Multiplicative properties of sets of residues

C. Pomerance (Hanover) and A. Schinzel (Warszawa)

Abstract: Given a natural number n, we ask whether every set of residues mod n of cardinality at least $n/2$ contains elements a, b, c with $ab = c$. It is proved that the set of numbers n failing to have this property has upper density smaller than 1.56×10^{-8}.

1. Introduction

In a recent paper [2] it has been shown that every set of positive integers with lower asymptotic density greater than 1/2 contains three integers whose product is a square. Thus, for every positive integer n, every set of residues mod n of cardinality larger than $n/2$ contains residues a, b, c, d with $abc = d^2$. We conjecture that more is true and every set of residues mod n of cardinality at least $n/2$ contains residues a, b, c with

$$ab = c. \tag{1}$$

That is, say a set S is *product free* if (1) has no solution with $a, b, c \in S$. We say a modulus n has "property P" if the largest product-free subset S of $\mathbb{Z}_n$ has cardinality *strictly* smaller than $n/2$. (We denote the ring of integers mod n by $\mathbb{Z}_n$.)

Question 1. *Does every natural number n have property P?*

If true, Question 1 is best possible, since for n an odd prime, the set of quadratic nonresidues mod n is product free and has cardinality $(n-1)/2$. We were initially prepared to assert as a conjecture an affirmative answer to Question1, but in preliminary work of J. Lagarias, P. Kurlberg, and the first author, there appear to be examples of numbers n that fail to have property P. They have yet to come up with concrete examples, but such would seem to have an enormous number of distinct prime factors.

In this paper we show that "most" numbers have property P in the following sense. Let $s(n)$ denote the largest square-full divisor of n and let $\omega(n)$ denote the number of distinct prime factors of n.

Theorem 1. *A natural number n has property P if* $\omega(s(n)) \le 5$.

Theorem 2. *The asymptotic density of the set of integers n with $\omega(s(n)) \ge 6$ is smaller than* 1.56×10^{-8}. *In particular, the set of integers failing to have property P has upper density at most* 1.56×10^{-8}.

The first author was supported in part by NSF grants DMS-0703850, DMS-1001180.

We record some questions that we have not been able to settle, but which may be tractable. It is easy to see that if a number has property P, then so too does all of its divisors have property P. As a consequence, if a number does not have property P, then so too does all of its multiples. Say a number is P-primitive if it does not have property P, but all of its proper divisors do have have property P.

Question 2.
- *Is it true that the reciprocal sum of the P-primitive numbers is finite?*
- *Is it true that every P-primitive number is square-full?*
- *Is it true that as $x \to \infty$, the number of P-primitive numbers in $[1, x]$ is $x^{o(1)}$?*

Since the reciprocal sum of the square-full numbers is finite, an affirmative answer to either of the latter two parts implies an affirmative answer to the first part. Further, an affirmative answer to the first part implies that the set of numbers with property P has an asymptotic density.

In the final section we present some material showing that our Questions are related to some problems in linear programming.

We remark that there has been some consideration in the literature of large product-free subsets of finite groups. For a recent survey, with pointers to other papers, see [3].

Acknowledgments. We thank the referee for a careful reading and the editor for suggesting references [1] and [4]. In addition we thank Jeffrey Lagarias, Pär Kurlberg, and Robin Pemantle for useful discussions.

2. Preliminary results

For a natural number n and a prime p, we let $v_p(n)$ be the number of factors p in the prime factorization of n. We introduce some special notation that we will use throughout the paper. Suppose that n, m are coprime natural numbers. (We shall later take n square-full and m squarefree, but this is not necessary to assume in this section.) We consider the multiplicative monoid $\mathbb{Z}_n \times \mathbb{Z}_m^*$, where $\mathbb{Z}_m^*$ is the unit group mod m. By the Chinese remainder theorem, $\mathbb{Z}_n \times \mathbb{Z}_m^*$ may be thought of as $\{a \in \mathbb{Z}_{nm} : (a, m) = 1\}$. For $d \mid n$, let

$$T_d(n, m) = T_d = \{a \in \mathbb{Z}_n \times \mathbb{Z}_m^* : (a, n) = d\}.$$

Further, if $S \subset \mathbb{Z}_n \times \mathbb{Z}_m^*$, let

$$S_d(n, m) = S_d = T_d \cap S, \quad R_d(n, m) = R_d = T_d \setminus S_d.$$

Lemma 1. *Let n be a natural number. Suppose for each squarefree number m coprime to n, if $S \subset \mathbb{Z}_n \times \mathbb{Z}_m^*$ is product free, then $|S| \le \frac{1}{2}\varphi(m)n$, with strict inequality holding in the case $m = 1$. Then for every squarefree number m coprime to n, we have that mn has property P.*

Proof. Let m be squarefree and coprime to n. For each $j \mid m$, let $A_j = \{a \in \mathbb{Z}_{mn} : (a,m) = j\}$. Then A_j is a multiplicative monoid (with identity a_1, where $a_1 \equiv 1 \pmod{mn/j}$ and $a_1 \equiv 0 \pmod{j}$) that is isomorphic to $\mathbb{Z}_n \times \mathbb{Z}^*_{m/j}$. If $S \subset \mathbb{Z}_{mn}$ is product free, then so is $S \cap A_j$ for each $j \mid m$. By hypothesis then, $|S \cap A_j| \le \frac{1}{2}\varphi(m/j)n$ for each $j \mid m$, with strict inequality holding in the case $j = m$. Thus,

$$|S| = \sum_{j|m} |S \cap A_j| < \frac{1}{2} n \sum_{j|m} \varphi\left(\frac{m}{j}\right) = \frac{1}{2}mn.$$

We conclude that mn has property P, completing the proof. □

Lemma 2. *Suppose n, m are coprime natural numbers, $S \subset \mathbb{Z}_n \times \mathbb{Z}^*_m$ is product free, and D is a nonempty set of divisors of n with $S_d = \emptyset$ for each $d \in D$. Let $\sigma = \sum_{d\in D} 1/d$. If*

$$\frac{\varphi(n)}{n} > \frac{1}{2\sigma},$$

then $|S| < \frac{1}{2}\varphi(m)n$.

