

On a problem of Pillai and its generalizations

by

L. HAJDU (Debrecen) and N. SARADHA (Mumbai)

1. Introduction. For an integer $m \geq 2$ denote by S_m a set of m consecutive integers. Pillai [8] showed that in any set S_m with $m < 17$ there exists an integer x which is coprime to all other elements of S_m . Further, he showed that for $17 \leq m \leq 430$ there are infinitely many sets S_m for which no such x exists. The latter result was proved to be true for all $m \geq 17$ by Brauer [1]. Several other proofs were given by many authors; see [10] for some references. Pillai considered this problem in his attempt to prove that the product of two or more consecutive integers is never a perfect power. The latter problem was settled by Erdős and Selfridge [4].

The problem of Pillai has been generalized by Caro [2] in the following way. Let d be a positive integer. We say that S_m has *property* P_d if there exists an $x \in S_m$ such that for all $y \in S_m$, $y \neq x$ we have $\gcd(x, y) \leq d$. When $d = 1$, we get the original problem of Pillai. For fixed d , write $g(d)$ for the minimal m such that some S_m does not have property P_d . Further, let $G(d)$ be the smallest integer M such that for every $m \geq M$ property P_d does not hold for some S_m . Note that by the results of Pillai and Brauer we have $g(1) = G(1) = 17$. The existence of $g(d)$ and $G(d)$ for $d > 1$ was shown by Caro [2] who derived upper bounds for these quantities using estimates for the prime counting function $\pi(X)$. These bounds were improved by Saradha and Thangadurai [10]. Among other results they proved that

$$(1) \quad g(d) \leq 27d \log d \quad \text{for } d \geq 20, \quad G(d) \leq 44d \log d \quad \text{for } d \geq 11.$$

For $d \leq 19$ and $d \leq 10$, respectively, Saradha and Thangadurai obtained better bounds by a computer search. We reproduce the table from [10] as Table 1.

In this paper we consider the following further generalization of Pillai's problem. Let T be a non-empty set of positive integers. We say that S_m

2010 *Mathematics Subject Classification*: Primary 11A05; Secondary 11Y16.

Key words and phrases: Pillai's problem, greatest common divisor, blocks of consecutive integers.

Table 1. Bounds for $g(d)$ and $G(d)$ from [10]

d	$g(d) \leq$	$G(d) \leq$	d	$g(d) \leq$
2	79	134	11	763
3	151	239	12	898
4	208	335	13	928
5	286	463	14	1009
6	361	578	15	1114
7	424	650	16	1234
8	529	799	17	1315
9	628	879	18	1429
10	664	1050	19	1531

has *property* P_T if there exists an $x \in S_m$ such that for all $y \in S_m, y \neq x$ we have $\gcd(x, y) \in T$. Observe that if $1 \notin T$, then as for all $x \in \mathbb{Z}$ we have $\gcd(x, x + 1) = 1$, P_T does not hold for any S_m ($m \geq 2$). So with no further mention throughout the paper we assume that $1 \in T$. We write $g(T)$ for the minimal m such that property P_T does not hold for some S_m , and $G(T)$ for the smallest integer M such that for every $m \geq M$ property P_T does not hold for some S_m . Observe that these quantities do not exist for all T (e.g. for $T = \mathbb{Z}_{>0}$). Note also that the choices $T = \{1\}$ and $T = \{1, \dots, d\}$ yield the problems of Pillai and Caro, respectively. For simplicity, we keep the notation $P_d, g(d)$ and $G(d)$ in place of $P_{\{1, \dots, d\}}, g(\{1, \dots, d\})$ and $G(\{1, \dots, d\})$, respectively, whenever d is a positive integer.

The aim of the paper is twofold. On the one hand, we prove in a quantitative form the existence of $g(T)$ and $G(T)$, provided that T does not have “too many” elements. (For the precise formulation see the next section.) Our results cover all finite sets T , thus all the previously mentioned finiteness results are included. However, our assumptions allow certain infinite sets T as well. In particular, suppose S is a finite set of primes. Then as a simple corollary we deduce that T can be chosen as the set of so-called S -integers, i.e. positive integers composed of only the primes from S . Further, our results imply the solution of a generalization of Pillai’s problem to arithmetic progressions, hence as a special case, also a result of Ohtomo and Tamari [7]. Besides the above-mentioned theoretical results we give sharp bounds for $g(T)$ and $G(T)$ in the case of certain fixed choices of T . In particular, we provide an improvement upon Table 1 above. Furthermore, we calculate the exact values of these functions for $T = \{1, 2\}, \{1, 2, 3\}$ and for the sets $T = T_p = \{p^\alpha \mid \alpha \geq 0\}$, where p is an arbitrary prime.

The proofs of the theoretical results depend on the Chinese Remainder Theorem as in [2] and [10] together with finding enough primes in specific intervals. For the latter part, we use results of Dusart [3] which are better

than hitherto widely known results of Rosser and Schoenfeld [9] on the distribution of primes and related functions.

For certain choices of T , we find the exact values of $g(T)$ and $G(T)$. The theoretical upper bounds for these quantities are far from being satisfactory. In fact we have to handle a kind of “combinatorial explosion” to deal with an enormous number of possibilities. Hence our numerical results depend on several heuristic but efficient algorithms. We have implemented our algorithms in Maple. The calculation of the values $g(T)$ and $G(T)$ varied from a few seconds to several days. The most time consuming computation was calculating the value of $g(T_2) = G(T_2) = 86$ in Theorem 2.8, which has taken six days on an average PC.

2. Main results. We shall use the following notation. For any set T of positive integers, we denote by V_T the set of primes p such that $p \in V_T$ implies that p divides some integer in T . If $T = \{1\}$, then we set $V_T = \emptyset$. Also, $T(X)$ and $V_T(X)$ denote the sets of integers $\leq X$ in T and in V_T , respectively. For $c \in \mathbb{R}$ let $\lceil c \rceil$ and $\lfloor c \rfloor$ denote the upper and lower integer parts of c , respectively. That is,

$$\lceil c \rceil = \min\{n \in \mathbb{Z} \mid n \geq c\}, \quad \lfloor c \rfloor = \max\{n \in \mathbb{Z} \mid n \leq c\}.$$

THEOREM 2.1. *Suppose that*

$$(2) \quad |T(X)| \leq .1 \frac{X}{\log X}$$

for all $X \geq X_1$. Then for any integer $m \geq \max(425, 2X_1 + 1)$ there exists a set S_m for which P_T does not hold and hence

$$G(T) \leq \max(425, 2X_1 + 1).$$

The following statement is a simple consequence of the above theorem.

COROLLARY 2.2. *Suppose that for any $X \geq X_2$ we have*

$$(3) \quad |V_T(X)| \leq .25 \frac{\log X}{\log \log X}.$$

Then for any $m \geq \max(425, 2X_2 + 1)$ there exists a set S_m for which P_T does not hold and hence

$$G(T) \leq \max(425, 2X_2 + 1).$$

In particular, when $|V_T| = 1$, i.e. T contains only powers of a fixed prime p , we have $G(T) \leq G_0$ where G_0 is given by

$$(4) \quad G_0 = \begin{cases} 1296 & \text{for } p = 2, \\ 705 & \text{for } p = 3, \\ 431 & \text{for } p = 5, \\ 425 & \text{for } p \geq 7. \end{cases}$$

REMARK 2.3. When $V_T = \{2\}$, i.e. $T \subseteq T_2 = \{2^\alpha \mid \alpha \geq 0\}$, it follows from the work of Ohtomo and Tamari [7] that in fact one can take $G_0 = 384$. The connection between their work and the problem we are dealing with here is given in Theorem 2.10 below. Also, in Corollary 2.12, $G_0 = 384$ is improved to 86, which is best possible, since it is the exact value of $G(T_2)$.

