modulus must be repeated).

Say an integer H is “covering” if there is a covering system with distinct moduli with each modulus a divisor of H exceeding 1. For example, 12 is covering, as one can see from our opening example. From the above result, if H is covering, then $\sigma(H)/H > 2$, where σ is the sum-of-divisors function. Benkoski and Erdős [1] wondered if $\sigma(H)/H$ is large enough, would this condition suffice for H to be covering. In [9], Haight showed that this is not the case. We obtain a strengthening of this result, and by a shorter proof.

If one takes moduli n_1, n_2, \dots, n_l that are pairwise coprime, there is no mystery about the density of the residual set if one sieves with these moduli. For any choice of residues r_1, r_2, \dots, r_l ,

the Chinese remainder theorem implies that the asymptotic density of the residual set of integers that are not covered by any of the residue classes $r_i \pmod{n_i}$ is

$$\prod_{i=1}^l (1 - 1/n_i), \quad (1.1)$$

which is necessarily positive if each $n_i > 1$.

One central idea in this paper is to determine how to estimate the density of the residual set when the moduli are arbitrary large integers, not necessarily pairwise coprime. We note that for any n_1, n_2, \dots, n_l , there is a choice for r_1, r_2, \dots, r_l such that the density of the residual set of integers not covered by any of the residue classes $r_i \pmod{n_i}$ is bounded above by the product (1.1). Indeed, this is obvious if $l = 1$. Assume it is true for l , and say we have chosen residues r_1, r_2, \dots, r_l such that the residual set R has density

$$\delta \leq \prod_{i=1}^l (1 - 1/n_i).$$

The residue classes modulo n_{l+1} partition any subset of \mathbb{Z} , and in particular partition R , so that at least one of these residue classes, when intersected with R , has density at least δ/n_{l+1} . Removing such a residue class, the residual set for the $l + 1$ congruences thus has density at most

$$\delta - \delta/n_{l+1} = (1 - 1/n_{l+1})\delta \leq \prod_{i=1}^{l+1} (1 - 1/n_i).$$

Thus, the assertion follows.

Let us look for a moment at Conjecture 3 in the specific case $K = 3$. By the above argument, there is a choice of residues so that if we use all of the integers in $(N, 3N]$ as moduli, the residual set has density at most $1/3$. Conjecture 3 implies that for N large this density cannot be 0, and Conjecture 2 implies that, in fact, the density stays bounded above 0 as N grows. If we sieve optimally does this density approach a limit as $N \rightarrow \infty$? Is this limit $1/3$ or is it smaller?

In general, if S is a finite set of positive integers, let $\delta_0(S)$ be the least possible asymptotic density of a residual set with distinct moduli from S . That is, if $S = \{n_1, n_2, \dots, n_l\}$, and r_1, r_2, \dots, r_l are any integers, we may look at the residual set of integers n that do not satisfy any congruence $n \equiv r_i \pmod{n_i}$, and choose r_1, r_2, \dots, r_l so that this residual set has the least possible asymptotic density. This minimum density is $\delta_0(S)$. Further, let

$$\alpha(S) = \prod_{n \in S} (1 - 1/n),$$

so that we always have $\delta_0(S) \leq \alpha(S)$. With this notation we now state our principal results.

Theorem A. *Let $0 < c < 1/3$ and let N be sufficiently large (depending on c). If S is a finite set of integers $n > N$ such that*

$$\sum_{n \in S} \frac{1}{n} \leq c \frac{\log N \log \log \log N}{\log \log N},$$

then $\delta_0(S) > 0$.

Theorem B. *For any numbers c with $0 < c < 1/2$, $N \geq 20$, and K with*

$$1 < K \leq \exp(c \log N \log \log \log N / \log \log N),$$

if S is a set of integers contained in $(N, KN]$, then

$$\delta_0(S) = (1 + o(1))\alpha(S)$$

as $N \rightarrow \infty$, where the function “ $o(1)$ ” depends only on the choice of c .

Using Lemma 3.4 below, we can make the $o(1)$ term in Theorem B explicit in terms of N and c . Both Theorems A and B, as well as several other of our results, are proved in a more general context of multisets S or, equivalently, where multiple residue classes are allowed for each modulus. Note that Theorems A and B prove Conjectures 1 and 2, respectively, and so Conjecture 3 as well.

If we only bound from below the minimum modulus and remove the upper bound on the largest modulus, then we are able to construct examples of sets of integers S where $\delta_0(S)$ is much smaller than $\alpha(S)$. This kind of result might be interpreted as lending weight towards the existence of covering systems with least modulus being arbitrarily large.

Similar to the definition of $\delta_0(S)$, let $\delta_1(S)$ be the *largest* possible density for a residual set with S being a set of (distinct) moduli. It is known from early work of Erdős [2], that for each $\varepsilon > 0$ there is some $\eta > 0$, such that if S is the set of integers in $(N, N^{1+\eta}]$, then $\delta_1(S) \geq 1 - \varepsilon$ for all large N . This is achieved by taking the 0 residue class for each modulus in S . From Theorem 1 of [7], it follows that for $0 < \eta < 1/2$ and N large depending on η , the density of integers which lie in at least one of the residue classes $0 \pmod n$ for $N < n \leq N^{1+\eta}$ is between $c_1 \eta^\theta (\log 1/\eta)^{-3/2}$ and $c_2 \eta^\theta (\log 1/\eta)^{-3/2}$, where c_1, c_2 are positive absolute constants and $\theta = 1 - (1 + \log \log 2) / \log 2 = 0.08607 \dots$ (see also Theorem 21 of [11]). This raises a natural question (also raised in [6]). Is it the case that for any finite set of positive integers S that are larger than 1, that $\delta_1(S)$ is attained when we choose the residue classes so that there is a single integer that is in each residue class?

In the above example, we have $\delta_0(S) \leq \alpha(S) \leq (1 + o(1))N^{-\eta} = o(1)$ as $N \rightarrow \infty$, while $\delta_1(S) \gg_\eta 1$. What might we expect for the density of the residual set for a random choice of residue classes with moduli in S ? Should the typical case be closer to $\delta_0(S)$, $\alpha(S)$, or $\delta_1(S)$? We

show in general that for any finite integer set S , the average (and typical) case has residual density close to $\alpha(S)$.

Finally we mention another problem we have not been able to settle. Is it true that for each positive number B , there are positive numbers Δ_B, N_B , such that if S is a finite set of positive integers greater than N_B with reciprocal sum at most B , then $\delta_0(S) \geq \Delta_B$? If this holds it would imply each of Conjectures 1, 2, and 3.

2 A basic lemma and Haight's theorem

Let C be a finite multiset of ordered pairs of positive integers (n, r) , which we interpret as a collection of residue classes $r \pmod{n}$. We say such a multiset is a *residue system*. Let $S = S(C)$ be the multiset of the moduli n appearing in C . The number of times an integer n appears in S we call the *multiplicity* of n . By $R(C)$ we denote the set of integers *not* congruent to $r \pmod{n}$ for any $(n, r) \in C$. Since $R(C)$ is a union of residue classes modulo the least common multiple of the members of $S(C)$, it follows that $R(C)$ possesses a (rational) asymptotic density, which we denote by $\delta(C)$. If $C = \{(n_1, r_1), \dots, (n_l, r_l)\}$, then we set

$$\alpha(C) = \prod_{n \in S(C)} \left(1 - \frac{1}{n}\right) = \prod_{j=1}^l \left(1 - \frac{1}{n_j}\right),$$

and

$$\beta(C) = \sum_{\substack{i < j \\ \gcd(n_i, n_j) > 1}} \frac{1}{n_i n_j}.$$

We set $P(n)$ to be the largest prime factor of n . Also, p will always denote a prime.