Proof. We have

$$\varphi(m)n - |S| = \sum_{d|n} |R_d| \ge \sum_{d\in D} |T_d| = \sum_{d\in D} \varphi\left(\frac{mn}{d}\right) \ge \varphi(mn)\sigma > \frac{1}{2}\varphi(m)n.$$

Thus, $|S| < \frac{1}{2}\varphi(m)n$, completing the proof. □

Lemma 3. *Suppose n, m are coprime natural numbers, $S \subset \mathbb{Z}_n \times \mathbb{Z}^*_m$ is product free, and $S_1 \ne \emptyset$. Then $|S| \le \frac{1}{2}\varphi(m)n$. Further, in the case $m = 1$, the inequality is strict.*

Proof. Let $s_1 \in S_1$ and let $d \mid n$. Note that multiplication by s_1 is a bijection of T_d and the image of S_d under this map is disjoint from S_d, that is, it is contained in R_d. Thus, $|S_d| \le \frac{1}{2}|T_d|$ so that

$$|S| = \sum_{d|n} |S_d| \le \frac{1}{2} \sum_{d|n} |T_d| = \frac{1}{2}\varphi(m)n.$$

Now assume that $m = 1$. We need only show that at least one of the inequalities $|S_d| \le \frac{1}{2}|T_d|$ is strict, and indeed this is the case for $d = n$, since $|T_n| = 1$. This completes the proof of the lemma. □

Remark. The multiplication-by-s_1 argument in the proof is used in various guises throughout the paper.

Corollary 1. *Suppose n, m are coprime natural numbers, $\varphi(n) > \frac{1}{2}n$, and m is squarefree. Then mn has property P. In particular, every squarefree number has property P.*

Proof. By Lemma 1 it suffices to consider product-free subsets S of $\mathbb{Z}_n \times \mathbb{Z}^*_m$. Lemma 2 handles the case $S_1 = \emptyset$ and Lemma 3 handles the case $S_1 \ne \emptyset$. □

For any natural number n, let $\mathrm{rad}(n)$ denote the largest squarefree divisor of n and let $\sigma(n)$ denote the sum of the divisors of n. Another way of stating Corollary 1 is that if $u = n/\mathrm{rad}(n)$ and $u/\varphi(u) < 2$, then n has property P. A stronger result holds: If $\sigma(u)/u < 2$, then n has property P. However we will not need this stronger assertion. We do not know how to replace "2" in either of these assertions with any larger number.

3. Propositions

The heart of our method is contained in the three propositions in this section. With some effort it is likely they can be extended to more complicated cases and so allow an improvement in our main result. Such efforts might even lead to a complete proof of Conjecture 1.

Proposition 1. *Suppose n, m are coprime natural numbers and S is a product-free subset of $\mathbb{Z}_n \times \mathbb{Z}_m^*$. Suppose that p is a prime factor of n and that $S_p \neq \emptyset$. Let D be a nonempty set of divisors of n not divisible by p with $S_d = \emptyset$ for each $d \in D$, and let $\sigma = \sum_{d\in D} 1/d$. If*

$$\frac{\varphi(n)}{n} > \frac{p-1}{2p\sigma}, \tag{2}$$

then $|S| < \frac{1}{2}\varphi(m)n$.

Proof. Suppose not and S is a counterexample for n. For any k, let $n' = n^2p^k$ and let π_k be the projection from $\mathbb{Z}_{n'} \times \mathbb{Z}_m^*$ to $\mathbb{Z}_n \times \mathbb{Z}_m^*$ given by reducing the first coordinate modulo n. Note that $\pi_k(ab) = \pi_k(a)\pi_k(b)$ for each pair $a, b \in \mathbb{Z}_{n'} \times \mathbb{Z}_m^*$, whence $S' = \pi_k^{-1}(S)$ is product free. We claim that S' is a counterexample for n'. Indeed, $|S'| = np^k|S| \geq \frac{1}{2}\varphi(m)n^2p^k = \frac{1}{2}\varphi(m)n'$. Further, for $d \in D$, $S_d = \emptyset$ implies that $S'_d = \emptyset$, and $S_p \neq \emptyset$ implies that $S'_p \neq \emptyset$. Since $\varphi(n)/n = \varphi(n')/n'$, we have an exact correspondence. In the sequel we do not use the dash and instead we assume that $d^2 \mid n$ for each $d \in D$ and that $v_p(n)$ is very large. In addition, we denote $v_p(n)$ with the letter k.

For a divisor d of n with $p \nmid d$ and $d \notin D$, consider the sets $S_{p^{2i}d}, S_{p^{2i+1}d}$ for $0 \leq i < (k-1)/2$. Say $s_p \in S_p$. Multiplication by s_p is a $p:1$ mapping of $T_{p^{2i}d}$ onto $T_{p^{2i+1}d}$. Since S is product free, $s_pS_{p^{2i}d}$ is disjoint from $S_{p^{2i+1}d}$. We conclude that

$$\frac{1}{p}|S_{p^{2i}d}| + |S_{p^{2i+1}d}| \leq |T_{p^{2i+1}d}| = \varphi\left(\frac{mn}{p^{2i+1}d}\right) = \frac{1}{p^{2i+1}}\varphi\left(\frac{mn}{d}\right).$$

In addition,

$$|S_{p^{2i}d}| \leq |T_{p^{2i}d}| = \frac{1}{p^{2i}}\varphi\left(\frac{mn}{d}\right), \quad |S_{p^{2i+1}d}| \leq |T_{p^{2i+1}d}| = \frac{1}{p^{2i+1}}\varphi\left(\frac{mn}{d}\right).$$

These inequalities imply that

$$|S_{p^{2i}d}| + |S_{p^{2i+1}d}| \leq \frac{1}{p^{2i}}\varphi\left(\frac{mn}{d}\right)$$

and so

$$|R_{p^{2i}d}| + |R_{p^{2i+1}d}| \geq \frac{1}{p^{2i+1}}\varphi\left(\frac{mn}{d}\right).$$