When T is a finite set, then assumption (2) is satisfied for X sufficiently large. Thus $G(T)$ exists whenever T is finite. When V_T is finite, assumption (3) is satisfied and again $G(T)$ exists. In this case T is a subset of the set of S -integers with $S = V(T)$. Thus there are infinitely many infinite sets T for which $G(T)$ exists. On the other hand, the next result and its corollary demonstrate that some condition as in Theorem 2.1 is necessary for the existence of $G(T)$. In particular, it is possible that $T^c = \mathbb{Z}_{>0} \setminus T$ is infinite and yet $G(T)$ does not exist. In other words, property P_T holds for infinitely many values of m for all S_m .

PROPOSITION 2.4. *Let T be a set of positive integers and put $T^c = \mathbb{Z}_{>0} \setminus T$. Write $l_1 < l_2 < \dots$ for the elements of T^c , and put $n = |T^c|$ (which is possibly ∞). Suppose that any one of the following conditions holds:*

- (i) *n is finite and m is an integer $\geq \text{lcm}(l_1, \dots, l_n)$.*
- (ii) *For some $i \geq 1$,*

$$\text{lcm}(l_1, \dots, l_i) \leq l_{i+1}$$

and m is an integer satisfying

$$\text{lcm}(l_1, \dots, l_i) \leq m \leq l_{i+1}.$$

Then every set S_m has property P_T .

As a direct consequence of Proposition 2.4, and the definition of $G(T)$, we get the following corollary.

COROLLARY 2.5. *In the notation of Proposition 2.4, if either T^c is finite, or*

$$\text{lcm}(l_1, \dots, l_i) \leq l_{i+1}$$

for infinitely many indices i , then $G(T)$ does not exist.

REMARK 2.6. It seems to be an interesting task to characterize those sets T for which $G(T)$ exists. As a concrete problem we propose the following question. Let T be the set of integers which do not have prime divisors congruent to 1 modulo 4. Is it true that $G(T)$ exists?

Note that if $G(T)$ exists then $g(T)$ exists as well, and $g(T) \leq G(T)$. The following results sharpen the previously derived bounds for $g(T)$ and $G(T)$ for some “small” choices of T . In particular, we provide the exact values of these functions in some cases as well. We recall the notation $g(d) = g(\{1, \dots, d\})$ and $G(d) = G(\{1, \dots, d\})$.

THEOREM 2.7. *We have $g(2) = G(2) = 25$ and $g(3) = 49$, $G(3) = 53$. Further, for $4 \leq d \leq 19$ we have the improved version of Table 1 provided by Table 2.*

Table 2

d	$G(d) \leq$	d	$G(d) \leq$
4	144	12	594
5	195	13	623
6	248	14	664
7	299	15	753
8	362	16	818
9	421	17	863
10	458	18	952
11	521	19	1019

Next we consider sets T consisting of integers composed only of one prime, i.e. with $|V_T| = 1$.

THEOREM 2.8. *For a prime p put $T_p = \{p^\alpha \mid \alpha \geq 0\}$. Then the exact values of $g(T_p)$ and $G(T_p)$ are given by Table 3.*

Table 3

p	2	3	5	7	11	13	17	≥ 19
$g(T_p)$	86	77	47	43	27	27	17	17
$G(T_p)$	86	81	47	43	39	31	29	17

REMARK 2.9. From Table 3 we have, for instance, $g(T_{11}) = 27$ and $G(T_{11}) = 39$. Thus for $2 \leq m \leq 26$ and for $m = 38$, every S_m has property $P_{T_{11}}$, but for $m = 27$ and for all $m \geq 39$, there is some S_m not having this property. For example, one can easily check that

$$S_{27} = \{3611480, 3611481, 3611482, \dots, 3611506\}$$

does not have property $P_{T_{11}}$. For the values $28 \leq m \leq 37$, Table 3 does not give any information. However, our methods and algorithms provide complete information. In fact our calculations revealed that for $m = 28, 29, 30, 31, 32, 36, 37$ every S_m has property $P_{T_{11}}$, while for $m = 33, 34, 35$ there exist sets S_m not having this property. We have performed similar calculations for all T considered in the paper. The reader may consult the resulting tables [6].

Ohtomo and Tamari [7] generalized the problem of Pillai from consecutive integers to arithmetic progressions. Let D be a positive integer. Consider

sets of the form

$$S_m(D) = \{k + D, \dots, k + mD\} \quad \text{with } k > 0, \gcd(k, D) = 1.$$

Due to the gcd-condition, it is clear that no prime divisor of D divides any of the integers $k + iD$. In [7] it was shown that if m exceeds a value X_3 depending only on D , then for any i with $1 \leq i \leq n$ there exists a j with $1 \leq j \leq n, j \neq i$ such that $\gcd(k + iD, k + jD) > 1$.

To give a generalization of our previous results to this problem, let T be a set of positive integers with $1 \in T$ and $\gcd(t, D) = 1$ for all $t \in T$. We say that $S_m(D)$ has *property* $P_T(D)$ if there exists an $x \in S_m(D)$ such that for all $y \in S_m(D), y \neq x$, we have $\gcd(x, y) \in T$. Obviously, the case $D = 1$ gives back the original problem, that is, property $P_T(1)$ coincides with property P_T . We define $g(T, D)$ and $G(T, D)$ for the sets $S_m(D)$ similarly to the quantities $g(T)$ and $G(T)$. Note that with this notation the results of [7] imply that $G(\{1\}, D)$ exists for any D . In [7] it was also proved that $G(\{1\}, 2) \leq 384$.

The next result shows that the problem for arithmetic progressions and the original problem are in fact equivalent.

THEOREM 2.10. *Let D and T be as above. Put*

$$T' = \{l \cdot t \mid l \in L, t \in T\},$$

where L is the set of integers (including 1) composed exclusively of primes dividing D . Then for any $m \geq 2$, there exists a sequence $S_m(D)$ not having property $P_T(D)$ if and only if there exists a set S_m not having property $P_{T'}$.

The following two statements are immediate and obvious consequences of Theorems 2.1, 2.8 and 2.10. They extend and improve the previously mentioned results from [7].

COROLLARY 2.11. *Let D, T and T' be as in Theorem 2.10. Suppose that*

$$|T'(X)| \leq .1 \frac{X}{\log X}$$

for all $X \geq X_4$. Then for any integer $m \geq \max(425, 2X_4 + 1)$ there exists an arithmetic progression $S_m(D)$ for which $P_T(D)$ does not hold and hence

$$G(T, D) \leq \max(425, 2X_4 + 1).$$

COROLLARY 2.12. *$G(\{1\}, p^\beta)$ exists for any prime p and $\beta \geq 1$. Further, the values of $G(\{1\}, p^\beta) = G(T_p)$ are given by Table 3. In particular, $G(\{1\}, 2) = 86$.*

3. Lemmas. Our theoretical results depend on estimates for $\pi(X)$, the prime counting function which gives the number of primes $\leq X$. These esti-

mates are applied to get lower bounds for the number of primes in specific intervals. We make use of the following inequalities for $\pi(X)$.

LEMMA 3.1. *We have*

- (i) $\pi(X) > \frac{X}{\log X - 1}$ for $X \geq 5393$,
- (ii) $\pi(X) < \frac{X}{\log X} \left(1 + \frac{1.2762}{\log X}\right)$ for $X > 1$.

The lower and upper bounds for $\pi(X)$ in (i) and (ii) are due to Dusart [3]. The upper bound in (ii) is better than the bound (3.2) of Rosser and Schoenfeld from Theorem 1 of [9] where 1.2762 is replaced by 1.5. The lower bound in (i) implies that

$$(5) \quad \pi(X) > \frac{X}{\log X} \left(1 + \frac{1}{\log X}\right) \quad \text{for } X \geq 5393.$$

We begin with an application of Lemma 3.1 to get the next statement, which will be used when $T = \{1, \dots, d\}$. This lemma is already proved in [10]. However, for the convenience of the reader we give the main steps of the proof.