Lemma 2.1. *For any residue system C , we have $\delta(C) \geq \alpha(C) - \beta(C)$.*

Proof. Let $\alpha = \alpha(C)$ and $\beta = \beta(C)$. We use induction on l . If $l = 1$, then $\beta = 0$ and the statement is trivial. Let $l > 1$; we will describe an induction step from $l - 1$ to l . We denote $C' = \{(n_1, r_1), \dots, (n_{l-1}, r_{l-1})\}$, $C'' = \{(n_j, r_j) : j < l, \gcd(n_j, n_l) = 1\}$,

$$\alpha' = \alpha(C') = \prod_{j=1}^{l-1} \left(1 - \frac{1}{n_j}\right) \quad \text{and} \quad \beta' = \beta(C') = \sum_{\substack{i < j \leq l-1, \\ \gcd(n_i, n_j) > 1}} \frac{1}{n_i n_j}.$$

By the induction supposition,

$$\delta(C') \geq \alpha' - \beta'. \quad (2.1)$$

Also,

$$\delta(C'') \leq \delta(C') + \sum_{n_j \in S(C') \setminus S(C'')} \frac{1}{n_j} = \delta(C') + \sum_{\substack{j < l \\ \gcd(n_j, n_l) > 1}} \frac{1}{n_j}. \quad (2.2)$$

The density of integers covered by the residue class $r_l \pmod{n_l}$ but not covered by $r_j \pmod{n_j}$ for every $n_j \in S(C'')$ is equal to $\delta(C'')/n_l$. Therefore,

$$\begin{aligned} \delta(C') - \delta(C) &= \text{density}\{n \equiv r_l \pmod{n_l} : n \in R(C')\} \\ &\leq \text{density}\{n \equiv r_l \pmod{n_l} : n \in R(C'')\} = \delta(C'')/n_l, \end{aligned}$$

so that, by (2.1) and (2.2),

$$\begin{aligned} \delta(C) &\geq \delta(C') - \left(\delta(C') + \sum_{\substack{j < l \\ \gcd(n_j, n_l) > 1}} \frac{1}{n_j} \right) \frac{1}{n_l} \\ &= \left(1 - \frac{1}{n_l} \right) \delta(C') - \sum_{\substack{j < l \\ \gcd(n_j, n_l) > 1}} \frac{1}{n_j n_l} \\ &\geq \left(1 - \frac{1}{n_l} \right) (\alpha' - \beta') - (\beta - \beta') \geq \left(1 - \frac{1}{n_l} \right) \alpha' - \beta = \alpha - \beta. \end{aligned}$$

This completes the proof of the lemma. □

Remark 1. The proof of Lemma 2.1 actually gives the better bound

$$\delta(C) \geq \alpha(C) - \sum_{\substack{i < j \\ \gcd(n_i, n_j) > 1}} \frac{1}{n_i n_j} \prod_{u > j} \left(1 - \frac{1}{n_u} \right).$$

There is a very interesting negative result of Haight [9]. As in the introduction, we say an integer H is covering if there is a covering system with the moduli being the (distinct) divisors of H that are larger than 1. It is shown in [9] that there exist integers H that are *not* covering, yet $\sum_{d|H} 1/d = \sigma(H)/H$ is arbitrarily large. Although Haight's theorem follows directly from Theorem A (by taking K fixed, N large and H to be the product of the primes in $(N, N^K]$), Lemma 2.1 by itself leads to a new (and short) proof of a stronger version of Haight's result:

Theorem 1. *There is an infinite set of positive integers H such that for any residue system C with $S(C) = \{d : d > 1, d \mid H\}$, we have*

$$\delta(C) \geq (1 + o(1))\alpha(C) \quad \text{and} \quad \sigma(H)/H = (\log \log H)^{1/2} + O(\log \log \log H).$$

In particular, for large H in this set, no such C can have $\delta(C) = 0$.

Proof. Let N be a large parameter, and let

$$H = \prod_{e\sqrt{\log N} \leq p \leq N} p.$$

Then

$$\log \sum_{d \mid H} \frac{1}{d} = \sum_{e\sqrt{\log N} \leq p \leq N} \left(\frac{1}{p} + O\left(\frac{1}{p^2}\right) \right) = \frac{1}{2} \log \log N - \frac{\log \log N + O(1)}{\sqrt{\log N}},$$

by Mertens' theorem. Thus, as $\log H = (1 + o(1))N$ by the prime number theorem, we have

$$\frac{\sigma(H)}{H} = \sum_{d \mid H} \frac{1}{d} = (\log N)^{1/2} - \log \log N + O(1) = (\log \log H)^{1/2} + O(\log \log \log H).$$

Let C be a residue system with $S(C) = \{d : d > 1, d \mid H\}$. We have

$$\log \alpha(C) = \sum_{d \in S(C)} \log(1 - 1/d) = - \sum_{d \in S(C)} 1/d + O\left(\exp(-\sqrt{\log N})\right),$$

so that

$$\alpha(C) = \exp\left(-\sqrt{\log N} + O(1)\right) \log N.$$

Also,

$$\beta(C) \leq \sum_{d > 1} \sum_{\substack{d_1, d_2 \in S(C) \\ d \mid d_1, d \mid d_2}} \frac{1}{d_1 d_2} \leq \sum_{d \mid H, d > 1} \frac{1}{d^2} \sum_{\substack{d_1 \mid H \\ d_2 \mid H}} \frac{1}{d_1 d_2} \ll \log N \sum_{d \mid H, d > 1} \frac{1}{d^2}.$$

Further,

$$\sum_{d \mid H, d > 1} \frac{1}{d^2} \leq \sum_{d > e\sqrt{\log N} \log N} \frac{1}{d^2} \ll \exp\left(-\sqrt{\log N}\right) (\log N)^{-1}.$$

Thus,

$$\beta(C) \ll \exp\left(-\sqrt{\log N}\right) = o(\alpha(C))$$

and the theorem follows from Lemma 2.1. □

Remark 2. An examination of our proof shows that we have a more general result. Let \mathcal{H} be the set of integers H which have no prime factors below $\exp(\sqrt{\log \log H}) \log \log H$. As $H \rightarrow \infty$ in \mathcal{H} we have for any residue system C with $S(C) = \{d : d > 1, d \mid H\}$ that $\delta(C) \geq (1 + o(1))\alpha(C)$. In particular, at most finitely many integers $H \in \mathcal{H}$ are covering.

We also remark that the proof gives the following result. Say that a positive integer H is s -covering, if for each $d \mid H$ with $d > 1$ there are s integers $r_{d,1}, \dots, r_{d,s}$ such that the union of the residue classes $r_{d,i} \pmod{d}$ for $i = 1, \dots, s$, and $d \mid H$ with $d > 1$ is \mathbb{Z} . Then for each fixed $\varepsilon > 0$ there are values of H where $\sigma(H)/H$ is arbitrarily large, yet H is not s -covering with $s = \lceil (\log \log H)^{1-\varepsilon} \rceil$. Indeed, take H to be the product of the primes in $(\exp((\log N)^{1-\varepsilon/3}), N]$ and follow the same proof. This too strengthens a result in [9].

3 The smooth number decomposition

What makes our proof of Theorem 1 work is that the members of $S(C)$ have no small prime factors. We now try to introduce this idea in the general case by splitting the members of $S(C)$ into a smooth part and a part with no small prime factors. In this section we give some further lemmas that quantify this decomposition.

Lemma 3.1. *Let C be an arbitrary residue system. Let P be an arbitrary finite set of primes, and set*

$$M = \prod_{p \in P} p^{\nu(p)},$$

where $\nu(p)$ is the exponent of p in the factorization of $\text{lcm}\{n : n \in S(C)\}$. For $0 \leq h \leq M - 1$, let C_h be the multiset

$$C_h = \left\{ \left(\frac{n}{\gcd(n, M)}, r \right) : (n, r) \in C, r \equiv h \pmod{\gcd(n, M)} \right\}.$$

Then

$$\delta(C) = \frac{1}{M} \sum_{h=0}^{M-1} \delta(C_h).$$

Proof. Fix h so that $0 \leq h \leq M - 1$. For $(n, r) \in C$, the simultaneous congruences

$$x \equiv r \pmod{n}, \quad x \equiv h \pmod{M}$$

have a solution if and only if $r \equiv h \pmod{\gcd(n, M)}$, in which case the system is equivalent to the system

$$x \equiv r \pmod{n/\gcd(n, M)}, \quad x \equiv h \pmod{M}.$$

Thus, $R(C_h) \cap (h \bmod M) = R(C) \cap (h \bmod M)$. Observe that all elements of $S(C_h)$ are coprime to M . Thus, the proportion of the numbers in $R(C_h)$ in the class h modulo M is equal to $\delta(C_h)$. Hence, the density of $R(C) \cap (h \bmod M)$ is $\delta(C_h)/M$ and the result follows. \square

