MAXIMAL SETS OF INTEGERS WITH DISTINCT DIVISORS

R. Balasubramanian and K. Soundararajan

Institute for Mathematical Sciences, Tharamani P. O., Madras 600 113, India.
Department of Mathematics, Princeton University, Princeton, N. J. 08544, U.S.A.

Submitted: May 23, 1995; Accepted October 22, 1995

Abstract. A set of positive integers is said to have the *distinct divisor property* if there is an injective map that sends every integer in the set to one of its proper divisors. In 1983, P. Erdős and C. Pomerance showed that for every $c > 1$, a largest subset of $[N, cN]$ with the distinct divisor property has cardinality $\sim \delta(c)N$, for some constant $\delta(c) > 0$. They conjectured that $\delta(c) \sim c/2$ as $c \to \infty$. We prove their conjecture. In fact we show that there exist positive absolute constants D_1, D_2 such that $D_1 \leq c^{\beta}(c/2 - \delta(c)) \leq D_2$ where $\beta = \log 2/\log(3/2)$.

1. Introduction

Let S denote a set of positive integers and $\tau : S \to \mathbb{N}$ be defined so that $\tau(s)$ is a proper divisor of s (that is, $\tau(s)$ divides s and $\tau(s) < s$). The ensemble (S, τ) is said to have the '*distinct divisor property*' if τ is injective, that is, if the $\tau(s)$ are different for different values of s. We will also say that S has the distinct divisor property if there exists a τ, as above, such that (S, τ) has the distinct divisor property.

Let $c > 1$ denote a real number and N a large natural number. Let S be a subset of $[N, cN]$ with the distinct divisor property such that, of all subsets of $[N, cN]$ having distinct divisors, S has maximal cardinality. If c is fixed and N tends to infinity then P. Erdős and C. Pomerance, [1], have shown that

$$|S| = (\delta(c) + o(1))N$$

where $\delta(c)$ is a continuous increasing function of c. As c tends to 1 they established that

$$\delta(c) = c - 1 + o(1).$$

In this note we are concerned with the behaviour of $\delta(c)$ as c tends to infinity. Division by 2 clearly invests the set of even integers in $[N, cN]$ with the distinct divisor property; hence $\delta(c) \geq (c-1)/2$. Also, since a proper divisor of an integer less than cN is less than $cN/2$ clearly $\delta(c) \leq c/2$. Erdős and Pomerance conjectured that this latter upper bound is actually the truth for large c. In other words they conjectured that as c tends to infinity

$$\delta(c) = \frac{c}{2} + o(1).$$

1991 *Mathematics Subject Classification.* Primary 11A05.

Typeset by $\mathcal{AMS}$-TEX

We prove this and more by finding the exact order of magnitude for $c/2-\delta(c)$ as $c\to\infty$.

Theorem 1. *There exist positive absolute constants D_1 and D_2 such that*

$$\frac{D_1}{c^\beta}\le\frac{c}{2}-\delta(c)\le\frac{D_2}{c^\beta},$$

where $\beta=\log 2/\log(3/2)=1.7095\ldots$.

We realise Theorem 1 as the sum of the following two Propositions, which are proved by two very different arguments.

Proposition 2. *Let k denote the greatest integer not exceeding $\log c/\log(3/2)$. Suppose S is a subset of the integers in $[N,cN]$ and that (S,τ) satisfies the distinct divisor property. Then*

$$\frac{cN}{2}-|S|\ge\frac{N}{2^{k+2}}+O(k).$$

Proposition 3. *Suppose $c>2$. There exists a subset, S, of integers in $[N,cN]$ and a map τ such that (S,τ) obeys the distinct divisor property and with*

$$\frac{cN}{2}-|S|\ll\frac{N}{c^\beta}.$$

All implied constants are absolute; that is they are independent of c and N. The restriction to $c>2$ in Proposition 3 is obviously harmless. The presence of the constant β is best explained by noting that it is the minimum value of the function $\log p_i/\log(p_{i+1}/p_i)$ (where p_i denotes the ith smallest prime).

We thank Professor A. Granville to whom our present exposition is largely due. An earlier version of this note proved the weaker result $\delta(c)=c/2+o(1)$. We are grateful to the referee, Professor C. Pomerance, who, by simplifying our earlier proof, helped clarify the situation and motivated us to strengthen our result.