LEMMA 3.2. *Let $d \geq 1$. There exists $Y_0(d) > 0$ such that for all $Y \geq Y_0(d)$ there are at least $4d - 1$ primes in the interval $[Y, 2Y]$. In fact one may take $Y_0(d) = 9d \log d$ for $d \geq 20$. Further, for every $2 \leq d \leq 19$, the value of $Y_0(d)$ can be chosen as the bound for $G(d)$ in Table 1.*

Proof. Let $Y \geq 2697$. We require that

$$(6) \quad \pi(2Y) - \pi(Y) \geq 4d - 1.$$

By (5) and Lemma 3.1(ii), it is enough to show that

$$(7) \quad \frac{2Y}{\log 2Y} + \frac{2Y}{(\log 2Y)^2} - \frac{Y}{\log Y} - \frac{1.2762Y}{(\log Y)^2} \geq 4d - 1.$$

The left hand side of the above inequality is an increasing function of Y and the inequality is valid with $Y = Y_0(d) = 9d \log d$ for $d \geq 1000$. For $20 \leq d < 1000$, (6) is verified directly by computation.

Let $2 \leq d \leq 19$. For each of these values, first we find a value of $Y = Y'_0$ for which (7) is valid. Then we bring the value of Y'_0 down to $Y_0 = Y_0(d)$ by checking (6) with exact values of the function π by the help of a computer search. It was shown in [10] that for any integer m with the property that there are $4d - 1$ primes in the interval $[m, 2m]$, one can find a set S_m for which property P_d does not hold. Hence the least value $Y_0(d)$ satisfying (6) can be taken as an upper bound for $G(d)$. ■

The next application of Lemma 3.1 deals with the number of primes in a shorter interval than the one considered in the previous lemma.

LEMMA 3.3. *Let $Y \geq 212$. Then there exist at least*

$$\frac{.3Y}{\log Y} \quad \text{and} \quad \frac{.565Y}{\log Y}$$

primes in the intervals $(.65Y, Y]$ and $(Y, 1.65Y]$, respectively.

Proof. First we take $Y \geq 5393$. We apply Lemma 3.1 as in (7) and estimate

$$(8) \quad \pi(Y) - \pi(.65Y) \quad \text{and} \quad \pi(1.65Y) - \pi(Y)$$

to get the assertion of the lemma. Next we assume that $212 \leq Y < 5393$. In this range, we estimate the quantities in (8) with exact values of the π -function to get the statement. ■

REMARK 3.4. Note that by improving the constants in Lemma 3.3, one can increase the constant .1 in Theorem 2.1. For the purposes of this paper, Theorem 2.1 is sufficient.

Our last lemma will be used in the proof of Theorem 2.10. We denote by $[1, m]$ the set of positive integers not exceeding m . Further, if p is a prime and u is an integer then we denote by $\text{ord}_p(u)$ the largest exponent α such that $p^\alpha \mid u$ with the convention $\text{ord}_p(0) = \infty$.

LEMMA 3.5. *Let a and $d > 0$ be coprime integers, and consider the arithmetic progression $a + d, a + 2d, \dots, a + md$ with some $m \geq 1$. Let p be any prime not dividing d , and let $i_p \in [1, m]$ be an index such that $\text{ord}_p(a + i_p d) \geq \text{ord}_p(a + id)$ for all $i \in [1, m]$. Then for all $i \in [1, m]$, $i \neq i_p$, we have*

$$\text{ord}_p(a + id) = \text{ord}_p(i - i_p).$$

Proof. Put $\theta_p := \text{ord}_p(a + i_p d)$. Let $i \in [1, m]$, $i \neq i_p$. Then by the definition of i_p we have $\text{ord}_p(a + id) \leq \theta_p$. Assume to the contrary that

$$\text{ord}_p(a + id) \neq \text{ord}_p(i - i_p).$$

Then, as $p \nmid d$,

$$\text{ord}_p((a + id) - (a + i_p d)) \neq \text{ord}_p(a + id),$$

which implies that in fact $\text{ord}_p(a + id) = \theta_p$ and hence

$$\text{ord}_p((a + id) - (a + i_p d)) > \text{ord}_p(a + id).$$

By $p \nmid d$, we obtain

$$i \equiv i_p \pmod{p^{\theta_p+1}}.$$

Since d is invertible modulo p^{θ_p+1} , there exists an integer j such that

$$j \equiv -ad^{-1} \pmod{p^{\theta_p+1}}.$$

Hence we can find an index j_0 such that $j_0 \equiv j \pmod{p^{\theta_p+1}}$ and it lies between i and i_p . This gives $p^{\theta_p+1} \mid a + j_0d$, which contradicts the definition of i_p and θ_p . Hence the lemma follows. ■

4. Proofs of the qualitative results. In this section we give the proofs of our “theoretical” results.

Proof of Theorem 2.1. As in [2], [7] and [10], the proof is constructive and depends on the Chinese Remainder Theorem. Let $m \geq \max(425, 2X_1 + 1)$. If m is even, then let $M = m - 1$, otherwise set $M = m$. Let $k = (M - 1)/2$, and write

$$T(k) = T \cap \{1, \dots, k\} = \{t_1 < \dots < t_s\}$$

with $s = |T(k)|$. By Lemma 3.3, the intervals $I := (.65k, k]$ and $J := (k, 1.65k]$ contain more than $.3k/\log k$ and $.565k/\log k$ primes, respectively, whenever $k \geq 212$. Hence by our assumption on m , the intervals I and J contain respectively more than $.2k/\log k$ and $.4k/\log k$ primes which do not belong to T . As $s \leq .1k/\log k$, there are primes $.65k < p_1 < \dots < p_{2s} < p_{2s+1} \leq k$ and $k < q_1 < \dots < q_{4s} < q_{4s+1} \leq 1.65k$ such that $p_i, q_j \notin T$. Put

$$Q = \left(\frac{\prod_{p \leq k} p}{\prod_{i=1}^{2s} p_i} \right)^\gamma \quad \text{where} \quad \gamma = \left\lceil \frac{\log k}{\log 2} \right\rceil,$$

and consider the following system of linear congruences:

$$\begin{cases} x \equiv t_i \pmod{p_i} & \text{for } i = 1, \dots, s, \\ x \equiv -t_i \pmod{p_{s+i}} & \text{for } i = 1, \dots, s, \\ x \equiv p_i \pmod{q_i} & \text{for } i = 1, \dots, 2s, \\ x \equiv -p_i \pmod{q_{2s+i}} & \text{for } i = 1, \dots, 2s, \\ x \equiv -k - 1 \pmod{q_{4s+1}}, \\ x \equiv 0 \pmod{Q}. \end{cases}$$

By the Chinese Remainder Theorem this system has infinitely many solutions in positive integers x . We prove that neither of the sets $S_M = \{x - k, x - k + 1, \dots, x + k\}$ and $S_{M+1} = \{x - k, x - k + 1, \dots, x + k + 1\}$ has property P_T . Let H denote any of these sets. To prove that property P_T fails, for every $h_1 \in H$ we need to find another $h_2 \in H$ (with $h_1 \neq h_2$) such that $\gcd(h_1, h_2) \notin T$. Observe that every $h_1 \in H$ has one of the following forms:

- (i) $h_1 = x$,
- (ii) $h_1 = x \pm t_i, 1 \leq i \leq s$,
- (iii) $h_1 = x \pm p_i, 1 \leq i \leq 2s$,
- (iv) $h_1 = x \pm l$ where $1 \leq l \leq k, l \neq p_i$ with $1 \leq i \leq 2s$ and $l \notin T$,
- (v) $h_1 = x + k + 1$ when $H = S_{M+1}$.

We give below an appropriate choice of $h_2 \in H$ in each of the above cases.