We conclude that

$$\sum_{j=0}^{k} |R_{p^j d}| \geq \sum_{0\leq i<(k-1)/2} \frac{1}{p^{2i+1}}\varphi\left(\frac{mn}{d}\right) = \left(\frac{p}{p^2-1} + O\left(p^{-k}\right)\right)\varphi\left(\frac{mn}{d}\right),$$

where O-constants may depend on p. Thus,

$$\begin{aligned}\sum_{d\mid n\,:\,p\nmid d,\, d\notin D}\ \sum_{j=0}^{k} |R_{p^j d}| &\geq \left(\frac{p}{p^2-1} + O\left(p^{-k}\right)\right)\varphi(m) \sum_{d\mid n\,:\,p\nmid d,\, d\notin D} \varphi\left(\frac{n}{d}\right)\\ &= \left(\frac{p}{p^2-1} + O\left(p^{-k}\right)\right)\varphi(m)\varphi(p^k)\left(\frac{n}{p^k} - \sum_{d\in D}\varphi\left(\frac{n}{p^k d}\right)\right)\\ &= \left(\frac{1}{p+1} + O\left(p^{-k}\right)\right)\varphi(m)n - \left(\frac{p}{p^2-1} + O\left(p^{-k}\right)\right)\varphi(mn)\sigma.\end{aligned}$$

For $d \in D$, we consider pairs $S_{p^{2i+1}d}, S_{p^{2i+2}d}$ for $0 \leq i < (k-2)/2$ and we find in the same way that

$$\begin{aligned}\sum_{d\in D}\sum_{j=0}^{k} |R_{p^j d}| &\geq \sum_{d\in D} |T_d| + \sum_{d\in D}\ \sum_{0\leq i<(k-2)/2} \frac{1}{p^{2i+2}}\varphi\left(\frac{mn}{d}\right)\\ &= \sum_{d\in D} |T_d| + \left(\frac{1}{p^2-1} + O\left(p^{-k}\right)\right)\sum_{d\in D}\varphi\left(\frac{mn}{d}\right)\\ &= \left(\frac{p^2}{p^2-1} + O\left(p^{-k}\right)\right)\varphi(mn)\sigma.\end{aligned}$$

Hence,

$$\varphi(m)n - |S| = \sum_{d\mid n} |R_d| \geq \frac{1}{p+1}\varphi(m)n + \frac{p}{p+1}\varphi(mn)\sigma + O\left(p^{-k}\varphi(m)n\sigma\right).$$

By the hypothesis of the proposition,

$$\frac{1}{\varphi(m)n}\left(\frac{1}{p+1}\varphi(m)n + \frac{p}{p+1}\varphi(mn)\sigma\right) > \frac{1}{p+1} + \frac{1}{2}\frac{p-1}{p+1} = \frac{1}{2}.$$

Thus, if k is sufficiently large, then

$$\varphi(m)n - |S| > \frac{1}{2}\varphi(m)n$$

and the proposition follows. □

Proposition 2. *Suppose n, m are coprime natural numbers, $4 \mid n$, $S \subset \mathbb{Z}_n \times \mathbb{Z}_m^*$ is product free, $S_2 = \emptyset$, $S_4 \neq \emptyset$, and D is a set of odd divisors of n containing 1 with $S_d = \emptyset$ for each $d \in D$. Let $\sigma = \sum_{d\in D} 1/d$. If*

$$\frac{\varphi(n)}{n} > \frac{3}{4+8\sigma}, \tag{3}$$

then $|S| < \frac{1}{2}\varphi(m)n$.

Proof. As with the proof of Proposition 1, we may assume that $d^2 \mid n$ for each $d \in D$ and we may assume that $k = v_2(n)$ is very large. For $d \mid n$, d odd, $d \notin D$, we consider the pairs $S_{4^{2i}d}, S_{4^{2i+1}d}$ and also the pairs $S_{2\cdot 4^{2i}d}, S_{2\cdot 4^{2i+1}d}$ and we find that

$$\begin{aligned}\sum_{j=0}^{k} |R_{2^j d}| &\ge \sum_{0\le i<(k-4)/4} \left(\frac{1}{4^{2i+1}} + \frac{1}{2\cdot 4^{2i+1}}\right)\varphi\left(\frac{mn}{d}\right)\\ &= \left(\frac{2}{5} + O\left(2^{-k}\right)\right)\varphi\left(\frac{mn}{d}\right).\end{aligned}$$

Thus,

$$\begin{aligned}\sum_{d\mid n\,:\,d\ \text{odd},\, d\notin D}\ \sum_{j=0}^{k} |R_{2^j d}| &\ge \left(\frac{2}{5} + O\left(2^{-k}\right)\right)\sum_{d\mid n\,:\,d\ \text{odd},\, d\notin D} \varphi\left(\frac{mn}{d}\right)\\ &= \left(\frac{2}{5} + O\left(2^{-k}\right)\right)\varphi(2^k)\varphi(m)\left(\frac{n}{2^k} - \sum_{d\in D}\varphi\left(\frac{n}{2^k d}\right)\right)\\ &= \left(\frac{1}{5} + O\left(2^{-k}\right)\right)\varphi(m)n - \left(\frac{2}{5} + O\left(2^{-k}\right)\right)\varphi(mn)\sigma.\end{aligned}$$

For $d \in D \setminus \{1\}$ we consider the pairs $S_{4^{2i+1}d}, S_{4^{2i+2}d}$ and the pairs $S_{2\cdot 4^{2i}d}, S_{2\cdot 4^{2i+1}d}$, and we find that

$$\begin{aligned}\sum_{d\in D\setminus\{1\}} |R_{2^j d}| &\ge \sum_{d\in D\setminus\{1\}} |T_d| + \left(\frac{1}{5} + O\left(2^{-k}\right)\right)\varphi(mn)(\sigma - 1)\\ &= \left(\frac{6}{5} + O\left(2^{-k}\right)\right)\varphi(mn)(\sigma - 1).\end{aligned}$$