Lemma 3.2. *Let $K > 1$, and suppose $S(C)$ consists of integers in the interval $(N, KN]$, each with multiplicity at most s . Suppose $Q \geq 2$, and let P be the set of primes $\leq Q$. Define M and C_h as in Lemma 3.1. Then*

$$\frac{1}{M} \sum_{h=0}^{M-1} \beta(C_h) \ll \frac{s^2 \log^2(QK)}{Q}. \quad (3.1)$$

Proof. For $m|M$, let S_m be the set of distinct numbers $n/\gcd(n, M)$, where $n \in S(C)$ and $\gcd(n, M) = m$. Let

$$F(r_1, m_1, r_2, m_2) = \#\{0 \leq h \leq M-1 : h \equiv r_1 \pmod{m_1}, h \equiv r_2 \pmod{m_2}\}.$$

Then

$$\frac{1}{M} \sum_{h=0}^{M-1} \beta(C_h) = \frac{1}{M} \sum_{\substack{m_1|M \\ m_2|M}} \sum_{\substack{n_1 \in S_{m_1} \\ n_2 \in S_{m_2} \\ \gcd(n_1, n_2) > 1}} \frac{1}{n_1 n_2} \sum_{\substack{(n_1 m_1, r_1) \in C \\ (n_2 m_2, r_2) \in C}} F(r_1, m_1, r_2, m_2).$$

Since $F(r_1, m_1, r_2, m_2)$ is either 0 or $M/\text{lcm}[m_1, m_2]$, the inner sum is at most

$$s^2 \frac{M}{\text{lcm}[m_1, m_2]}.$$

Next,

$$\begin{aligned} \sum_{\substack{n_1 \in S_{m_1} \\ n_2 \in S_{m_2} \\ \gcd(n_1, n_2) > 1}} \frac{1}{n_1 n_2} &\leq \sum_{p>Q} \sum_{\substack{n_1 \in S_{m_1} \\ n_2 \in S_{m_2} \\ p|n_1, p|n_2}} \frac{1}{n_1 n_2} \\ &= \sum_{p>Q} \left(\sum_{\substack{N/m_1 < n_1 \leq KN/m_1 \\ p|n_1, \gcd(n_1, M)=1}} \frac{1}{n_1} \right) \left(\sum_{\substack{N/m_2 < n_2 \leq KN/m_2 \\ p|n_2, \gcd(n_2, M)=1}} \frac{1}{n_2} \right). \end{aligned}$$

By standard sieve methods (e.g., Theorem 3.3 of [10]), uniformly in $x \geq 2$, $z \geq 2$, the number of integers $\leq x$ which have no prime factor $\leq z$ is $\ll x/\log z + 1$. By partial summation,

$$\sum_{\substack{N/m_j < n_j \leq KN/m_j \\ p|n_j, \gcd(n_j, M)=1}} \frac{1}{n_j} = \frac{1}{p} \sum_{\substack{\frac{N}{pm_j} < t \leq \frac{KN}{pm_j} \\ \gcd(t, M)=1}} \frac{1}{t} \ll \frac{1}{p} \left(\frac{\log K}{\log Q} + 1 \right) = \frac{\log(QK)}{p \log Q}$$

for $j = 1, 2$. We have the estimate $\sum_{p>Q} p^{-2} \ll 1/(Q \log Q)$, which follows from the prime number theorem and partial summation. Thus,

$$\sum_{\substack{n_1 \in S_{m_1} \\ n_2 \in S_{m_2} \\ \gcd(n_1, n_2) > 1}} \frac{1}{n_1 n_2} \ll \frac{\log^2(QK)}{Q \log^3 Q},$$

so that

$$\frac{1}{M} \sum_{h=0}^{M-1} \beta(C_h) \ll \frac{s^2 \log^2(QK)}{Q \log^3 Q} \sum_{\substack{m_1 | M \\ m_2 | M}} \frac{1}{\text{lcm}[m_1, m_2]} = \frac{s^2 \log^2(QK)}{Q \log^3 Q} \sum_{m|M} \sum_{\substack{m_1 | M, m_2 | M \\ \text{lcm}[m_1, m_2] = m}} m^{-1}.$$

The double sum is equal to

$$\sum_{m|M} m^{-1} \tau(m^2) \leq \prod_{p \in P} \left(1 + \frac{3}{p} + \frac{5}{p^2} + \cdots\right) = \prod_{p \leq Q} \frac{1 + 1/p}{(1 - 1/p)^2} \ll \log^3 Q,$$

and this completes the proof. \square

Lemma 3.3. *Suppose that C is any residue system, $Q \geq 2$, P is the set of primes $\leq Q$, and define M and C_h as in Lemma 3.1. Also let $C' = \{(n, r) \in C : n|M\}$ and suppose $\delta(C') > 0$. Then*

$$\frac{1}{M} \sum_{h=0}^{M-1} \alpha(C_h) \geq (\alpha(C))^{(1+1/Q)/\delta(C')}.$$

Proof. Note that $1 \in S(C_h)$ if and only if there is a pair $(n, r) \in C'$ with $h \equiv r \pmod{n}$. Let

$$\mathcal{M}_0 = \{0 \leq h \leq M-1 : 1 \notin S(C_h)\}, \quad M_0 = |\mathcal{M}_0|.$$

Then

$$\frac{M_0}{M} = \delta(C'). \tag{3.2}$$

The hypothesis $\delta(C') > 0$ thus implies that $M_0 > 0$. Observe that $1 \in S(C_h)$ implies $\alpha(C_h) = 0$. By the inequality of the arithmetic and geometric means,

$$\begin{aligned} \frac{1}{M} \sum_{h=0}^{M-1} \alpha(C_h) &= \frac{1}{M} \sum_{h \in \mathcal{M}_0} \alpha(C_h) \geq \frac{M_0}{M} \left(\prod_{h \in \mathcal{M}_0} \alpha(C_h) \right)^{1/M_0} \\ &= \frac{M_0}{M} \left(\prod_{h \in \mathcal{M}_0} \prod_{n' \in S(C_h)} \left(1 - \frac{1}{n'}\right) \right)^{1/M_0}. \end{aligned}$$

Since $\log(1 - 1/k) > -\frac{1}{k}(1 + \frac{1}{k})$ for $k \geq 2$ and since each $n' > Q$, we have

$$1 - \frac{1}{n'} > \exp(-\lambda/n'), \quad \text{where } \lambda = 1 + 1/Q.$$

Thus,

$$\begin{aligned} \frac{1}{M} \sum_{h=0}^{M-1} \alpha(C_h) &\geq \frac{M_0}{M} \exp\left(-\frac{\lambda}{M_0} \sum_{h \in \mathcal{M}_0} \sum_{n' \in S(C_h)} \frac{1}{n'}\right) \\ &\geq \frac{M_0}{M} \exp\left(\frac{\lambda(M - M_0)}{M_0} - \frac{\lambda}{M_0} \sum_{h=0}^{M-1} \sum_{n' \in S(C_h)} \frac{1}{n'}\right), \end{aligned}$$

where the last inequality uses that $1 \in S(C_h)$ for $h \notin \mathcal{M}_0$.

Each pair $(n, r) \in C$ produces the pair $(n/\gcd(n, M), r)$ in exactly $M/\gcd(n, M)$ mulitsets C_h , namely for each $h \in [0, M - 1]$ satisfying $h \equiv r \pmod{\gcd(n, M)}$. Hence,

$$\sum_{h=0}^{M-1} \sum_{n' \in S(C_h)} \frac{1}{n'} = M \sum_{n \in S(C)} \frac{1}{n},$$

so that

$$\frac{1}{M} \sum_{h=0}^{M-1} \alpha(C_h) \geq \frac{M_0}{M} \exp\left(\frac{\lambda(M - M_0)}{M_0} - \frac{\lambda M}{M_0} \sum_{n \in S(C)} \frac{1}{n}\right).$$

Also, $(M_0/M) \exp((M - M_0)/M_0) \geq 1$. Thus,

$$\frac{1}{M} \sum_{h=0}^{M-1} \alpha(C_h) \geq \exp\left(-\frac{\lambda M}{M_0} \sum_{n \in S(C)} \frac{1}{n}\right) \geq (\alpha(C))^{\lambda M/M_0}.$$

The lemma follows by (3.2). □

We now combine our lemmas into one easily-applied statement.