(i) Let $h_1 = x$. Take $h_2 = x + p_{2s+1}$. Then $h_2 \in H$. By the last congruence of the system above, $p_{2s+1} \mid x$. Hence $\gcd(h_1, h_2) = p_{2s+1}$ and $p_{2s+1} \notin T$.

(ii) Let $h_1 = x - t_i, 1 \leq i \leq s$. Take $h_2 = x - t_i + p_i$. Then $\gcd(h_1, h_2) = p_i$ by the first branch of the congruences, and p_i does not belong to T . Let now $h_1 = x + t_i, 1 \leq i \leq s$. Take $h_2 = x + t_i - p_{s+i}$. Then $\gcd(h_1, h_2) = p_{s+i}$ by the second branch of the congruences, and p_{s+i} does not belong to T .

(iii) Suppose $h_1 = x - p_i, 1 \leq i \leq 2s$. Then we choose $h_2 = x - p_i + q_i$. We have $x < h_2 < x - .65k + 1.65k = x + k$. By the third branch of the congruences we get $\gcd(h_1, h_2) = q_i$, which is not in T . If $h_1 = x + p_i$, then we take $h_2 = x + p_i - q_{2s+i}$. Then $x > h_2 > x + .65k - 1.65k = x - k$. Further, the fourth branch of the congruences implies $\gcd(h_1, h_2) = q_{2s+i}$ and it is not in T .

(iv) Let $h_1 = x \pm l$ with l of the given form. Take $h_2 = x$. Then $\gcd(h_1, h_2) \mid l$. Note that any such l is divisible only by primes dividing Q . Hence by the last congruence of the system we get $\gcd(h_1, h_2) = l \notin T$.

(v) Finally, suppose that $h_1 = x + k + 1$ in the case of $H = S_{M+1}$. Take $h_2 = x + k + 1 - q_{4s+1}$. Then $h_2 > x - k$. By the fifth congruence we get $\gcd(h_1, h_2) = q_{4s+1}$ and it is not in T .

Since $m = M$ or $m = M + 1$, we see that P_T is not valid for some S_m whenever $m \geq \max(425, 2X_1 + 1)$. ■

Proof of Corollary 2.2. One can easily check that for any $X > 2$,

$$|T(X)| \leq \left\lceil \frac{\log X}{\log 2} \right\rceil^{|V_T(X)|}.$$

Further, a simple calculation yields, for $X \geq 425$,

$$\left\lceil \frac{\log X}{\log 2} \right\rceil^{.25 \frac{\log X}{\log \log X}} \leq .1 \frac{X}{\log X}.$$

Hence the first part of the corollary follows from Theorem 2.1.

In the case of $|V_T| = 1$, i.e. when $T \subseteq \{p^\alpha \mid \alpha \geq 0\}$ where p is a prime, we find that

$$|T(X)| \leq \left\lceil \frac{\log X}{\log p} \right\rceil \leq .1 \frac{X}{\log X}$$

for any $X \geq X_2 = (G_0 - 1)/2$. Thus by Theorem 2.1, $G(T) \leq \max(425, G_0)$, and the statement is proved. ■

Proof of Proposition 2.4. Suppose either (i) or (ii) holds. Let m be an integer with $\text{lcm}(l_1, \dots, l_i) \leq m$ where $i = n$ if (i) holds. Then in any set S_m there exists an element x which is coprime to $\text{lcm}(l_1, \dots, l_i)$, whence

$$(9) \quad \gcd(x, l_j) = 1 \quad \text{for all } j \text{ with } 1 \leq j \leq i.$$

Further note that for all $y \in S_m$, $y \neq x$, we have $\gcd(x, y) \leq m - 1$. This together with (9) and $1 \notin T^c$ implies that $\gcd(x, y) \notin T^c$ in both cases (i) and (ii). Now the statement follows. ■

Proof of Theorem 2.10. For integers u, v write $\gcd_D(u, v)$ for the greatest common divisor w of u, v such that $\gcd(w, D) = 1$. Note that if $u = \prod_p p^{\gamma_p}$ and $v = \prod_p p^{\delta_p}$, then $\gcd_D(u, v) = \prod_{p \nmid D} p^{\min(\gamma_p, \delta_p)}$.

Suppose first that property $P_{T'}$ does not hold for some set $S_m = \{k + 1, \dots, k + m\}$. For any prime p with $p < m$ and $p \nmid D$ let $i_p \in [1, m]$ be an index such that $\text{ord}_p(k + i_p) \geq \text{ord}_p(k + i)$ for all $i \in [1, m]$. Consider the following system of linear congruences:

$$(10) \quad \begin{cases} x \equiv 1 \pmod{D}, \\ x \equiv -i_p D \pmod{p^{\alpha_p}} \end{cases} \quad \text{for all } p < m, p \nmid D,$$

where $\alpha_p = \lceil \log m / \log p \rceil$. By the Chinese Remainder Theorem this system has infinitely many solutions. Let x_0 be one. Take a prime p with $p < m$, $p \nmid D$ and let $i \in [1, m]$ be an arbitrary index with $i \neq i_p$. Then by (10), Lemma 3.5 (applied with $a = k$ and $d = 1$), and the definitions of i_p and α_p we have

$$\begin{aligned} \text{ord}_p(x_0 + iD) &= \text{ord}_p(x_0 + i_p D + (i - i_p)D) = \text{ord}_p((i - i_p)D) \\ &= \text{ord}_p(i - i_p) = \text{ord}_p(k + i). \end{aligned}$$

Thus, by (10) and the choices of i_p and α_p , for any $1 \leq i < j \leq m$ we have

$$(11) \quad \gcd(x_0 + iD, x_0 + jD) = \gcd_D(k + i, k + j).$$

Since S_m does not have property $P_{T'}$, for any $i \in [1, m]$ there exists a $j \in [1, m]$, $j \neq i$, such that $\gcd(k + i, k + j) \notin T'$. Hence (11) implies that $\gcd(x_0 + iD, x_0 + jD) \notin T$. That is, the arithmetic progression $\{x_0 + D, \dots, x_0 + mD\}$ does not have property $P_T(D)$, and the “if” part of the statement follows.

To prove the “only if” part, assume that property $P_T(D)$ is not valid for the arithmetic progression $S_m(D) = \{k + D, \dots, k + mD\}$ (with $\gcd(k, D) = 1$). Now for any prime p with $p < m$, $p \nmid D$ let $i_p \in [1, m]$ be such that $\text{ord}_p(k + i_p D) \geq \text{ord}_p(k + iD)$ for all $i \in [1, m]$. Take the following system of linear congruences:

$$(12) \quad x \equiv -i_p \pmod{p^{\alpha_p}} \quad \text{for all } p < m, p \nmid D,$$

where α_p is as in (10). By the Chinese Remainder Theorem this system has infinitely many solutions. Let x_0 be one. By a similar argument to the first part of the proof (but now applying Lemma 3.5 with $a = k$ and $d = D$), one can easily check that by (12) and the choices of i_p and α_p we have

$$\gcd_D(x_0 + i, x_0 + j) = \gcd(k + iD, k + jD)$$

for any $1 \leq i < j \leq m$. Since $S_m(D)$ does not have property $P_T(D)$, we deduce that $\{x_0+1, \dots, x_0+m\}$ does not have property $P_{T'}$, and the theorem follows. ■

5. Proofs of the quantitative results. In this section we give the proofs of our results yielding sharp bounds for $g(T)$ and $G(T)$. We also find exact values of these quantities for certain choices of T .