Finally, we consider the pairs $S_{4^{2i+1}}, S_{4^{2i+2}}$ and the pairs $S_{2\cdot 4^{2i+1}}, S_{2\cdot 4^{2i+2}}$ and we find that

$$\begin{aligned}\sum_{j=0}^{k} |R_{2^j}| &\ge |T_1| + |T_2| + \left(\frac{1}{10} + O\left(2^{-k}\right)\right)\varphi(mn)\\ &= \left(\frac{8}{5} + O\left(2^{-k}\right)\right)\varphi(mn).\end{aligned}$$

We conclude that

$$\begin{aligned}\varphi(m)n - |S| &= \sum_{d\mid n} |R_d|\\ &\ge \left(\frac{1}{5} + O\left(2^{-k}\right)\right)\varphi(m)n + \left(\frac{4}{5}\sigma + \frac{2}{5} + O\left(2^{-k}\right)\right)\varphi(mn),\end{aligned}$$

where the O-constant may depend on σ. By the hypothesis,

$$\frac{1}{\varphi(m)n}\left(\frac{1}{5}\varphi(m)n+\left(\frac{4}{5}\sigma+\frac{2}{5}\right)\varphi(mn)\right)=\frac{1}{5}+\left(\frac{4}{5}\sigma+\frac{2}{5}\right)\frac{\varphi(n)}{n}$$
$$>\frac{1}{5}+\frac{4\sigma+2}{5}\cdot\frac{3}{8\sigma+4}=\frac{1}{2},$$

so for k sufficiently large, we have $n\varphi(m)-|S|>\frac{1}{2}\varphi(m)n$. This proves the proposition. □

Proposition 3. *Suppose n, m are coprime positive integers, $S\subset\mathbb{Z}_n\times\mathbb{Z}_m^*$ is product free, $p, q \mid n$ are different primes, $S_p, S_q\neq\emptyset$, and D is a nonempty set of divisors of n coprime to pq with $S_d=\emptyset$ for each $d\in D$. Let $\sigma=\sum_{d\in D}1/d$. If*

$$\frac{\varphi(n)}{n}>\frac{\varphi(pq)}{2pq\sigma}, \tag{4}$$

then $|S|<\frac{1}{2}\varphi(m)n$.

Proof. Similarly as with the two previous propositions, we may assume that $d^2\mid n$ for each $d\in D$ and $k=v_p(n), l=v_q(n)$ are both large. Suppose that $d\mid n$, $(d,pq)=1$, and $d\notin D$. Let $0\le i<(k-2)/2$, $0\le j<(l-2)/2$, and let $u=p^{2i}q^{2j}d$. We consider 4-tuples $S_u, S_{pu}, S_{qu}, S_{pqu}$. Using that S is product free and $S_p, S_q\neq\emptyset$, we show that

$$\sum_{v\mid pq}|R_{vu}|\ge|T_{pu}|+|T_{qu}|=\left(\frac{1}{p^{2i+1}q^{2j}}+\frac{1}{p^{2i}q^{2j+1}}\right)\varphi\left(\frac{mn}{d}\right). \tag{5}$$

To see this, let $s_p\in S_p$, $s_q\in S_q$. We have s_pS_u disjoint from S_{pu} and s_pS_{qu} disjoint from S_{pqu}. Similarly, s_qS_u is disjoint from S_{qu} and s_qS_{pu} is disjoint from S_{pqu}. Now multiplication by s_p is a $p:1$ mapping of T_u onto T_{pu} and also of T_{qu} onto T_{pqu}, and similarly multiplication by s_q is a $q:1$ mapping of T_u onto T_{qu} and of T_{pu} onto T_{pqu}. For $v\mid pq$, let $\alpha_v=|S_{vu}|/|T_{vu}|$, so that each $\alpha_v\in[0,1]$ and

$$\alpha_1+\alpha_p\le 1,\quad \alpha_1+\alpha_q\le 1,\quad \alpha_q+\alpha_{pq}\le 1,\quad \alpha_p+\alpha_{pq}\le 1.$$

The maximal value of

$$\alpha_1+\frac{1}{p}\alpha_p+\frac{1}{q}\alpha_q+\frac{1}{pq}\alpha_{pq}$$

subject to these constraints occurs when $\alpha_1=\alpha_{pq}=1$ and $\alpha_p=\alpha_q=0$. This proves (5).

In the sequel, O-constants possibly depend on p, q, and σ.

We have

$$\sum_{d|n\,:\,(d,pq)=1,\,d\notin D}\ \sum_{i=0}^{k}\sum_{j=0}^{l}|R_{p^iq^jd}|$$
$$\geq\left(\frac{1}{p}+\frac{1}{q}\right)\left(\frac{p^2q^2}{(p^2-1)(q^2-1)}+O\left(p^{-k}+q^{-l}\right)\right)\sum_{d|n\,:\,(d,pq)=1,\,d\notin D}\varphi\left(\frac{mn}{d}\right)$$
$$=\left(\frac{1}{p}+\frac{1}{q}\right)\frac{p^2q^2}{(p^2-1)(q^2-1)}\varphi(m)\varphi(p^kq^l)\left(\frac{n}{p^kq^l}-\sum_{d\in D}\varphi\left(\frac{n}{p^kq^ld}\right)\right)$$
$$+O\left(p^{-k}+q^{-l}\right)\varphi(m)n$$
$$=\frac{p+q}{(p+1)(q+1)}\varphi(m)n-\frac{pq(p+q)}{(p^2-1)(q^2-1)}\varphi(mn)\sigma$$
$$+O\left(p^{-k}+q^{-l}\right)\varphi(m)n.$$

Next suppose that $d\in D$. With $u=p^{2i+1}q^{2j}d$, we consider the 4-tuple $S_u,S_{pu},S_{qu},S_{pqu}$ as before, so that

$$\sum_{v|pq}|R_{vu}|\geq|T_{pu}|+|T_{qu}|=\left(\frac{1}{p^{2i+2}q^{2j}}+\frac{1}{p^{2i+1}q^{2j+1}}\right)\varphi\left(\frac{mn}{d}\right).$$

We also consider pairs $S_{q^{2j+1}d},S_{q^{2j+2}d}$ and we have

$$|R_{q^{2j+1}d}|+|R_{q^{2j+2}d}|\geq|T_{q^{2j+2}d}|=\frac{1}{q^{2j+2}}\varphi\left(\frac{mn}{d}\right).$$