Lemma 3.4. *Suppose $K > 1$, N is a positive integer, and C is a residue system with $S(C)$ consisting of integers in $(N, KN]$, each with multiplicity at most s . For each number $Q \geq 2$, let $C' = C'(Q) = \{(n, r) \in C : P(n) \leq Q\}$. If $\delta(C') > 0$, then*

$$\delta(C) \geq \alpha(C)^{(1+1/Q)/\delta(C')} + O\left(\frac{s^2 \log^2(QK)}{Q}\right),$$

where the implied constant is uniform in all parameters.

Proof. Let P be the set of primes $\leq Q$ and define M and C_h as in Lemma 3.1. By Lemmas 2.1, 3.1, 3.2, and 3.3, we have

$$\begin{aligned}\delta(C) &= \frac{1}{M} \sum_{h=0}^{M-1} \delta(C_h) \geq \frac{1}{M} \sum_{h=0}^{M-1} \alpha(C_h) - \frac{1}{M} \sum_{h=0}^{M-1} \beta(C_h) \\ &\geq \alpha(C)^{(1+1/Q)/\delta(C')} + O\left(\frac{s^2 \log^2(QK)}{Q}\right).\end{aligned}$$

Thus, we have the lemma. \square

4 Lower bounds on $\delta(C)$

In this section we prove stronger versions of Theorems A and B. The main results will involve absolute constants c_j which are of minor interest. Nevertheless, in each case, we indicate a specific value of c_j for which the stated result and subsequent proof follows.

We begin with a useful lemma about smooth numbers.

Lemma 4.1. *Suppose $Q \geq 2$ and $Q < N \leq \exp(\sqrt{Q})$. Then*

$$\sum_{\substack{n > N \\ P(n) \leq Q}} \frac{1}{n} \ll (\log Q) e^{-u \log u}, \quad \text{where } u = \frac{\log N}{\log Q}.$$

Proof. We use standard upper-bound estimates for the distribution of smooth numbers. Say n is Q -smooth if $P(n) \leq Q$. The number of Q -smooth numbers at most t is $\ll t/u_t^{u_t}$, where $u_t = \log t / \log Q$, provided $Q \leq t \leq \exp(Q^{1-\varepsilon})$ ([12], Theorem 1.2 and Corollary 2.3). Further, for $t > \exp(6\sqrt{Q})$, the Q -smooth numbers are distributed more sparsely than the squares. We thus have

$$\begin{aligned}\sum_{\substack{n > N \\ P(n) \leq Q}} \frac{1}{n} &= \int_N^\infty \frac{1}{t^2} \sum_{\substack{N < n \leq t \\ P(n) \leq Q}} 1 dt \leq \sum_{0 \leq i \leq 10\sqrt{Q}} \int_{N^i}^{N^{i+1}} \frac{1}{t^2} \sum_{\substack{n \leq t \\ P(n) \leq Q}} 1 dt + \int_{\exp(6\sqrt{Q})}^\infty \frac{1}{t^2} \sum_{\substack{n \leq t \\ P(n) \leq Q}} 1 dt \\ &\ll \sum_{i \geq 0} \frac{\log Q}{(u+i)^{u+i}} + \int_{\exp(6\sqrt{Q})}^\infty \frac{1}{t^{3/2}} dt \ll \frac{\log Q}{u^u},\end{aligned}$$

implying the lemma. \square

Let

$$L(N, s) = \exp\left(\log N \frac{\log \log(s \log N)}{\log(s \log N)}\right).$$

Theorem 2. Suppose $0 < b < \frac{1}{2}$, $0 < c < \frac{1}{3}(1 - 4b^2)$ and let N be sufficiently large, depending on the choice of b and c . Suppose C is a residue system with $S(C)$ consisting of integers $n > N$, each having multiplicity at most s , where $s \leq \exp(b\sqrt{\log N \log \log N})$, and such that

$$\sum_{n \in S(C)} \frac{1}{n} \leq c \log L(N, s). \quad (4.1)$$

Then $\delta(C) > 0$.

Proof. Throughout we assume N is sufficiently large, depending only on b and c . Let $\beta = \frac{1}{3}(1 - 4b^2)$ and put $\varepsilon = \frac{1}{20}(\beta - c)$. First, we have

$$-\log \alpha(C) \leq \sum_{n \in S(C)} \left(\frac{1}{n} + \frac{1}{n^2} \right) \leq \left(1 + \frac{1}{N} \right) \sum_{n \in S(C)} \frac{1}{n} \leq (c + \varepsilon) \log L(N, s) = G,$$

say. Define

$$Q_0 = L(N, s)^{1-\varepsilon}, \quad Q_j = \exp(Q_{j-1}^{\beta+\varepsilon}) \quad (j \geq 1) \quad (4.2)$$

and

$$K_j = \exp(Q_{j-1}^{\beta+2\varepsilon}) \quad (j \geq 1).$$

Let

$$C_j = \{(n, r) \in C : P(n) \leq Q_j\}.$$

Also, define

$$\delta_0 = 1 - \varepsilon, \quad \delta_j = e^{-1-G(1+1/Q_0)/\delta_{j-1}} \quad (j \geq 1), \quad (4.3)$$

where G is defined above. Since C is finite and Q_j tends to infinity with j , it follows that $C = C_j$ for large j . Thus, the theorem will follow if we show that

$$\delta(C_j) \geq \delta_j \quad (j \geq 0). \quad (4.4)$$

First, by Lemma 4.1,

$$1 - \delta(C_0) \leq s \sum_{\substack{n > N \\ P(n) \leq Q_0}} \frac{1}{n} \ll s(\log Q_0)e^{-u \log u}, \quad \text{where } u = \frac{\log N}{\log Q_0}.$$

By the definition of Q_0 , we have

$$u = \frac{\log(s \log N)}{(1 - \varepsilon) \log \log(s \log N)}$$

so that

$$u \log u \geq \left(\frac{1}{1-\varepsilon} - \varepsilon^2 \right) \log(s \log N) \geq (1+\varepsilon) \log(s \log N).$$

Hence, $\delta(C_0) \geq \delta_0$. Next, suppose $j \geq 1$ and $\delta(C_{j-1}) \geq \delta_{j-1}$. Observe that N large and $s \leq s_0 := \exp(b\sqrt{\log N \log \log N})$ imply

$$\frac{\log \log(s \log N)}{\log(s \log N)} \geq \frac{\log \log s_0}{\log(s_0 \log N)} \geq \frac{\log \log N}{2 \log(s_0 \log N)} \geq \frac{(1-\varepsilon) \log \log N}{2b\sqrt{\log N \log \log N}}.$$

Therefore,

$$s^2 \leq \exp(2b\sqrt{\log N \log \log N}) \leq L(N, s)^{4b^2/(1-\varepsilon)} = Q_0^{4b^2/(1-\varepsilon)^2} \leq Q_{j-1}^{4b^2(1+3\varepsilon)}.$$

Let

$$C'_j = \{(n, r) \in C_j : n \leq K_j\}, \quad C''_j = \{(n, r) \in C_j : n > K_j\}.$$

Observe that

$$\delta(\{(n, r) \in C'_j : P(n) \leq Q_{j-1}\}) \geq \delta(C_{j-1}) \geq \delta_{j-1} \quad \text{and} \quad \alpha(C'_j) \geq \alpha(C) \geq e^{-G}.$$

By Lemma 3.4 with $Q = Q_{j-1}$ and $K = K_j/N$, there is an absolute constant D such that

$$\begin{aligned} \delta(C'_j) &\geq \alpha(C'_j)^{(1+1/Q_{j-1})/\delta_{j-1}} - D \frac{s^2 \log^2(Q_{j-1} K_j)}{Q_{j-1}} \\ &\geq e^{-G(1+1/Q_0)/\delta_{j-1}} - Q_{j-1}^{-1+4b^2(1+3\varepsilon)+2\beta+5\varepsilon} \geq 2\delta_j - Q_{j-1}^{-\beta+8\varepsilon}. \end{aligned} \tag{4.5}$$