5.1. Bounding the values of $g(d)$ and $G(d)$. Theorem 2.1 gives an upper bound for $G(T)$, and hence also for $g(T)$. However, for some fixed T , one can sharpen these bounds. In particular, when $T = \{1, \dots, d\}$ for some positive integer d , one can use a similar but more efficient method to bound these functions. Since the case $d = 1$ has been completely settled by Brauer [1], we may assume that $d \geq 2$. As noted in the Introduction, Saradha and Thangadurai [10] have obtained the bounds given in (1) and in Table 1. To get these bounds for $g(d)$ and $G(d)$, they needed to find an X such that there are at least $4d - 1$ primes in the intervals $[X/2, X]$ and $[X/2, 3X/4]$, respectively. The bounds are obtained using Lemma 3.2 and some computation. By an improved inductive argument we show below that one can take the interval $[X/2, X]$ for both quantities and we obtain reduced bounds for both $g(d)$ and $G(d)$. In fact, by getting rid of X we can work with slightly simplified settings. This is helpful also in deriving sharper bounds for $g(d)$ and $G(d)$ later on. In what follows, p_i denotes the i th prime. We shall use the obvious inequality

$$p_{i+j} \geq p_i + 2j \quad \text{for } i \geq 2 \text{ and } j \geq 0$$

with no further mention.

LEMMA 5.1. *Let $d \geq 2$ be fixed. Assume that for some $t \geq 2$ we have $2p_{t+1} > p_{t+4d-1}$. Let $M_1(t) = \max_{1 \leq i \leq 2d-1} (p_{t+2d+i} - p_{t+i})$ and $M_2(t) = p_{t+2d} - d$. Then $M_1(t) \leq p_{t+1} - 1$ and there exists an integer x_0 such that the interval*

$$J_1(t) = [x_0 - M_1(t), x_0 + M_2(t)]$$

does not have property P_d . Further, for any integers i_1, i_2 with $M_1(t) \leq i_1 \leq p_{t+1} - 1$ and $M_2(t) \leq i_2 \leq p_{t+2d} - 1$ the interval $[x_0 - i_1, x_0 + i_2]$ does not have property P_d .

Proof. In fact the statement immediately follows from the explanation given in Section 3 of [10]. However, for the convenience of the reader we give the proof.

Since $2p_{t+1} > p_{t+4d-1}$, for any $i \in \{1, \dots, 2d - 1\}$ we have

$$p_{t+2d+i} - p_{t+i} \leq p_{t+4d-1} - p_{t+1} \leq 2p_{t+1} - 1 - p_{t+1} = p_{t+1} - 1.$$

Hence $M_1(t) \leq p_{t+1} - 1$. Note that $p_{t+1} > p_{t+4d-1}/2 > d$. For $i = 1, \dots, t$ set $\beta_i = \lceil \log(d+1)/\log p_i \rceil$. By the Chinese Remainder Theorem we can find infinitely many integers x satisfying the following linear congruence system:

$$\begin{cases} x \equiv -i \pmod{p_{t+d-i+1}} & \text{for } i = 1, \dots, d, \\ x \equiv i \pmod{p_{t+d+i}} & \text{for } i = 1, \dots, d, \\ x \equiv -p_{t+i} \pmod{p_{t+2d+i}} & \text{for } i = 1, \dots, 2d - 1, \\ x \equiv 0 \pmod{\prod_{i=1}^t p_i^{\beta_i}}. \end{cases}$$

Let x_0 be any solution, and set $J_1(t) = [x_0 - M_1(t), x_0 + M_2(t)]$. We claim that the integers in this interval do not have property P_d . That is, we need to show that for any $r \in J_1(t)$ there is another $s \in J_1(t)$ such that $\gcd(r, s) > d$. We prove this by distinguishing five different cases.

(1) If $r = x_0 + i$ with $1 \leq i \leq d$, then choose $s = x_0 + i + p_{t+d-i+1}$. Since $i + p_{t+d-i+1} \leq p_{t+2d} - d$, we have $s \in J_1(t)$. Further, by the first congruence of the above system we find $\gcd(r, s) = p_{t+d-i+1} > d$.

(2) If $r = x_0 - i$ with $1 \leq i \leq d$, then choose $s = x_0 - i + p_{t+d+i}$. As $p_{t+d+i} - i \leq p_{t+2d} - d$, we see that $s \in J_1(t)$. Furthermore, the second congruence yields $\gcd(r, s) = p_{t+d+i} > d$.

(3) If $r = x_0 + p_{t+i}$ with $1 \leq i \leq 2d - 1$, then choose $s = x_0 + p_{t+i} - p_{t+2d+i}$. Since by definition $p_{t+2d+i} - p_{t+i} \leq M_1(t)$, we have $s \in J_1(t)$. Moreover, by the third congruence we obtain $\gcd(r, s) = p_{t+2d+i} > d$.

(4) If $r = x_0$, then choose $s = x_0 + d + 1$. Obviously, $s \in J_1(t)$. Further, by the last congruence we have $d + 1 \mid x_0$, whence $\gcd(r, s) = d + 1 > d$.

(5) Finally, suppose that r does not have any of the above forms. We show that then $s = x_0$ is an appropriate choice. (Obviously, $x_0 \in J_1(t)$.) Write $r = x_0 + j$ with $M_2(t) \geq j \geq -M_1(t)$. Note that by (1), (2) and (4), we have $|j| > d$. Further, since

$$2p_{t+1} > p_{t+2d} > M_2(t) \geq j \geq -M_1(t) > -p_{t+1},$$

and $j \neq p_{t+i}$ ($i = 1, \dots, 2d - 1$) by (3), all the prime divisors of j are $\leq p_t$. Write $j = \prod_{i=1}^t p_i^{\gamma_i}$. If for some i we have $\gamma_i > \beta_i$, then by the last congruence $p_i^{\beta_i}$ divides both x_0 and j , whence by the definition of β_i we have $\gcd(r, s) = \gcd(x_0 + j, x_0) \geq p_i^{\beta_i} > d$. Otherwise, if $\gamma_i \leq \beta_i$ for all i , then $j \mid x_0$, that is, $\gcd(r, s) = |j| > d$ again.

Finally, take any i_1, i_2 with

$$M_1(t) \leq i_1 \leq p_{t+1} - 1 \quad \text{and} \quad M_2(t) \leq i_2 \leq p_{t+2d} - 1.$$

Since $[x_0 - i_1, x_0 + i_2]$ contains $J_1(t)$, the points (1)–(4) work just as previously. Take an $r \in [x_0 - i_1, x_0 + i_2]$ not considered in these points, and write $r = x_0 + j$ with $i_2 \geq j \geq -i_1$. Since

$$2p_{t+1} > p_{t+2d} > i_2 \geq j \geq -i_1 > -p_{t+1},$$

j cannot have prime divisors exceeding p_t . From this point on, the argument in (5) shows that property P_d does not hold for the integers in the interval $[x_0 - i_1, x_0 + i_2]$ either, and the statement follows. ■

REMARK 5.2. Here and later on let $I(J)$ denote the number of integers in an interval J . For later use, note that $I(J_1(t)) = M_1(t) + M_2(t) + 1 > p_{t+2d} + 3d$. For a fixed d let x be an arbitrary solution to the congruence system occurring in the proof of Lemma 5.1, and put $J_2(t) = [x - p_{t+1} + 1, x + p_{t+2d} - 1]$. Observe that $J_1(t) \subseteq J_2(t)$. Let

$$\mathcal{T} = \mathcal{T}_d = \{t \mid 2p_{t+1} > p_{t+4d-1}\}.$$

By Lemma 5.1 we know that for any

$$(13) \quad m \in \bigcup_{t \in \mathcal{T}} [I(J_1(t)), I(J_2(t))] =: L_d$$

there is a set S_m which does not have property P_d . Lemma 5.1 already yields $g(d) \leq I(J_1(t_0))$ where t_0 is the smallest element of \mathcal{T} . Further, note that if $t_1, t_2 \in \mathcal{T}$ with $t_1 \leq t_2$ then $I(J_2(t_1)) \leq I(J_2(t_2))$. This together with the above observation based upon (13) makes it possible to get improved bounds for the values of $G(d)$ as well (see the proof of Theorem 2.7 later on).