Thus,

$$\sum_{d\in D}\sum_{i=0}^{k}\sum_{j=0}^{l}|R_{p^iq^jd}|$$
$$\geq\sum_{d\in D}|T_d|+\left(\frac{q^2+pq}{(p^2-1)(q^2-1)}+\frac{1}{q^2-1}+O\left(p^{-k}+q^{-l}\right)\right)\sum_{d\in D}\varphi\left(\frac{mn}{d}\right)$$
$$=\left(1+\frac{q^2+pq}{(p^2-1)(q^2-1)}+\frac{1}{q^2-1}+O\left(p^{-k}+q^{-l}\right)\right)\varphi(mn)\sigma.$$

We conclude that

$$\varphi(m)n-|S|=\sum_{d|n}|R_d|$$
$$\geq\frac{p+q}{(p+1)(q+1)}\varphi(m)n+\left(1+\frac{q^2+pq+p^2-1-pq(p+q)}{(p^2-1)(q^2-1)}\right)\varphi(mn)\sigma$$
$$+O\left(p^{-k}+q^{-l}\right)\varphi(m)n$$
$$=\frac{p+q}{(p+1)(q+1)}\varphi(m)n+\frac{pq\sigma}{(p+1)(q+1)}\varphi(mn)+O\left(p^{-k}+q^{-l}\right)\varphi(m)n.$$

By (4),

$$\frac{1}{\varphi(m)n}\left(\frac{p+q}{(p+1)(q+1)}\varphi(m)n + \frac{pq\sigma}{(p+1)(q+1)}\varphi(mn)\right)$$
$$= \frac{p+q}{(p+1)(q+1)} + \frac{pq\sigma}{(p+1)(q+1)}\frac{\varphi(n)}{n}$$
$$> \frac{p+q}{(p+1)(q+1)} + \frac{(p-1)(q-1)}{2(p+1)(q+1)} = \frac{1}{2}.$$

Thus, if k, l are sufficiently large,

$$\varphi(m)n - |S| > \frac{1}{2}\varphi(m)n,$$

which proves the proposition. □

4. Proof of Theorem 1

Let n be a square-full natural number with $\omega(n) \leq 5$. Via Lemma 1, to prove that mn has property P for every squarefree number m coprime to n it suffices to show that for each such m, the largest product-free subset of $\mathbb{Z}_n \times \mathbb{Z}_m^*$ has cardinality at most $\frac{1}{2}\varphi(m)n$, with strict inequality in the case $m = 1$.

So, we fix some integer m coprime to n and we take a product-free set $S \subset \mathbb{Z}_n \times \mathbb{Z}_m^*$. By Lemma 3, we may assume that $S_1 = \emptyset$. We consider the 4 cases depending on the 4 possibilities for $(6, n)$.

First, assume that $(6, n) = 1$. Then

$$\frac{\varphi(n)}{n} \geq \frac{4}{5}\frac{6}{7}\frac{10}{11}\frac{12}{13}\frac{16}{17} > \frac{1}{2},$$

so that Corollary 1 handles this case.

Next assume that $(6, n) = 3$. Then $\varphi(n)/n \geq 384/1001$. If $S_3 = \emptyset$, Lemma 2 with $D = \{1, 3\}$ completes the proof, so we may assume $S_3 \neq \emptyset$. Then Proposition 1 with $p = 3$ and $D = \{1\}$ completes the argument.

Now assume that $(6, n) = 2$. Then $\varphi(n)/n \geq 288/1001$. If $S_2 \neq \emptyset$, Proposition 1 with $p = 2$, $D = \{1\}$ shows that $|S| < \frac{1}{2}\varphi(m)n$. Thus, we may assume that $S_2 = \emptyset$. If $5 \nmid n$, then $\varphi(n)/n > 1/3$, and then Lemma 2 with $D = \{1, 2\}$ completes the proof, so we may assume that $5 \mid n$. If $S_5 \neq \emptyset$, Proposition 1 with $p = 5$, $D = \{1, 2\}$ implies that we are done with this case. So, assume that $S_5 = \emptyset$. If $S_4 \neq \emptyset$, the result follows from Proposition 2 with $D = \{1, 5\}$. So assume that $S_4 = \emptyset$. Then Lemma 2 with $D = \{1, 2, 4, 5\}$ completes the argument.

The hardest case is when $(6, n) = 6$. In this case we have $\varphi(n)/n \geq 16/77$. If $S_2, S_3 \neq \emptyset$, the result follows from Proposition 3 with $p = 2$, $q = 3$, and $D = \{1\}$. Next assume that $S_2 \neq \emptyset$ and $S_3 = \emptyset$. Then the result follows from Proposition 1 with $p = 2$, $D = \{1, 3\}$. Now assume that $S_2 = \emptyset$ and $S_3 \neq \emptyset$. If $5 \nmid n$ then $\varphi(n)/n \geq 240/1001$ and the result follows from Proposition 1 with $p = 3$, $D = \{1, 2\}$. So assume that $5 \mid n$. If $S_5 \neq \emptyset$, the result follows from Proposition 3 with $p = 3$, $q = 5$, $D = \{1, 2\}$, so we may take $S_5 = \emptyset$. Then the result follows from Proposition 1 with $p = 3$, $D = \{1, 2, 5\}$.

We are left with the case that $6 \mid n$ and $S_1 = S_2 = S_3 = \emptyset$. Proposition 2 with $D = \{1, 3\}$ handles the case $S_4 \neq \emptyset$, so we may assume that $S_4 = \emptyset$. We consider the four possibilities for $(35, n)$. If $(35, n) = 1$, then $\varphi(n)/n \geq 640/2431$, so that Lemma 2 with $D = \{1, 2, 3, 4\}$ handles this case.

Suppose that $(35, n) = 7$, so that $\varphi(n)/n \geq 240/1001$. Proposition 1 with $p = 7$ and $D = \{1, 2, 3, 4\}$ handles the case $S_7 \neq \emptyset$, while Lemma 2 with $D = \{1, 2, 3, 4, 7\}$ handles the case $S_7 = \emptyset$.