Also, by Lemma 4.1,

$$1 - \delta(C''_j) \leq s \sum_{\substack{n > K_j \\ P(n) \leq Q_j}} \frac{1}{n} \ll s(\log Q_j) e^{-u_j \log u_j}, \tag{4.6}$$

where

$$u_j = \frac{\log K_j}{\log Q_j} = Q_{j-1}^\varepsilon.$$

Thus, $1 - \delta(C''_j) \leq Q_{j-1}^{-1}$. Together with (4.5), this implies

$$\delta(C_j) \geq \delta(C'_j) - (1 - \delta(C''_j)) \geq 2\delta_j - Q_{j-1}^{-\beta+9\varepsilon}. \tag{4.7}$$

To complete the proof of (4.4) and the theorem, it suffices to prove that

$$Q_{j-1}^{-\beta+9\varepsilon} \leq \delta_j \quad (j \geq 1). \tag{4.8}$$

First,

$$Q_0^{-\beta+9\epsilon} = L(N, s)^{(-\beta+9\epsilon)(1-\epsilon)} \leq L(N, s)^{-\beta+10\epsilon} = L(N, s)^{-c-10\epsilon},$$

while

$$\delta_1 \geq e^{-1-G(1+1/Q_0)(1+1.1\epsilon)} \geq L(N, s)^{-c-2\epsilon}.$$

This proves (4.8) when $j = 1$. Suppose (4.8) holds for some $j \geq 1$. Since $G \leq \log Q_0$, we have

$$-\log \delta_{j+1} = 1 + G(1 + 1/Q_0)/\delta_j \leq 2GQ_{j-1}^{\beta-9\epsilon} < Q_{j-1}^{\beta-8\epsilon}.$$

And, by (4.2), we have $-\log(Q_j^{-\beta+9\epsilon}) \gg Q_{j-1}^{\beta+\epsilon}$. Thus, $Q_j^{-\beta+9\epsilon} \leq \delta_{j+1}$ and by induction (4.8) holds for all j . This completes our proof. \square

Theorem 2 implies Theorem A of the introduction by setting $s = 1$. Observe that the bound on the sum in Theorem 2 given in (4.1) decreases as s increases. If one is interested in a result similar to Theorem A but with an emphasis on allowing the multiplicity of the moduli to be large, one may take b arbitrarily close to $1/2$ in Theorem 2.

Theorem 2 should be compared with Theorem 5 of the next section which shows that coverings, even exact coverings with squarefree moduli, exist when we allow the multiplicity of the moduli to be of size $\exp(\sqrt{\log N \log \log N})$.

We can also consider the case that $S(C)$ consists of integers from $(N, KN]$ with multiplicities at most $s \leq \exp(b\sqrt{\log N \log \log N})$, where $b < \sqrt{3\epsilon/4}$. If $0 < \epsilon < 1/3$, N is large, and $K = L(N, s)^{(1/3-\epsilon)/s}$, then Theorem 2 implies that $\delta(C) > 0$. By a different argument, we can extend the range of K a bit.

Theorem 3. *Suppose $0 < \epsilon < (1 - \log 2)^{-1}$, $b < \frac{1}{2}\sqrt{(1 - \log 2)\epsilon}$ and N is sufficiently large, depending on the choice of ϵ and b . Suppose that C is a residue system with $S(C)$ consisting of integers from $(N, KN]$ with multiplicity at most s , where $s \leq \exp(b\sqrt{\log N \log \log N})$ and $K = L(N, s)^{((1-\log 2)^{-1}-\epsilon)/s}$. Then $\delta(C) > 0$.*

Note that for $s \geq \log N$, $K = 1 + o(1)$. Before proving Theorem 3, we present a lemma.

Lemma 4.2. *Suppose s is a positive integer and C is a residue system with $S(C)$ consisting of integers from $(1, B]$ with multiplicity at most s . Let*

$$C_0 = \{(n, r) \in C : P(n) \leq \sqrt{sB}\}.$$

If $\delta(C_0) > 0$, then $\delta(C) > 0$.

Proof. Suppose that $\delta(C_0) > 0$. Denote by P the product of all primes in $(\sqrt{sB}, B]$, and let L be the least common multiple of the elements of $S(C_0)$.

Let p be a prime divisor of P . Since $p > \sqrt{sB}$ implies $sB/p < p$, there are at most $p - 1$ multiples of p in the multiset $S(C)$. Call them m_1, \dots, m_t , and let r_1, \dots, r_t be the corresponding residue classes. Then there is a choice for $b = b(p) \in \{0, 1, \dots, p - 1\}$ such that each integer satisfying $x \equiv b \pmod{p}$ is not covered by (i.e., does not satisfy) any of the congruences $x \equiv r_j \pmod{m_j}$ with $1 \leq j \leq t$.

By assumption, there is a residue class $a \pmod{L}$ contained in $R(C_0)$. Let A be a solution to the Chinese remainder system $A \equiv a \pmod{L}$ and $A \equiv b(p) \pmod{p}$ for each prime p dividing P . Then not only do we have $A \not\equiv r \pmod{n}$ for each $(n, r) \in C_0$, we also have for each prime $p \mid P$ and $(n, r) \in C$ with $p \mid n$, that $A \not\equiv r \pmod{n}$. Since this exhausts the pairs $(n, r) \in C$, we have $A \in R(C)$, so we have the lemma. \square

Proof of Theorem 3. We may suppose that $\varepsilon > 0$ is sufficiently small and $K \geq 2$. Let C_0 be as in Lemma 4.2 where we take $B = KN$. Then

$$\begin{aligned} \sum_{n \in S(C_0)} \frac{1}{n} &\leq s \sum_{\substack{N < n \leq KN \\ P(n) \leq \sqrt{sKN}}} \frac{1}{n} = s \sum_{N < n \leq KN} \frac{1}{n} - s \sum_{\substack{N < n \leq KN \\ P(n) > \sqrt{sKN}}} \frac{1}{n} \\ &= s \log K + O(s/N) - s \sum_{\sqrt{sKN} < p \leq KN} \frac{1}{p} \sum_{N/p < m \leq KN/p} \frac{1}{m}. \end{aligned}$$

Now,

$$\sum_{N/p < m \leq KN/p} \frac{1}{m} = \begin{cases} \log K + O(p/N), & p \leq N \\ \log(KN/p) + O(1), & N < p \leq KN. \end{cases}$$

Thus,

$$\begin{aligned} &\sum_{\sqrt{sKN} < p \leq KN} \frac{1}{p} \sum_{N/p < m \leq KN/p} \frac{1}{m} \\ &= \sum_{\sqrt{sKN} < p \leq N} \left(\frac{\log K}{p} + O(1/N) \right) + \sum_{N < p \leq KN} \left(\frac{\log K}{p} + \frac{\log N - \log p + O(1)}{p} \right) \\ &= \sum_{\sqrt{sKN} < p \leq KN} \frac{\log K}{p} + \sum_{N < p \leq KN} \frac{\log N - \log p}{p} + O(\log K / \log N) \\ &= \log 2 \log K + O\left(\frac{\log K \log(sK)}{\log N} \right) = (\log 2 + o(1)) \log K. \end{aligned}$$

Hence, since $-\log \alpha(C_0) \leq \sum_{n \in S(C_0)} 1/n + O(s/N)$, we have

$$-\log \alpha(C_0) \leq s(1 - \log 2 + o(1)) \log K \leq (1 - (1 - \log 2)\varepsilon + o(1)) \log L(N, s).$$

Let $Q = L(N, s)^{1-\beta}$, where $\beta = \frac{1}{4}((1 - \log 2)\varepsilon - 4b^2)$. Also let $C' = \{(n, r) \in C_0 : P(n) \leq Q\}$. As before, using Lemma 4.1 yields

$$\delta(C') = 1 + O\left(s \sum_{\substack{n > N \\ P(n) \leq Q}} \frac{1}{n}\right) = 1 + o(1) \quad (N \rightarrow \infty).$$

Hence,

$$\alpha(C_0)^{(1+1/Q)/\delta(C')} \gg L(N, s)^{-1+(1-\log 2)\varepsilon-\beta}.$$

On the other hand,

$$\frac{s^2 \log^2(QK)}{Q} \ll L(N, s)^{-1+4b^2+2\beta}.$$

By Lemma 3.4, we have $\delta(C_0) > 0$ for N sufficiently large. Thus, $\delta(C) > 0$ by Lemma 4.2. \square

We now show that if K is a bit smaller than in Theorem 3, then in fact

$$\delta(C) \geq (1 + o(1))\alpha(C).$$

The following result generalizes Theorem B from the introduction.