5.2. H -covering. In the context of Pillai’s problem, Gassko [5] studied so-called coverings of S_m by primes (see Lemmas 3.1 and 3.2 in [5]). We outline the theory in a more general form which is convenient for our purposes. Let $H = \{h_1, \dots, h_t\}$ be a set of pairwise coprime integers such that $1 < h_1 < \dots < h_t$. We say that H covers a set $L \subseteq \mathbb{Z}$ if there exists a function $f : H \rightarrow L$ such that for each $x \in L$ there is a $h \in H$ and a $y \in L, y \neq x$, such that $h \mid x - y$ and $f(h) \in \{x, y\}$. We also say that f is an H -covering function of L and that h covers x . Note that there may be more than one h covering x . Also there may be elements $h \in H$ which do not cover any x . We refer to such elements as *spared elements*. We call H a *minimal covering* of L if no proper subset H' of H covers L . Note that when H is a minimal covering of L , for each $h \in H$ there exists an $x \in L$ which is covered only by h , in other words, there are no spared elements.

In what follows, H -coverings of intervals $[1, m]$ will play a vital role. Observe that if an $h \in H$ covers some $x \in [1, m]$, then $h < m$. Hence when we consider an H -covering of $[1, m]$, we may assume that every $h \in H$ satisfies $h < m$.

LEMMA 5.3. *Let H be a set of pairwise coprime integers. Then H covers $[1, m]$ if and only if there exists a function $f_1 : H \rightarrow [1, m]$ with the following properties:*

- (i) $f_1(h) \leq \min(h, m - h)$ for all $h \in H$,
- (ii) for all $x \in [1, m]$, there exists an $h \in H$ with $x \equiv f_1(h) \pmod{h}$.

Proof. Suppose first that $f_1 : H \rightarrow [1, m]$ satisfies (i) and (ii). We show that H covers $[1, m]$. Let $x \in [1, m]$. By (ii), there exists $h \in H$ such that $x \equiv f_1(h) \pmod{h}$. If $x \neq f_1(h)$, then we take $y = f_1(h)$. If $x = f_1(h)$, we take $y = f_1(h) + h$. Using (i), in either case we see that $y \in [1, m]$, $y \neq x$ and $h \mid x - y$. Hence H covers $[1, m]$.

Suppose now that H covers $[1, m]$. Assume that $f : H \rightarrow [1, m]$ is an H -covering function. Suppose that $f(h) > h$ for some $h \in H$. Let $f(h) = rh + \theta_h$ with $1 \leq \theta_h \leq h$. Consider $f_1 : H \rightarrow [1, m]$ defined by

$$f_1(h) = \begin{cases} f(h) & \text{if } f(h) \leq h, \\ \theta_h & \text{if } f(h) > h. \end{cases}$$

Then f_1 is obviously an H -covering function of $[1, m]$. Hence (ii) is automatically satisfied. To prove (i), take an arbitrary $h \in H$. Then for any y covered by h with $y \neq f_1(h)$ we have $y > f_1(h)$ since h divides $y - f_1(h)$ and $f_1(h) \leq h$. Hence for some integer $r > 0$, we have

$$f_1(h) = y - rh \leq m - h.$$

Thus we always have

$$f_1(h) \leq \min(h, m - h),$$

that is, (i) is also valid. ■

The following lemma is new. It plays a fundamental role in our computational arguments (in particular in the proofs of Theorems 2.7 and 2.8), as it transforms the problem for S_m into a covering problem for $[1, m]$.

LEMMA 5.4. *Let m be a positive integer, and H be a set of pairwise coprime integers ≥ 2 . The following two statements are equivalent:*

- (i) *There exists a set S_m such that for each $x \in S_m$ there is a $y \in S_m$, $y \neq x$, and an $h \in H$ with $\gcd(x, y) = h$.*
- (ii) *The set H covers the interval $[1, m]$.*

Proof. Suppose first that (i) is valid, and write $S_m = \{k + 1, \dots, k + m\}$. Define $f : H \rightarrow [1, m]$ in the following way. For any $h \in H$ let $f(h)$ be the smallest $l \in [1, m]$ for which $h \mid k + l$. If such an l does not exist then put $f(h) = 1$. We show that f is an H -covering function of $[1, m]$. Let $i \in [1, m]$. Then by (i) there exists a $j \in [1, m]$, $j \neq i$, and $h \in H$ such that $\gcd(k + i, k + j) = h$. Fix this h , and let $i^* \in \{1, \dots, m\} \setminus \{i\}$ be the smallest with $h \mid k + i^*$. Then h divides $i - i^* \neq 0$ and by the minimality of i^* we also have $f(h) \in \{i, i^*\}$. Thus H covers $[1, m]$ indeed.

Assume now that (ii) holds. Then there is $f : H \rightarrow [1, m]$ such that for every $i \in [1, m]$ there exists a $j \in [1, m]$, $j \neq i$, and an $h \in H$ such that

$h \mid i - j$ and $f(h) \in \{i, j\}$. By the Chinese Remainder Theorem, since the elements of H are pairwise coprime, there exists an integer k such that

$$k \equiv -i \left(\text{mod } \prod_{\substack{h \in H \\ f(h)=i}} h \right) \quad (i = 1, \dots, m).$$

Put $S_m = \{k + 1, \dots, k + m\}$, and let $x = k + i$ be an element of S_m . Take any $j \in [1, m]$, $j \neq i$, and $h \in H$ such that $h \mid i - j$ and $f(h) \in \{i, j\}$. By the above congruence system we deduce that either $h \mid k + i$ or $h \mid k + j$. However, then $h \mid i - j$ implies that in fact both $h \mid k + i$ and $h \mid k + j$. Hence by putting $y = k + (i + h)$ if $i < j$ and $y = k + (i - h)$ if $i > j$, we get $\text{gcd}(x, y) = h$ and (i) follows. ■

REMARK 5.5. In some cases we need to take H such that $\text{gcd}(h, h') > 1$ for some $h, h' \in H$. Then we need to modify Lemma 5.4 and the underlying notation in a suitable way. We briefly explain a case considered in this paper. Suppose that

$$H = \{h_1, \dots, h_t, p_1^{\alpha_1}, p_2^{\alpha_2}, p_1 p_2\}$$

where the h_i 's are pairwise coprime, p_1, p_2 are distinct primes not dividing any of the h_i 's, and α_1, α_2 are positive integers. In this case we say that H covers $[1, m]$ if there exists a function $f : H \rightarrow [1, m]$ as before with the additional properties that

$$(14) \quad f(p_1 p_2) \equiv f(p_1^{\alpha_1}) \pmod{p_1} \quad \text{and} \quad f(p_1 p_2) \equiv f(p_2^{\alpha_2}) \pmod{p_2}.$$

In other words, $f(p_1 p_2)$ gets fixed in accordance with $f(p_1^{\alpha_1})$ and $f(p_2^{\alpha_2})$. Here we only consider the case of minimal coverings. Hence by Lemma 5.3, the congruences in (14) make sense. We show that Lemma 5.4 is valid in this case also. As in the proof of the lemma, we see that (i) implies (ii).

Suppose now that $[1, m]$ is covered by such an H . As in the lemma, choose k such that

$$k \equiv -i \left(\text{mod } \prod_{\substack{h \in H \setminus \{p_1 p_2\} \\ f(h)=i}} h \right) \quad (i = 1, \dots, m).$$

Observing that then by (14) in fact

$$k \equiv -f(p_1 p_2) \pmod{p_1 p_2},$$

we deduce (i) as in the proof of Lemma 5.4.

We shall use such an H -covering to find the exact values of $g(3)$ and $G(3)$, with the particular choice

$$H = \{p \mid p \text{ is a prime } > 3\} \cup \{4, 6, 9\}.$$

Now we give an algorithm which checks if a given set H covers $[1, m]$ or not. For this we need some further notation. Let m be a fixed integer.