Suppose that $(35, n) = 5$, so that $\varphi(n)/n \geq 32/143$. Proposition 1 with $p = 5$ and $D = \{1, 2, 3, 4\}$ handles the case $S_5 \neq \emptyset$, while Lemma 2 with $D = \{1, 2, 3, 4, 5\}$ handles the case $S_5 = \emptyset$.

Finally suppose that $35 \mid n$. If either $S_5 \neq \emptyset$ or $S_7 \neq \emptyset$, Proposition 1 with $D = \{1, 2, 3, 4\}$ completes the proof. So assume that $S_5 = S_7 = \emptyset$. Then Lemma 2 with $D = \{1, 2, 3, 4, 5, 7\}$ completes the proof.

We remark that our existing tools make it possible to begin handling the case $\omega(s(n)) = 6$ and perhaps it is possible to complete this case. Even a partial result would give a better density estimate in the next section.

5. Density

In this section we prove Theorem 2. For a natural number n, recall that $\mathrm{rad}(n)$ is the largest squarefree divisor of n. Let m be a squarefree integer and let d_m be the density of those integers n with $\mathrm{rad}(s(n)) = m$. For $\mathrm{rad}(s(n)) = m$ it is necessary and sufficient that $m^2 \mid n$ and $v_p(n) \leq 1$ for each prime $p \nmid m$. Thus,

$$d_m = \frac{1}{m^2} \prod_{p \nmid m} \left(1 - p^{-2}\right) = \frac{6}{\pi^2 m^2} \prod_{p \mid m} \left(1 - p^{-2}\right)^{-1}.$$

Let $f(m) = \prod_{p \mid m} 1/(p^2 - 1)$, so that

$$d_m = \frac{6}{\pi^2} f(m). \tag{6}$$

It is our task in this section to compute the asymptotic density d of the set of those integers n with $\omega(s(n)) \geq 6$. Namely, we wish to compute

$$d := \sum_{\omega(m) \geq 6} \mu^2(m) d_m = \frac{6}{\pi^2} \sum_{\omega(m) \geq 6} \mu^2(m) f(m) = 1 - \frac{6}{\pi^2} \sum_{\omega(m) \leq 5} \mu^2(m) f(m).$$

Let $\delta_j = \sum_{\omega(m) = j} \mu^2(m) f(m)$. We now compute δ_j for $j = 0, 1, \ldots, 5$.

We evidently have

$$\delta_0 = 1.$$

For δ_1, we accelerate the convergence of the series as follows:

$$\delta_1 = \sum_p \frac{1}{p^2 - 1} = \log\left(\frac{\pi^2}{6}\right) + \sum_p \left(\frac{1}{p^2 - 1} + \log\left(1 - p^{-2}\right)\right),$$

and so we find that

$$\delta_1 \doteq 0.551693297656999$$

rounded to 15 decimal places.

The computation for δ_j for $j > 1$ is simplified by applying the Newton–Girard formula for symmetric functions. In particular, with

$$\eta_j = \sum_p \frac{1}{(p^2-1)^j},$$

we have

$$\delta_j = \frac{1}{j}\sum_{i=1}^{j}(-1)^{i-1}\eta_i\delta_{j-i}. \tag{7}$$

Note that (7) allows one to compute each δ_j recursively in terms of previous values of δ_i and values of the very rapidly converging series η_i (where $\eta_1 = \delta_1$ has already been computed). To 15 decimal places, we have

$$\begin{aligned}
\eta_2 &\doteq 0.129038925897808,\\
\eta_3 &\doteq 0.039072405735575,\\
\eta_4 &\doteq 0.012593028398642,\\
\eta_5 &\doteq 0.004145873475259.
\end{aligned}$$

Thus, via (7), we have

$$\begin{aligned}
\delta_2 &\doteq 0.087663284390923,\\
\delta_3 &\doteq 0.005415247209989,\\
\delta_4 &\doteq 0.000159633875359,\\
\delta_5 &\doteq 0.000002578156405.
\end{aligned}$$

We conclude that

$$\begin{aligned}
d = 1 - \frac{6}{\pi^2}(\delta_0+\delta_1+\delta_2+\delta_3+\delta_4+\delta_5) \doteq 1 - \frac{6}{\pi^2}(1.64493404128968)\\
\doteq 1.553774 \times 10^{-8},
\end{aligned}$$

which proves Theorem 2.

6. Further remarks

One might consider large product-free subsets of $\mathbb{N}$, the set of natural numbers. It is easy to see that there are product-free subsets of $\mathbb{N}$ with asymptotic density equal to $1/2$. Here are some examples:

- the set of natural numbers n that are the product of an odd number of primes;
- the set of natural numbers n that are the product of a number that is 3 mod 4 and a power of 2;
- the set of natural numbers n that are the product of a number that is 2 mod 3 and a power of 3;

- more generally, for any odd prime p, the set of natural numbers n which are a product of a quadratic nonresidue mod p and a power of p.

These examples, the first of which was noted in [2], also show that the principal result of [2] is best possible. A further example is supplied in Fish [1] where it is shown that there are "normal" subsets of $\mathbb{N}$ which are product free. (A subset S of $\mathbb{N}$ is normal if the characteristic function of S, written as a sequence of 0's and 1's, is normal. Necessarily a normal subset of $\mathbb{N}$ has density 1/2.) If, as we think now, there are numbers n which do not have property P, then there are product-free subsets of $\mathbb{N}$ with density larger than 1/2.