Theorem 4. *Suppose $0 < \varepsilon < 1/2$, $0 < b < \frac{1}{2}\sqrt{\varepsilon}$ and $N \geq 100$. Suppose that C is a residue system with $S(C)$ consisting of integers from $(N, KN]$ with multiplicity at most s , where $s \leq \exp(b\sqrt{\log N \log \log N})$ and $K = L(N, s)^{(1/2-\varepsilon)/s}$. Then*

$$\delta(C) \geq \left(1 + O\left(\frac{1}{(\log N)^\beta}\right)\right) \alpha(C),$$

where β is a positive constant depending only on ε and b .

Proof. We follow the same general plan as in the proof of Theorem 2. Since the sum of $1/n$ for all $n \in (N, KN]$ is $\log K + O(1/N)$ we have

$$\alpha(C) \gg L(N, s)^{-1/2+\varepsilon}.$$

Let $Q = L(N, s)^{1/2-\beta}$, where $\beta = \frac{1}{3}(\varepsilon - 4b^2)$. In particular $Q \geq \log^2 N$. Let $u = \log N / \log Q$, and let C' be as in Lemma 3.4. By Lemma 4.1, we have

$$1 - \delta(C') \ll \frac{s \log Q}{u^u} \ll \frac{s \log N}{(s \log N)^{2+\beta}},$$

so that $1/\delta(C') = 1 + O((s \log N)^{-1-\beta})$. Since $|\log \alpha(C)| \leq \log N$, we have

$$\alpha(C)^{(1+1/Q)/\delta(C')} = (1 + O(1/(\log N)^\beta))\alpha(C).$$

So, by Lemma 3.4 it suffices to show that $s^2(\log QK)^2/Q = O(\alpha(C)(\log N)^{-\beta})$. But, for large N we have $s^2 \leq L(N, s)^{4b^2+\beta}$. Thus,

$$\frac{s^2(\log QK)^2}{Q} \ll \frac{s^2 \log^2 L(N, s)}{L(N, s)^{1/2-\beta}} \ll \frac{1}{L(N, s)^{1/2-2\beta-4b^2}} \ll \frac{1}{L(N, s)^{1/2-\varepsilon+\beta}} \ll \frac{\alpha(C)}{L(N, s)^\beta}.$$

This completes the proof. \square

5 Coverings and near-coverings of the integers

In this section, we address two items. The first shows that there are coverings of the integers with the moduli bounded below by N and the multiplicity of the moduli *near* the upper bound on the multiplicity of the moduli given by Theorem 2. The second shows that, when we allow K to be large, the density of the integers which are not covered by a covering system using distinct moduli from $(N, KN]$ can be considerably smaller than what is suggested by Theorem 4.

Theorem 5. *For sufficiently large N and $s = \exp(\sqrt{\log N \log \log N})$, there exists an exact covering system with squarefree moduli greater than N such that the multiplicity of each modulus does not exceed s .*

Proof. Let p denote a prime and let $X_j = (j+1)^{j+1}$ for $j = 0, 1, \dots$. We first show that

$$\sum_{X_{j-1} < p \leq X_j} [X_j/p] \geq X_{j-1} \quad (j \geq 1). \quad (5.1)$$

Here $[x]$ denotes the largest integer which is $\leq x$. Note that (5.1) holds for $j \leq 5$. Suppose then that $j \geq 6$. Using the estimates (3.4), (3.17), and (3.18) in Rosser and Schoenfeld [14], we have that

$$\begin{aligned} \sum_{X_{j-1} < p \leq X_j} [X_j/p] &\geq X_j \sum_{X_{j-1} < p \leq X_j} 1/p - \pi(X_j) \\ &\geq X_j \left(\log \frac{\log X_j}{\log X_{j-1}} - \frac{1}{\log^2 X_{j-1}} - \frac{1}{\log X_j - \frac{3}{2}} \right). \end{aligned}$$

The expression in the parentheses is

$$\log \frac{(j+1) \log(j+1)}{j \log j} - \frac{1}{j^2 \log^2 j} - \frac{1}{(j+1) \log(j+1) - \frac{3}{2}}$$

$$> \frac{1}{j+1} \left(\frac{j+1}{j} - \frac{j+1}{2j^2} - \frac{j+1}{j^2 \log^2 j} - \frac{1}{\log(j+1) - 3/(2j+2)} \right) > \frac{0.43}{j+1}.$$

And $X_j = (j+1)j^j(1+1/j)^j > 2.5(j+1)j^j$. Thus,

$$\sum_{X_{j-1} < p \leq X_j} [X_j/p] > \frac{2.5(j+1)0.43}{j+1} j^j > j^j,$$

which proves (5.1).

We describe now an explicit construction of a covering system, which we will then show satisfies the conditions of the theorem. For $J \geq 1$ and $s = X_J$, we establish that there exists an exact covering system C_J with squarefree moduli greater than

$$N_J = \prod_{j=0}^{J-1} X_j$$

such that the multiplicity of each modulus does not exceed s . Set

$$P_j = \{p : X_{j-1} < p \leq X_j\}.$$

We construct C_J , through induction on J , by choosing moduli of the form $p_1 \cdots p_J$ where each $p_j \in P_j$. Observe that such a product $p_1 \cdots p_J$ is necessarily $> N_J$. One checks that $C_1 = \{(2, 0), (2, 1)\}$ satisfies the conditions for C_J with $J = 1$. Now, suppose that we have C_J as above for some $J \geq 1$. Thus, we have an exact covering system C_J with moduli of the form $p_1 \cdots p_J$ where each $p_j \in P_j$. Fix such a modulus $n = p_1 \cdots p_J$, and let $(n, r_1), \dots, (n, r_t)$, with $t \leq X_J$, be the pairs of the form (n, r) in C_J . Let $q_1 < q_2 < \dots$ be the complete list of primes from P_{J+1} . To construct C_{J+1} , we replace each pair (n, r_i) , $i \leq [X_{J+1}/q_1]$, with the q_1 pairs $(nq_1, r_i + n\mu)$, where $\mu = 0, \dots, q_1 - 1$. Notice that the multiplicity of the modulus nq_1 is at most $[X_{J+1}/q_1]q_1 \leq X_{J+1}$. Next, we replace each pair (n, r_i) , $[X_{J+1}/q_1] < i \leq [X_{J+1}/q_1] + [X_{J+1}/q_2]$, with the q_2 pairs $(nq_2, r_i + n\mu)$, where $\mu = 0, \dots, q_2 - 1$. We proceed with this construction until all the pairs $(n, r_1), \dots, (n, r_t)$ are replaced with new pairs. As $t \leq X_J$, this will happen at some point by (5.1). This completes the inductive construction of our exact covering systems C_J .

To complete the proof of the theorem, it suffices to show that $\log N_J \log \log N_J \geq \log^2 s$ for large J . Now

$$\log N_J = \sum_{j=1}^J j \log j \geq \int_1^J t \log t dt > \frac{1}{2} J^2 \log J - \frac{1}{4} J^2,$$

so that

$$\log \log N_J > 2 \log J + \log \log J - \log 2 + \log(1 - 1/(2 \log J)) > 2 \log J + \log \log J - 1,$$

for $J \geq 7$. Thus,

$$\log N_J \log \log N_J > J^2 \log^2 J + \frac{1}{2} J^2 \log J \left(\log \log J - 1.5 - \frac{\log \log J}{2 \log J} \right) > J^2 \log^2 J + 3J \log^2 J,$$

for $J \geq 350$. But $\log^2 s = (J+1)^2 \log^2(J+1) < J^2 \log^2 J + 3J \log^2 J$ in the same range. This completes the proof of the theorem. \square

Remark 3. A more elementary proof, that does not use the estimates from [14], is possible by defining the sequence X_j inductively as the minimal numbers for which (5.1) holds.