For each $h \in H$ with $h < m$ put $U(h) := \min(h, m - h)$. Thus if f is an H -covering of $[1, m]$, then

$$(15) \quad (f(h_1), \dots, f(h_t)) \in [1, U(h_1)] \times \dots \times [1, U(h_t)].$$

Further, for any $n \in \mathbb{Z}_{>0}$ and $r \in \mathbb{Z}$ let

$$R(r, n) = \{z \in \mathbb{Z} \mid z \equiv r \pmod{n}\}.$$

Then the elements of $[1, m]$ covered by an h_i ($1 \leq i \leq t$) are given by $R(f(h_i), h_i) \cap [1, m]$, implying

$$(16) \quad [1, m] = \bigcup_{i=1}^t R(f(h_i), h_i) \cap [1, m].$$

Thus in principle, we have to check (16) for all possible $U(h_1) \dots U(h_t)$ t -tuples given by (15). This can be done by the use of a nested system of t loops where the i th loop runs from 1 to $U(h_i)$ for $1 \leq i \leq t$. We do this checking in a more “economical” way by the following algorithm.

COVERING ALGORITHM. Given $H = \{h_1, \dots, h_t\}$, the algorithm checks whether there is a t -tuple $(f(h_1), \dots, f(h_t))$ yielding an H -covering of $[1, m]$.

Initialization. Let $H' = \{h'_1, \dots, h'_r\}$ be a subset of H , and (after reindexing H if necessary) write $H \setminus H' = \{h_1, \dots, h_{t^*}\}$ where $r + t^* = t$.

(CA.1) For each r -tuple $(f(h'_1), \dots, f(h'_r))$ with $1 \leq f(h'_i) \leq U(h'_i)$ ($i = 1, \dots, r$) execute the following steps.

(CA.2) Let $s = 1$.

(CA.3) Put $f(h_s) = 1$.

(CA.4) Let T_1 be the set which is “already covered” by the tuple

$$(f(h'_1), \dots, f(h'_r), f(h_1), \dots, f(h_s)),$$

and let T_2 be the “remaining” set. That is, put

$$(17) \quad T_1 = \bigcup_{i=1}^r R(f(h'_i), h'_i) \cup \bigcup_{i=1}^s R(f(h_i), h_i) \cap [1, m],$$

$$(18) \quad T_2 = [1, m] \setminus T_1.$$

(CA.5) For each $i = s + 1, \dots, t^*$, put

$$V_i := \max_{1 \leq l \leq U(h_i)} \#(R(l, h_i) \cap T_2),$$

that is, V_i denotes the maximal number of “remaining” elements that can be covered by h_i .

(CA.6) If $\sum_{i=s+1}^{t^*} V_i \geq \#T_2$, then do the following. If $s + 1 < t^*$ then increase s by one, and return to step (CA.3). If $s + 1 = t^*$, then with $f(h_{t^*}) = l$

for the l maximizing V_{t^*} in (CA.5), the tuple $(f(h'_1), \dots, f(h'_r), f(h_1), \dots, f(h_{t^*}))$ yields an H -covering of $[1, m]$ and we stop.

(CA.7) If $\sum_{i=s+1}^{t^*} V_i < \#T_2$, then $(f(h'_1), \dots, f(h'_r), f(h_1), \dots, f(h_s))$ cannot be extended to an H -covering of $[1, m]$. If

$$(f(h_1), \dots, f(h_s)) \neq (U(h_1), \dots, U(h_s)),$$

then find the largest index j such that $f(h_j) < U(h_j)$. Change the value of s to j , increase the value of $f(h_j) = f(h_s)$ by one (that is, we now have the tuple $(f(h_1), \dots, f(h_s)) = (f(h_1), \dots, f(h_{j-1}), f(h_j) + 1)$) and return to step (CA.4). If

$$(f(h_1), \dots, f(h_s)) = (U(h_1), \dots, U(h_s)),$$

then proceed to the next step.

(CA.8) Take the next possibility for the tuple $(f(h'_1), \dots, f(h'_r))$ in (CA.1), and go to step (CA.2). If all possibilities for this tuple have already been considered, then (since we have never obtained an H -covering in step (CA.6)) we conclude that there is no H -covering for $[1, m]$ and stop.

As one can easily check, the algorithm stops after a finite number of steps, and either finds a concrete H -covering of $[1, m]$, or concludes that there is no such covering. We illustrate how the algorithm works by an example. We take the original problem of Pillai, i.e. the case $T = \{1\}$ and $m = 17$. Observe that by Lemma 5.4 there exists a set S_{17} which does not have property P_T for this T if and only if $[1, 17]$ can be covered by the set $H = \{2, 3, 5, 7, 11, 13\}$.

Starting the algorithm with $H' = \emptyset$, at step (CA.3) we have $f(h_1) = 1$, hence in (CA.4) we get

$$T_1 = \{1, 3, 5, 7, 9, 11, 13, 15, 17\}, \quad T_2 = \{2, 4, 6, 8, 10, 12, 14, 16\}.$$

In (CA.5) we calculate the values

$$V_2 = 3, \quad V_3 = 2, \quad V_4 = 2, \quad V_5 = 1, \quad V_6 = 1.$$

As their sum is $9 > 8 = \#T_2$, in (CA.6) we put $s := 2$ and go to (CA.3). Here we have

$$(f(h_1), f(h_2)) = (1, 1),$$

which in (CA.4) yields

$$T_2 = \{2, 6, 8, 12, 14\}.$$

Now in (CA.5) we obtain

$$V_3 = 2, \quad V_4 = 1, \quad V_5 = 1, \quad V_6 = 1.$$

Since their sum is $5 = \#T_2$, we put $s := 3$ in (CA.6) and go to (CA.3). Now we get the tuple

$$(f(h_1), f(h_2), f(h_3)) = (1, 1, 1),$$

yielding

$$T_2 = \{2, 8, 12, 14\}$$

and

$$V_4 = 1, \quad V_5 = 1, \quad V_6 = 1.$$

As $V_4 + V_5 + V_6 = 3 < 4 = \#T_2$, this tuple cannot be extended to an H -covering of $[1, 17]$. So in (CA.7) we define $s := 3$ and return to (CA.4) with the tuple

$$(f(h_1), f(h_2), f(h_3)) = (1, 1, 2).$$

This gives

$$T_2 = \{6, 8, 14\}.$$

Now after a few similar steps we reach the tuple

$$(f(h_1), f(h_2), f(h_3), f(h_4), f(h_5)) = (1, 1, 2, 1, 6).$$

At this point we obtain $T_2 = \{14\}$ and $V_6 = 1$. Hence in step (CA.6) we conclude that

$$(f(h_1), f(h_2), f(h_3), f(h_4), f(h_5), f(h_6)) = (1, 1, 2, 1, 6, 1)$$

is an H -covering of $[1, 17]$ and the algorithm terminates.

REMARK 5.6. We note that the H -covering for $m = 17$ given by Pillai was

$$(f(2), f(3), f(5), f(7), f(11), f(13)) = (1, 2, 1, 3, 1, 4).$$

The above algorithm is quite effective for relatively small values of m (say up to $m \leq 60$), in particular if $[1, m]$ has many H -coverings and we need only find one. When $[1, m]$ does not have an H -covering, then we need to exclude all the possibilities, which is rather time consuming for larger values of m . In fact the choice $H' = \emptyset$ has been sufficient in most cases. However, when $t = |H|$ is “large”, say about 20, it is more efficient to begin with a given set of elements H' . For example, in Theorem 2.8 to get $g(T_2) = G(T_2) = 86$, we have taken $H = \{p \mid p \text{ is an odd prime} < 86\}$ and $H' = \{3, 5, 7, 83\}$.