Schur [4] showed that if $\mathbb{N}$ is k-colored there must be a monochromatic solution to $a+b=c$. A. Sárközy suggested to us that one might consider the multiplicative analog: If $\mathbb{N}$ is k-colored, must there be a monochromatic solution to $ab=c$? Since $1 \cdot 1 = 1$, the number 1 should not be allowed in the set, so we are k-coloring $\mathbb{N} \setminus \{1\}$. By considering the powers of 2, one sees that the multiplicative analog immediately follows from the original additive version. So, it is reasonable to consider then the multiplicative problem for squarefree numbers larger than 1. Here's a proof in the case $k=2$: Let $p_1, \dots, p_9$ be any 9 primes, and so without loss of generality, we may assume that each of $p_1, \dots, p_5$ is red. We then may assume that each product of 2 of these is blue and so each product of 4 of these is red. Then the product of all 5 is blue, and since a product of 4 can be written as one of the primes times the other 3, each product of 3 primes is blue. But then $p_1p_2 \cdot p_3p_4p_5 = p_1p_2p_3p_4p_5$ is all blue. It is possible, maybe even likely, that these thoughts generalize to k colors, and perhaps this and related topics would be interesting to explore.

Consider the following question. Let $\Omega(n)$ denote the number of prime factors of n counted with multiplicity.

Question 3. *Let $p_1, p_2, \dots, p_k$ be distinct primes, let b be a positive integer, and let $n = (p_1p_2 \dots p_k)^b$. For $u \mid n$ let α_u be a real variable in $[0,1]$ such that if $uv \mid n$ and $\alpha_u > 0$, then $\alpha_v + \alpha_{uv} \le 1$. Further suppose that $\alpha_1 = 0$. Then do we have*

$$\sum_{u \mid n} \frac{\alpha_u}{u} < \sum_{\substack{u:\ \mathrm{rad}(u) \mid n \\ \Omega(u)\ \mathrm{odd}}} \frac{1}{u}\ ?$$

Remark. Note that the second sum is over an infinite set of numbers u.

Theorem 3. *Suppose m is a squarefree number and that we have an affirmative answer to Question 3 for each n running over the powers of m. Then every number n with* $\mathrm{rad}(n) \mid m$ *has property P.*

Proof. Assume the hypothesis of the theorem and let $m = p_1p_2 \dots p_k$, where $p_1, p_2, \dots, p_k$ are distinct primes. Since every every divisor of a number with property P also has property P, it is thus sufficient to show that $n = m^{b+1}$ has property P for every large integer b.

Suppose that $n = m^{b+1}$ and $S \subset \mathbb{Z}/n\mathbb{Z}$ is product free. For $u \mid n$, let $T_u = T_u(n,1)$, $S_u = S \cap T_u$ as in Section 2, and let $\alpha_u = |S_u|/|T_u|$. By Lemma 3 (with "m" being 1), we may assume that $\alpha_1 = 0$. Assume $uv \mid m^b$ and $\alpha_u > 0$. Then $S_u \neq \emptyset$, say $s_u \in S_u$, and multiplication by s_u is a $u:1$ mapping of T_v onto T_{uv}. Since S is product free, we have $s_u S_v \cap S_{uv} = \emptyset$, so that

$$\frac{1}{u}|S_v| + |S_{uv}| \leq |T_{uv}|;$$

that is,

$$\alpha_v \frac{\varphi(n)}{uv} + \alpha_{uv}\frac{\varphi(n)}{uv} \leq \frac{\varphi(n)}{uv},$$

or $\alpha_v + \alpha_{uv} \leq 1$. Thus, the numbers α_u for $u \mid m^b$ satisfy the hypotheses of Conjecture 3, and so

$$\sum_{u \mid m^b} \frac{\alpha_u}{u} < \sum_{\substack{\mathrm{rad}(u) \mid m \\ \Omega(u)\ \mathrm{odd}}} \frac{1}{u} = \frac{1}{2} \sum_{\mathrm{rad}(u)\mid m} \left(\frac{1}{u} - \frac{(-1)^{\Omega(u)}}{u} \right) = \frac{1}{2}\left(\frac{m}{\varphi(m)} - \frac{m}{\sigma(m)} \right).$$

Note that

$$|S| = \sum_{u \mid n} |S_u| = \sum_{u\mid n} \alpha_u \varphi\left(\frac{n}{u}\right) \leq \varphi(n) \left(\sum_{u \mid m^b} \frac{\alpha_u}{u} + \sum_{\substack{u \mid n \\ u \nmid m^b}} \frac{1}{\varphi(u)} \right).$$

The first sum here is bounded as above, and the second sum is bounded by

$$\frac{m}{\varphi(m)} \sum_{\substack{u \mid n \\ u \nmid m^b}} \frac{1}{u} \leq \left(\frac{m}{\varphi(m)} \right)^2 \sum_{p \mid m} \frac{1}{p^{b+1}} < \frac{1}{2} \frac{m}{\sigma(m)}$$

if b is sufficiently large ($b \geq k+4$ is sufficient). For such b,

$$|S| < \frac{\varphi(n)}{2}\left(\frac{m}{\varphi(m)} - \frac{m}{\sigma(m)} \right) + \frac{\varphi(n)}{2}\frac{m}{\sigma(m)} = \frac{\varphi(n)m}{2\varphi(m)} = \frac{1}{2}n.$$

Thus, n has property P. □

Question 3 may be recast as a linear program as follows. We have the linear function $\sum_{u \mid n} \alpha_u/u$ in the variables α_u that we are seeking to maximize, but to be a linear program, the domain must be a convex polytope. Note that the condition "$\alpha_u > 0$ implies $\alpha_v + \alpha_{uv} \leq 1$" is equivalent to "$\alpha_u = 0$ or $\alpha_v + \alpha_{uv} \leq 1$", and so the domain is a finite union of polytopes. Since the maximum of a linear function over a finite union of polytopes is equal to the maximum over their convex hull, we thus may enlarge the domain to obtain a linear program which has the same maximum as the original problem.

We close this paper with a proof of an affirmative answer to Question 3 when $k \leq 2$ using tools close to those used in Section 3.