Suppose $s = 1$ and N, KN are integers in Theorem 4. Then $S(C)$ consists of distinct integers chosen from $(N, KN]$ so that

$$\alpha(C) \geq \prod_{j=N+1}^{KN} \left(1 - \frac{1}{j} \right) = \frac{1}{K}.$$

Thus, Theorem 4 implies a lower bound of approximately $1/K$ for any $\delta(C)$ with $S(C) \subseteq (N, KN]$, provided K is not too large. It is clear that the expression $1/K$ is not far from the truth, since the argument of the introduction gives a residue system C with $\delta(C) \leq 1/K$. However, we might ask about the situation when K is large compared to N . The following result shows that $\delta(C)$ can in fact be considerably smaller than $1/K$ when K is much larger than N .

Theorem 6. *Suppose N and K are integers with $N \geq 1$ and K sufficiently large. Then there is some residue system C consisting of distinct moduli from $(N, KN]$ such that*

$$\delta(C) \leq \frac{1}{K} \exp \left(-\frac{\log K}{3N} \right).$$

Before giving a proof of the above theorem, we give a lemma that will also play a role in the next section. For a multiset T of positive integers, we let $\mathcal{C}(T)$ be the set of residue systems C with $S(C) = T$ and where $(n, r) \in C$ implies $1 \leq r \leq n$. Also, define

$$W(T) = \#\mathcal{C}(T) = \prod_{n \in T} n.$$

Lemma 5.1. *Let T be a multiset of positive integers. Then the expected value of $\delta(C)$ over $C \in \mathcal{C}(T)$, denoted $\mathbf{E}\delta(C)$, is $\alpha(C)$.*

Proof. Put $W = W(T)$ and say $1 \leq m \leq W$. The number of systems $C \in \mathcal{C}(T)$ with $m \in R(C)$ is $\prod_{n \in T} (n - 1)$, since for each $n \in T$, there are $n - 1$ choices for r with $1 \leq r \leq n$ and $r \not\equiv m \pmod{n}$. Thus,

$$\begin{aligned} \sum_{C \in \mathcal{C}(T)} \delta(C) &= \sum_{C \in \mathcal{C}(T)} \frac{1}{W} \sum_{\substack{1 \leq m \leq W \\ m \in R(C)}} 1 = \frac{1}{W} \sum_{m=1}^W \sum_{\substack{C \in \mathcal{C}(T) \\ m \in R(C)}} 1 \\ &= \frac{1}{W} \sum_{m=1}^W \prod_{n \in T} (n - 1) = \prod_{n \in T} (n - 1). \end{aligned}$$

The result follows by dividing this equation by W . \square

Proof of Theorem 6. There is a known covering system with distinct moduli and smallest modulus 24 (a result of Morikawa; see [13]), so Theorem 6 follows for $N \leq 23$. Henceforth we assume that $N \geq 24$. We shall construct a residue system $C = \{(n, r(n)) : N < n \leq KN\}$ as follows. We will randomly choose the values of $r(n) \in [1, n]$ for $N < n \leq 2N$ so that each residue class modulo n is taken with the same probability $1/n$ and the variables $r(n)$ are independent. Based on the random choice of such $r(n)$ for $N < n \leq 2N$, we then select the remaining values of $r(n)$ with $2N < n \leq KN$ via a greedy algorithm. In fact, we show that, under our construction, the expected value of $\delta(C)$ over all randomly chosen values of $r(n) \in [1, n]$ for $N < n \leq 2N$ is

$$\leq \frac{1}{K} \exp\left(-\frac{\log K}{3N}\right).$$

The result will follow.

Let $C_{2N} = \{(n, r(n)) : N < n \leq 2N\}$, where each $r(n)$ is chosen randomly from $[1, n]$. From Lemma 5.1, it follows that $\mathbf{E}\delta(C_{2N}) = 1/2$. Hence, by the arithmetic mean–geometric mean inequality,

$$\mathbf{E} \log \delta(C_{2N}) \leq -\log 2. \quad (5.2)$$

We will also make use of Lemma 5.1 in another way. If D is a subset of the integers in $(N, 2N]$ and $\tilde{C} = \{(d, r(d)) : d \in D\}$, then it is not difficult to see that the expected value of $\delta(\tilde{C})$ over all randomly chosen values of $r(d) \in [1, d]$ for $d \in D$ is the same as the expected value of $\delta(\tilde{C})$ over all randomly chosen values of $r(n) \in [1, n]$ for $n \in (N, 2N]$; in other words, the random selection of extra residue classes not associated with \tilde{C} will not affect the expected value $\delta(\tilde{C})$. Thus, Lemma 5.1 implies $\mathbf{E}\delta(\tilde{C}) = \alpha(\tilde{C})$ where the expected value is over all randomly chosen $r(n) \in [1, n]$ for $N < n \leq 2N$.

Suppose then that the values of $r(n) \in [1, n]$ for $N < n \leq 2N$ have been chosen randomly. For $2N < j \leq KN$, we describe how to select $r(j)$. For this purpose, we set $C_j = \{(n, r(n)) : N <$

$n \leq j\}$. We use the greedy algorithm to choose $r(j)$ to be a residue class modulo j containing the largest proportion of $R(C_{j-1})$. As in the introduction, this gives trivially

$$\delta(C_j) \leq \left(1 - \frac{1}{j}\right) \delta(C_{j-1}).$$

We can sometimes do better. If j has a divisor d with $N < d \leq 2N$, then there are residue classes modulo j not intersecting $R(C_{j-1})$. In particular, the residue class $r(d) \pmod{d}$ contains $r \pmod{j}$ when $r \equiv r(d) \pmod{d}$. Let

$$D(j) = \{d : d|j, N < d \leq 2N\}, \quad \tilde{C}_j = \{(d, r(d)) : d \in D(j)\}.$$

Let $f(j)$ be the number of residue classes $r \pmod{j}$ for which $r \not\equiv r(d) \pmod{d}$ for each $d \in D(j)$. If we choose $r(j)$ appropriately from among these $f(j)$ choices for r , we have

$$\delta(C_j) \leq \left(1 - \frac{1}{f(j)}\right) \delta(C_{j-1}). \quad (5.3)$$

The last equality is nonsense if $f(j) = 0$, but in that case we have $R(C_{j-1}) = \emptyset$, and the theorem is trivial. Also, there is nothing to prove if $f(j) = 1$ since then $R(C_j) = \emptyset$. Throughout the following we assume that $f(j) > 1$.

We see from (5.3) and linearity of expectation that

$$\mathbf{E} \log \delta(C_j) - \mathbf{E} \log \delta(C_{j-1}) \leq \mathbf{E} \log \left(1 - \frac{1}{f(j)}\right) \leq -\mathbf{E} \left(\frac{1}{f(j)}\right). \quad (5.4)$$

Using Lemma 5.1 as described above, we have

$$\mathbf{E} \delta(\tilde{C}_j) = \prod_{d \in D(j)} \left(1 - \frac{1}{d}\right).$$

Since j is a common multiple of the members of $D(j)$, it follows that $\delta(\tilde{C}_j) = f(j)/j$, so that

$$\mathbf{E} f(j) = j \mathbf{E} \delta(\tilde{C}_j) = j \prod_{d \in D(j)} \left(1 - \frac{1}{d}\right).$$

By the arithmetic mean-harmonic mean inequality, we thus have

$$\mathbf{E} \left(\frac{1}{f(j)}\right) \geq j^{-1} \prod_{d \in D(j)} \left(1 - \frac{1}{d}\right)^{-1} \geq \frac{1}{j} + \sum_{d \in D(j)} \frac{1}{dj}.$$

After substituting the last inequality into (5.4), we get

$$\mathbf{E} \log \delta(C_j) - \mathbf{E} \log \delta(C_{j-1}) \leq -\frac{1}{j} - \sum_{d \in D(j)} \frac{1}{dj}.$$

Thus,

$$\begin{aligned} \mathbf{E} \log \delta(C) - \mathbf{E} \log \delta(C_{2N}) &\leq - \sum_{j=2N+1}^{KN} \frac{1}{j} - \sum_{j=2N+1}^{KN} \sum_{d \in D(j)} \frac{1}{dj} \\ &= - \sum_{j=2N+1}^{KN} \frac{1}{j} - \sum_{d=N+1}^{2N} \sum_{2N/d < l \leq KN/d} \frac{1}{d^2 l} \\ &= -\log(K/2) + O(1/N) - \sum_{d=N+1}^{2N} \frac{\log K + O(1)}{d^2} \end{aligned}$$

We have for $N \geq 4$ the estimate

$$\sum_{d=N+1}^{2N} \frac{1}{d^2} \geq \int_{N+1}^{2N+1} \frac{dt}{t^2} = \frac{N}{(N+1)(2N+1)} \geq \frac{1}{2.9N}.$$

Therefore, by (5.2),

$$\mathbf{E} \log \delta(C) \leq -\log K - \frac{\log K + O(1)}{2.9N}$$

The theorem now follows. \square

6 Normal value of $\delta(C)$

It is reasonable to expect that $\delta(C) \approx \alpha(C)$ for almost all residue systems C with fixed $S(C)$. In this section, we establish such a result when $S(C)$ consists of distinct integers, by considering the variance of $\delta(C)$ over $C \in \mathcal{C}(T)$, where, as before, $\mathcal{C}(T)$ is the set of residue systems C with $S(C) = T$.