2. Proof of Proposition 2

We partition the interval $(N,cN]$ into the sets $B_1\cup B_2\cup\cdots\cup B_{k+1}$ where $B_j=((2/3)^jcN,(2/3)^{j-1}cN]$ for $j=1,2,\ldots,k$, and $B_{k+1}=(N,(2/3)^kcN]$. Similarly we partition $[1,cN/2]$, where the potential divisors lie, into intervals $A_1\cup A_2\cup\cdots\cup A_{k+2}$, where $A_i=((2/3)^icN/2,(2/3)^{i-1}cN/2]$ for $i=1,2,\ldots,k$, with $A_{k+1}=(N/2,(2/3)^kcN/2]$ and $A_{k+2}=(1,N/2]$. Note that if $s\in B_j$ then any proper divisor of s must lie in some interval A_i with $i\ge j$; moreover, if that divisor lies in A_j, then it must be $s/2$, since any other proper divisor is $\le s/3\le(2/3)^{j-1}cN/3=(2/3)^jcN/2$ and thus belongs to A_i for some $i>j$.

Now $[cN/2]-|S|=[cN/2]-|\tau(S)|$ counts the number of integers in $[1,cN/2]$ that do not belong to $\tau(S)$. We obtain a lower bound for this quantity by only counting, for each i, those integers $n\in A_i$ which do not belong to $\tau(S)$, and which are divisible by 2^{i-1}. Thus

$$[cN/2]-|S|\ge\sum_{i=1}^{k+2}\left(\#\{n\in A_i:\ 2^{i-1}|n\}-\#\{s\in S:\tau(s)\in A_i,\ 2^{i-1}|\tau(s)\}\right).$$

As we saw above, if $\tau(s) \in A_i$ then $s \in B_j$ for some $j \leq i$. Suppose that 2^{i-1} divides $\tau(s)$. We claim that 2^j divides s, which follows if $j = i$ since 2^{j-1} divides $\tau(s) = s/2$; and which follows if $j < i$ since then 2^j divides 2^{i-1}, which divides $\tau(s)$, which divides s. Therefore

$$\sum_{i=1}^{k+2} \#\{s \in S : \tau(s) \in A_i,\ 2^{i-1} | \tau(s)\} \leq \sum_{j=1}^{k+1} \#\{s \in B_j :\ 2^j | s\}$$

(noting that, since τ is injective, no value of s gets counted twice in the argument above). Now $\#\{n \in A_i :\ 2^{i-1} | n\} = \#\{n \in B_i :\ 2^i | n\} + O(1)$, so substituting this into the two displays above, we get

$$[cN/2] - |S| \geq \#\{n \in A_{k+2} :\ 2^{k+1} | n\} + O(k) = N/2^{k+2} + O(k).$$

3. Proof of Proposition 3

We wish to construct a 'big' set S of integers s in $[N, cN]$ with the distinct divisors $\tau(s)$; since τ is injective, this is equivalent to constructing a 'big' set $R = \tau(S) \subset [1, cN/2]$, such that for each $n \in R$, there exists some distinct proper multiple $\tau^{-1}(n)$, of n, in $[N, cN]$. In fact we shall select $\tau^{-1}(n) = np(n)$ for some prime $p(n)$, which we choose as follows: For $n = [cN/2]$ let $p([cN/2]) = 2$. For $n = [cN/2] - 1, [cN/2] - 2, \ldots, 1$ we define $p(n)$ to be the *largest* prime p for which

i) $N < np \leq cN$, and
ii) $np \neq n'p(n')$ for any $n' > n$, with $n' \leq [cN/2]$,

provided such a prime p exists, otherwise we let $p(n) = 0$ (and then $n \notin R$). We note that $|S| = |R|$ is exactly the number of integers $n \leq cN/2$ for which $p(n) \neq 0$; and thus

$$[cN/2] - |S| = \#\{n \leq cN/2 :\ p(n) = 0\}. \tag{1}$$

For each prime p_k, we define the set of integers

$$\mathcal{I}_k = \{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} :\ \alpha_k \geq 1,\ \prod_{j=1}^{k} (p_{j+1}/p_j)^{\alpha_j} > c/2\}.$$