Theorem 4. *The answer to Question 3 is yes for $k=1$ and $k=2$.*

Proof. For $k=1$ with prime p and $n=p^b$, we have divisors p^i of n for $i=1,\dots,b$. If $\alpha_p=0$, then

$$\sum_{u\mid n}\frac{\alpha_u}{u}<\sum_{i\ge 2}\frac{1}{p^i}=\frac{1}{p(p-1)}.$$

But

$$\sum_{i\text{ odd}}\frac{1}{p^i}=\frac{p}{p^2-1}=\frac{1}{p-1/p},$$

which does indeed exceed the prior estimate. Thus, we may assume that $\alpha_p>0$. Then for i odd and $p^{i+1}\mid n$, we have $\alpha_{p^i}+\alpha_{p^{i+1}}\le 1$ so that

$$\frac{\alpha_{p^i}}{p^i}+\frac{\alpha_{p^{i+1}}}{p^{i+1}}\le\frac{1}{p^i}.$$

Using also $\alpha_{p^b}\le 1$, we have

$$\sum_{u\mid n}\frac{\alpha_u}{u}\le\sum_{\substack{i\le b\\ i\text{ odd}}}\frac{1}{p^i}<\sum_{i\text{ odd}}\frac{1}{p^i},$$

completing the case $k=1$.

For $k=2$, we write $n=(pq)^b$ where p,q are distinct primes. We wish to show that $L<R$, where

$$L:=\sum_{u\mid n}\frac{\alpha_u}{u},\quad R:=\sum_{\substack{\mathrm{rad}(u)\mid pq\\ \Omega(u)\text{ odd}}}\frac{1}{u}=\frac{1}{2}\left(\frac{pq}{\varphi(pq)}-\frac{pq}{\sigma(pq)}\right)=\frac{pq(p+q)}{(p^2-1)(q^2-1)},$$

(cf. the proof of Theorem 3). First assume that $\alpha_p=\alpha_q=0$. Then

$$L<\sum_{i+j\ge 2}\frac{1}{p^iq^j}=\frac{pq}{(p-1)(q-1)}-1-\frac{1}{p}-\frac{1}{q}=\frac{pq+p^2+q^2-p-q}{pq(p-1)(q-1)},$$

so that if $s=p+q$ and $m=pq$, we have

$$\begin{aligned}\frac{L}{R}&<\frac{(s^2-m-s)(p+1)(q+1)}{sm^2}=\frac{(s^2-m-s)(s+m+1)}{sm^2}\\&=\left(\frac{s-1}{m}-\frac{1}{s}\right)\left(\frac{s+1}{m}+1\right).\end{aligned}$$

As a function of m this expression is decreasing. But $m\ge 2(s-2)$, so we have

$$\frac{L}{R}<\left(\frac{s-1}{2(s-2)}-\frac{1}{s}\right)\left(\frac{s+1}{2(s-2)}+1\right)=\frac{3}{4}+\frac{3}{4(s-2)^2}+\frac{3}{2s(s-2)}.$$

As a function of s this expression is decreasing, and since $s\ge 5$, we have $L/R<14/15<1$.

Now assume $\alpha_p > 0$ and $\alpha_q = 0$ (the case where $\alpha_p = 0$, $\alpha_q > 0$ will follow in the same way). If $pd \mid n$, then $\alpha_d + \alpha_{pd} \le 1$, so that

$$\frac{\alpha_d}{d} + \frac{\alpha_{pd}}{pd} \le \frac{1}{d}. \tag{8}$$

We use (8) for $d = p^i$ with i odd, for $d = p^i q$ with i odd, and for $d = p^i q^j$ with i even and $j \ge 2$. But, if such a number $d \mid n$ has $v_p(d) = b$, we use $\alpha_d \le 1$. We thus have

$$L < \left(1 + \frac{1}{q}\right) \sum_{i \text{ odd}} \frac{1}{p^i} + \sum_{\substack{i \text{ even} \\ j \ge 2}} \frac{1}{p^i q^j} = \left(1 + \frac{1}{q}\right) \frac{p}{p^2 - 1} + \frac{p^2}{(p^2-1)q(q-1)},$$

and so

$$\frac{L}{R} < \frac{p(q+1)(q^2-1) + p^2(q+1)}{pq^2(p+q)} < \frac{q^2 + q - 1 + p + p/q}{q^2 + pq}.$$

Since $p(1 - 1/(q^2 - q)) > 1$, we have $p(q-1) > q - 1 + p/q$, so $L < R$.

Our last case is when $\alpha_p > 0, \alpha_q > 0$. If $pqd \mid n$ and $d > 1$, we have

$$\alpha_d + \alpha_{pd} \le 1, \quad \alpha_d + \alpha_{qd} \le 1, \quad \alpha_{pd} + \alpha_{pqd} \le 1, \quad \alpha_{qd} + \alpha_{pqd} \le 1,$$

so that as in the proof of Proposition 3, we have

$$\frac{\alpha_d}{d} + \frac{\alpha_{pd}}{pd} + \frac{\alpha_{qd}}{qd} + \frac{\alpha_{pqd}}{pqd} \le \frac{1}{d} + \frac{1}{pqd}.$$

We apply this when $d = p^i q^j$ when i is even and j is odd. When i is odd and $j = 0$, we apply (8). But, if such $d \mid n$ has either $v_p(d) = b$ or $v_q(d) = b$, we merely use $\alpha_d \le 1$. We thus have

$$L < \sum_{\substack{i \text{ even} \\ j \text{ odd}}} \left(\frac{1}{p^i q^j} + \frac{1}{p^{i+1} q^{j+1}}\right) + \sum_{i \text{ odd}} \frac{1}{p^i} = \sum_{\substack{\mathrm{rad}(u) \mid pq \\ \Omega(u) \text{ odd}}} \frac{1}{u} = R.$$

This concludes our proof. □

References

[1] A. Fish, *Random Liouville functions and normal sets*, Acta Arith., **120** (2005), 191–196.

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

[3] K. Kedlaya, *Product-free subsets of groups, then and now*, Communicating mathematics, 169–177, Contemp. Math., **479**, Amer. Math. Soc., Providence, RI, 2009.

[4] I. Schur, *Über die Kongruenz $x^m + y^m \equiv z^m \pmod p$*, Jahresb. Deutsche Math. Ver., **25** (1916), 114–117.

C. Pomerance
Department of Mathematics
Dartmouth College
Hanover, NH 03755, USA
e-mail: **carl.pomerance@dartmouth.edu**

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Sniadeckich 8, P.O. Box 21
00-956 Warszawa, Poland
e-mail: **schinzel@impan.pl**