Theorem 7. *Let T be a set of distinct positive integers with minimum element $N \geq 3$. Let α be the common value of $\alpha(C)$ for $C \in \mathcal{C}(T)$. Then,*

$$\frac{1}{W(T)} \sum_{C \in \mathcal{C}(T)} |\delta(C) - \alpha|^2 \ll \frac{\alpha^2 \log N}{N^2}.$$

Proof. From Lemma 5.1, we have $\mathbf{E}\delta(C) = \alpha(C) = \alpha$. Writing $W = W(T)$, we deduce then that

$$\frac{1}{W} \sum_{C \in \mathcal{C}(T)} |\delta(C) - \alpha|^2 = \frac{1}{W} \sum_{C \in \mathcal{C}(T)} (\delta(C)^2 - \alpha^2). \quad (6.1)$$

We have

$$\sum_{C \in \mathcal{C}(T)} \delta(C)^2 = \sum_{C \in \mathcal{C}(T)} \left(\frac{1}{W} \sum_{\substack{1 \leq m \leq W \\ m \in R(C)}} 1 \right)^2 = \frac{1}{W^2} \sum_{1 \leq m_1, m_2 \leq W} \sum_{\substack{C \in \mathcal{C}(T) \\ m_1, m_2 \in R(C)}} 1.$$

As in the proof of Lemma 5.1, the inner sum is

$$\begin{aligned} & \prod_{\substack{n \in T \\ m_1 \equiv m_2 \pmod{n}}} (n-1) \prod_{\substack{n \in T \\ m_1 \not\equiv m_2 \pmod{n}}} (n-2) = W \prod_{n \in T} \left(1 - \frac{2}{n}\right) \prod_{\substack{n \in T \\ m_1 \equiv m_2 \pmod{n}}} \frac{n-1}{n-2} \\ & = \alpha^2 W \prod_{n \in T} \frac{1 - \frac{2}{n}}{\left(1 - \frac{1}{n}\right)^2} \prod_{\substack{n \in T \\ n | (m_1 - m_2)}} \frac{n-1}{n-2} = \alpha^2 W \prod_{n \in T} \left(1 - \frac{1}{(n-1)^2}\right) \prod_{\substack{n \in T \\ n | (m_1 - m_2)}} \frac{n-1}{n-2}. \end{aligned}$$

Let $u = \sum_{n \in T} 1/n^2$ and note that $u \ll 1/N$. Also, define

$$f(m_1, m_2) = \prod_{\substack{n \in T \\ n | (m_1 - m_2)}} \frac{n-1}{n-2}.$$

Thus,

$$\sum_{C \in \mathcal{C}(T)} \delta(C)^2 = \frac{\alpha^2}{W} \left(1 - u + O\left(\frac{1}{N^2}\right)\right) \sum_{1 \leq m_1, m_2 \leq W} f(m_1, m_2). \quad (6.2)$$

For S a finite set of integers which are ≥ 3 , let $M(S)$ denote $\prod_{n \in S} (n-2)$, and let $L(S)$ denote the least common multiple of the members of S . We have

$$f(m_1, m_2) = \prod_{\substack{n \in T \\ n | (m_1 - m_2)}} \left(1 + \frac{1}{n-2}\right) = \sum_{\substack{S \subseteq T \\ L(S) | (m_1 - m_2)}} \frac{1}{M(S)}.$$

Thus,

$$\sum_{1 \leq m_1, m_2 \leq W} f(m_1, m_2) = \sum_{S \subseteq T} \frac{1}{M(S)} \sum_{\substack{1 \leq m_1, m_2 \leq W \\ L(S) | (m_1 - m_2)}} 1 = W^2 \sum_{S \subseteq T} \frac{1}{M(S)L(S)}. \quad (6.3)$$

We consider in this last sum the terms with $\#S \leq 1$ and the remaining terms with $\#S \geq 2$. We have

$$\sum_{\substack{S \subseteq T \\ \#S \leq 1}} \frac{1}{M(S)L(S)} = 1 + \sum_{n \in T} \frac{1}{(n-2)n} = 1 + u + O(1/N^2). \quad (6.4)$$

If $S \subseteq T$ and $\#S \geq 2$, let $k > h$ be the largest two members of S . Then $L(S) \geq \text{lcm}[h, k] = hk / \text{gcd}(h, k)$, so that

$$E := \sum_{\substack{S \subseteq T \\ \#S \geq 2}} \frac{1}{M(S)L(S)} \leq \sum_{k > h \geq N} \frac{\text{gcd}(h, k)}{(h-2)(k-2)hk} \sum_{U \subseteq [N, h-1]} \frac{1}{M(U)}.$$

The inner sum here is identical to $\prod_{N \leq n \leq h-1} (n-1)/(n-2) = (h-2)/(N-2)$, so that

$$E \ll \frac{1}{N} \sum_{k > h \geq N} \frac{\text{gcd}(h, k)}{hk^2} \leq \frac{1}{N} \sum_{d \geq 1} \sum_{\substack{k > h \geq N \\ d|h, d|k}} \frac{d}{hk^2} = \frac{1}{N} \sum_{d \geq 1} \sum_{v > u \geq N/d} \frac{1}{d^2 uv^2} \ll \frac{1}{N} \sum_{d \geq 1} \sum_{u \geq N/d} \frac{1}{d^2 u^2}.$$

In this last double sum, if $d \leq N$, then the sum on u is $\ll d/N$, so that the contribution to E is $\ll (\log N)/N^2$. And if $d > N$, the sum on u is $\ll 1$, so that the contribution to E is $\ll 1/N^2$. We conclude that $E \ll (\log N)/N^2$. Thus, with (6.3) and (6.4) we have

$$\sum_{1 \leq m_1, m_2 \leq W} f(m_1, m_2) = W^2 (1 + u + O((\log N)/N^2)),$$

so that from (6.2) we get

$$\sum_{C \in \mathcal{C}(T)} \delta(C)^2 = \alpha^2 W (1 + O((\log N)/N^2)).$$

The result now follows immediately from (6.1). □

References

- [1] S. J. Benkoski and P. Erdős, *On weird and pseudoperfect numbers*, Math. Comp. **28** (1974), 617–623.
- [2] P. Erdős, *A generalization of a theorem of Besicovitch*, J. London Math. Soc. **11** (1936), 92–98.

- [3] P. Erdős, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.
- [4] P. Erdős, *Problems and results in combinatorial number theory*, A survey of combinatorial theory, eds. J. N. Srivastava, North-Holland, Amsterdam, 1973, 117–138.
- [5] P. Erdős, *Some of my favourite problems in number theory, combinatorics, and geometry*, Combinatorics Week (Portuguese) (São Paulo, 1994), Resenhas **2** (1995), no. 2, 165–186.
- [6] P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique, No. 28, 1980.
- [7] K. Ford, *The distribution of integers with a divisor in a given interval*, preprint.
- [8] R. K. Guy, *Unsolved problems in number theory*, 3rd ed. Problem Books in Mathematics. Springer-Verlag, New York, 2004.
- [9] J. A. Haight, *Covering systems of congruences, a negative result*, Mathematika **26** (1979), 53–61.
- [10] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, 1974.
- [11] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge University Press, 1988.
- [12] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. de Théorie des Nombres de Bordeaux, **5** (1993), 411–484.
- [13] S. Porubský and J. Schönheim, *Covering systems of Paul Erdős: Past, present and future*, in Paul Erdős and his mathematics, vol. I, János Bolyai Math. Soc., Budapest, 2002, pp. 581–627.
- [14] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.