Lemma. *If $p(n) = 0$ for some integer $n \leq cN/2$, then there exists k such that $n \leq N/p_k$, and $\mathcal{I}_k$ contains a divisor d of n.*

We now complete the proof of Proposition 3, postponing the proof of the Lemma:

Proof of Proposition 3. Using the Lemma we have

$$\#\{n \leq cN/2 :\ p(n) = 0\} \leq \sum_{k \geq 1} \sum_{d \in \mathcal{I}_k} \#\{n \leq N/p_k :\ d | n\} \leq \sum_{k \geq 1} \frac{N}{p_k} \sum_{d \in \mathcal{I}_k} \frac{1}{d}. \tag{2}$$

By definition, we have that

$$\sum_{d \in \mathcal{I}_k} \frac{1}{d} \leq \sum_{\alpha_k \geq 1} \frac{1}{p_k^{\alpha_k}} \sum_{\alpha_{k-1} \geq 0} \frac{1}{p_{k-1}^{\alpha_{k-1}}} \cdots \sum_{\alpha_2 \geq 0} \frac{1}{p_2^{\alpha_2}} \sum_{\alpha_1 \geq A_1} \frac{1}{2^{\alpha_1}}, \tag{3}$$

where $(3/2)^{A_1} > (c/2)/\prod_{j=2}^{k}(p_{j+1}/p_j)^{\alpha_j} \geq (c/2)/(5/3)^{(\alpha_2+\alpha_3+\cdots+\alpha_k)}$, from the definition of the set $\mathcal{I}_k$, since $p_{j+1}/p_j \leq 5/3$ when $j \geq 2$. Therefore, setting $\gamma = 2^{\log(5/3)/\log(3/2)} \approx 2.39471$, we get

$$\sum_{\alpha_1 \geq A_1} \frac{1}{2^{\alpha_1}} \ll \frac{1}{2^{A_1}} \ll c^{-\beta}\gamma^{\alpha_2+\alpha_3+\cdots+\alpha_k}.$$

Substituting this into (3) gives

$$\sum_{d\in\mathcal{I}_k} \frac{1}{d} \ll c^{-\beta} \sum_{\alpha_k \geq 1} \left(\frac{\gamma}{p_k}\right)^{\alpha_k} \sum_{\alpha_{k-1}\geq 0} \left(\frac{\gamma}{p_{k-1}}\right)^{\alpha_{k-1}} \cdots \sum_{\alpha_2 \geq 0} \left(\frac{\gamma}{p_2}\right)^{\alpha_2}$$
$$= c^{-\beta}\frac{\gamma}{p_k}\prod_{i=2}^{k}\left(1-\frac{\gamma}{p_i}\right)^{-1} \ll c^{-\beta}\frac{1}{p_k}\prod_{3\leq p\leq p_k}\left(1-\frac{1}{p}\right)^{-\gamma} \ll c^{-\beta}\frac{(\log p_k)^\gamma}{p_k},$$

using Mertens' theorem that $\prod_{p\leq x}(1-1/p) \asymp 1/\log x$ (see [2] for example). Substituting this estimate into (2), and that estimate back into (1), gives

$$cN/2 - |S| = \#\{n \leq N/2 :\ p(n) = 0\} \ll c^{-\beta} N \sum_{k\geq 1} \frac{(\log p_k)^\gamma}{p_k^2} \ll N/c^\beta.$$

Finally we return to the

Proof of the Lemma. We must have $n \leq N/2$ for, if $cN/2 \geq n > N/2$ then $p = 2$ satisfies i) $N < 2n \leq cN$, and ii) $2n \neq n'p(n')$ for any $n' > n$, since $n'p(n') \geq 2n' > 2n$, so that $p(n) \geq 2$.

Let p_{k_0} be the least prime exceeding N/n; by Bertrand's postulate $p_{k_0} \leq 2N/n < cN/n$ (since $c > 2$), and so $N < np_{k_0} \leq cN$. However $p(n) = 0$, which means that np_{k_0} cannot satisfy (ii) above; in other words, there must exist an integer $n_1 > n$ such that $np_{k_0} = n_1 p_{k_1}$ (where we define k_1 so that $p_{k_1} = p(n_1)$). We note that $p_{k_0} > p_{k_1}$ (since $n_1 > n$ and $np_{k_0} = n_1p_{k_1}$), so that $p_{k_1} \leq N/n$ and thus $n \leq N/p_{k_1}$.

We now construct a useful sequence of integers $n_1, n_2, n_3, \ldots, n_m \in R$ (for some m); we show how to determine n_{j+1} from n_j:

Let k_j be defined by the relation $p_{k_j} = p(n_j)$.

- If $n_j p_{k_j+1} > cN$ then let $m = j$, and the sequence is terminated.
- If $n_j p_{k_j+1} \leq cN$ then there must exist an integer $n_{j+1} > n_j$ for which $n_j p_{k_j+1} = n_{j+1}p(n_{j+1})$ (else $p(n_j) \geq p_{k_j+1}$ by definition).

Since $n_{j+1}p_{k_{j+1}+1} > n_{j+1}p_{k_{j+1}} = n_j p_{k_j+1}$, we see that $n_1p_{k_1+1} < n_2p_{k_2+1} < n_3p_{k_3+1} < \ldots$ forms an increasing sequence of integers, and so we will eventually find an integer m for which $n_m p_{k_m+1} > cN$.

We have seen that $n < n_1 < n_2 < \cdots < n_m$, and thus $p_{k_0} > p_{k_1} \geq p_{k_2} \geq p_{k_3} \geq \cdots \geq p_{k_m}$ (since $n_{j+1} > n_j$ and $n_jp_{k_j+1} = n_{j+1}p_{k_{j+1}}$ imply that $p_{k_j+1} > p_{k_{j+1}}$, and thus $p_{k_j} \geq p_{k_{j+1}}$). Now $n_{j+1} = (p_{k_j+1}/p_{k_{j+1}})n_j$; iterating this gives

$$n_j = \left(\frac{p_{k_{j-1}+1}}{p_{k_j}}\right)\left(\frac{p_{k_{j-2}+1}}{p_{k_{j-1}}}\right)\cdots\left(\frac{p_{k_1+1}}{p_{k_2}}\right)\left(\frac{p_{k_0}}{p_{k_1}}\right)n. \tag{4}$$

Define $d = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = p_{k_m} p_{k_{m-1}} \dots p_{k_2} p_{k_1}$ where $k = k_1$. We show that d divides n by proving that $p_i^{\alpha_i}$ divides n for each i: Let j be the largest integer for which $k_j = i$. Then $p_{k_j} p_{k_{j-1}} \dots p_{k_1} = p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \dots p_k^{\alpha_k}$. Moreover $i \leq k_{j-1} < k_{j-1} + 1 \leq k_{j-2} + 1 \leq \cdots \leq k_1 + 1 \leq k_0$, and so p_i is coprime with $p_{k_{j-1}+1} p_{k_{j-2}+1} \dots p_{k_1+1} p_{k_0}$. Now, $p_i^{\alpha_i}$ divides $p_{k_j} p_{k_{j-1}} \dots p_{k_1}$, which is a divisor of $(p_{k_{j-1}+1} p_{k_{j-2}+1} \dots p_{k_1+1} p_{k_0}) n$ by (4), since n_j is an integer; and so $p_i^{\alpha_i}$ divides n.

To complete the proof of the Lemma we need to show that $d \in \mathcal{I}_k$, which we do by taking (4) with $j = m$, multiplying it by $p_{k_{m+1}}$ and rearranging, to get

$$\prod_{i=1}^{k} \left(\frac{p_{i+i}}{p_i} \right)^{\alpha_i} = \left(\frac{p_{k_m+1}}{p_{k_m}} \right) \left(\frac{p_{k_{m-1}+1}}{p_{k_{m-1}}} \right) \dots \left(\frac{p_{k_1+1}}{p_{k_1}} \right) = \frac{n_m p_{k_m+1}}{n p_{k_0}} > \frac{cN}{2N} = \frac{c}{2},$$

using the fact that $p_{k_0} \leq 2N/n$, by Bertrand's postulate.

References

[1] P. Erdős and C. Pomerance, *An analogue of Grimm's problem of finding distinct prime factors of consecutive integers.* Util. Math. **24** (1983), 45-65.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers.* Fourth edition; New York; Oxford University Press, 1960.