5.3. An algorithm for calculating $g(T)$ and $G(T)$ for fixed T .

Recall that $g(T)$ is the smallest integer such that there exists some set $S_{g(T)}$ for which property P_T does not hold and $G(T)$ is the smallest integer such that, for all $m \geq G(T)$, there exists some S_m for which P_T does not hold. Thus $g(T) \leq G(T)$. Since $1 \in T$, by Pillai’s result we have

$$17 \leq g(T) \leq G(T).$$

Under some assumptions on T , Table 1, Theorem 2.1 and Corollary 2.2 provide upper bounds for $G(T)$. Let us assume from now on that $G(T) \leq M_0$, say. To find a better bound for $g(T)$ or $G(T)$, we need to check, for every m with $17 \leq m \leq M_0$, whether or not there exists an S_m for which property

P_T holds. Using Lemma 5.4, we need only check if $[1, m]$ has H -covering with the appropriate H for each m with $17 \leq m \leq M_0$. For example, in the original case considered by Pillai, to calculate $G(1)$ one needs to consider the H -coverings of $[1, m]$ where H is the set of all primes.

To calculate $g(T)$ and $G(T)$ we provide the following algorithm. For a set L of positive integers we denote by $\min(L)$ and $\max(L)$ the minimal and maximal elements of L , respectively.

PRINCIPAL ALGORITHM

Step 1. Starting from $m = 17$, check whether $[1, m]$ has an H -covering or not. This is done using the Covering Algorithm. If $[1, m]$ has no H -covering, then we take $[1, m + 1]$ and repeat the process. If m_0 is the first value such that $[1, m_0]$ has an H -covering, then we conclude that $g(T) = m_0$.

Step 2. For each m with $m_0 < m < M_0$ check if $[1, m]$ has an H -covering or not. If there is such a covering in every case, then we have $G(T) = m_0$. Otherwise, if k_0 is the largest integer in (m_0, M_0) such that $[1, k_0]$ has no H -covering, then we conclude that $G(T) = k_0 + 1$. To execute this step, we provide the following heuristic algorithm, which is quite efficient.

WEIGHTED ALGORITHM. The algorithm tries to find an H -covering f for $[1, m]$ by fixing the values of f for the elements H in a certain order.

(WA.1) Let $s = 0$.

(WA.2) Let T_2 denote the set of elements from $[1, m]$ which are not covered by h'_1, \dots, h'_s of H . It is in fact given by (18). (If $s = 0$ then $T_2 = [1, m]$, and we do not assume any ordering of the h'_i s here.) If T_2 is empty, then we have an H -covering of $[1, m]$ already by $\{h'_1, \dots, h'_s\}$. The elements of $H \setminus \{h'_1, \dots, h'_s\}$ are spared elements and we take their f -values arbitrarily and stop. In this case H is not a minimal covering.

(WA.3) Define the weight function W for positive integers in the following way. Let α, β be some fixed positive numbers, and set

$$(19) \quad W(h) = W(h, \alpha, \beta) = h^\alpha \max_{1 \leq l \leq U(h)} \left(\sum_{i \in T_2 \cap R(l, h)} w(i, \beta) \right)$$

with

$$w(i, \beta) = (\min(i + 1 - \min(T_2), \max(T_2) + 1 - i))^\beta.$$

We choose h'_{s+1} as the h -value in $H \setminus \{h'_1, \dots, h'_s\}$ for which $W(h)$ attains its maximum. Then we take $f(h'_{s+1}) = l$ where l is the value which maximizes the term in brackets in (19) with $h = h'_{s+1}$.

(WA.4) If $s = t$ (the cardinality of H) then we stop. Otherwise, we increase s by one and go to step (WA.2).

After the algorithm has terminated, we check if $(f(h'_1), \dots, f(h'_t))$ covers $[1, m]$ or not. If so, we are done, otherwise we take other values for α and β , and repeat the whole process.

Note that the weight function in (WA.3) is defined in such a way that the elements of T_2 which get covered are given due weights (elements of T_2 closer to the “middle” have larger weights). Also it depends on the “sizes” of the elements $h \in H$ whose f -value gets fixed at this step (larger elements of H have larger weights). Our computations suggest that it is better to change the parameters α and β for different cases. For different sets H and for different values of m some weight values yield a covering but some other values not – and apparently it is achieved in a random way.

We illustrate the Weighted Algorithm by an example. Let $m = 23$ and $H = \{2, 3, 5, 7, 11, 13, 19\}$. To find an H -covering f of $[1, 23]$, we use the weight function $W(h)$ with $\alpha = .25$ and $\beta = .5$. We begin with $h'_1 = 2$ and $f(h'_1) = 1$. Then

$$T_2 = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}.$$

We find that $W(3)$ is maximal and the maximum is attained at $l = 1$. Hence $h'_2 = 3$ and $f(h'_2) = 1$. Thus the integers 4, 10, 16, 22 get covered, and we deduce that at this stage

$$T_2 = \{2, 6, 8, 12, 14, 18, 20\}.$$

Now $W(5)$ is maximal, at $l = 3$. Hence $h'_3 = 5$ and $f(h'_3) = 3$. This choice covers $\{8, 18\}$, whence

$$T_2 = \{2, 6, 12, 14, 20\}.$$

Here $W(11)$ is maximal with $l = 1$. Thus $h'_4 = 11$ and $f(h'_4) = 1$ covering 12, so that

$$T_2 = \{2, 6, 14, 20\}.$$

Then we find that $W(7)$ is maximal with $l = 6$, yielding $h'_5 = 7$, $f(h'_5) = 6$ and $T_2 = \{2, 14\}$. Lastly, $h'_6 = 19$, $f(h'_6) = 2$ covering 2 and then $h'_7 = 13$, $f(h'_7) = 1$ covering 14. This altogether yields the H -covering

$$(f(2), f(3), f(5), f(7), f(11), f(13), f(19)) = (1, 1, 3, 6, 1, 1, 2)$$

of $[1, 23]$. Here the prime 17 is spared. Compare this with the H -covering of Pillai given by

$$(f(2), f(3), f(5), f(7), f(11), f(13), f(17), f(19)) = (1, 2, 1, 3, 1, 4, 1, 3).$$

5.4. Proof of Theorems 2.7 and 2.8. In this final subsection we give the proofs of our “numerical” results.

Proof of Theorem 2.7. First we explain how to prove the bounds provided by Table 2. For this purpose one can use the procedure explained in

Section 5.2. We illustrate this by means of an example. Let $d = 4$. By Table 1, we have $g(d) \leq 208$ and $G(d) \leq 335$. We show that $G(d) \leq 144$. By Remark 5.2, we can achieve this by constructing the set L_4 . Note that in the definition of L_4 we need to consider only those t for which

$$p_{t+2d} = p_{t+8} < 335 - 3d = 323.$$

This yields $t \leq 66$. Further, since $t \in \mathcal{T}$, we have $2p_{t+1} > p_{t+15}$, which implies $t = 19$ or $t \geq 21$. Now for $t = 19$ and for each t with $21 \leq t \leq 66$ we calculate $I(J_1(t))$ and $I(J_2(t))$ given by

$$I(J_1(t)) = M_1(t) + M_2(t) + 1 = \max_{1 \leq i \leq 7} (p_{t+8+i} - p_{t+i}) + p_{t+8} - 3,$$

$$I(J_2(t)) = p_{t+1} + p_{t+2d} - 1.$$

Thus for example, when $t = 19$ we have $I(J_1(t)) = 144$ and $I(J_2(t)) = 173$ giving the interval $[144, 173]$. By taking the union of all such intervals for $t = 19$ and $21 \leq t \leq 66$ we find that $L_4 = [144, 703]$. Thus $G(4) \leq 144$.

The bounds for $G(d)$ for all values of $5 \leq d \leq 19$ are obtained similarly.

Now we explain the procedure for finding the exact values for $g(2)$, $G(2)$ and $g(3)$, $G(3)$. We start with the case of finding $g(2)$ and $G(2)$. First, by following the illustration in the previous paragraph, we get $G(2) \leq 56$. Now we use the Covering Algorithm provided in Section 5.2. Take an arbitrary m with $17 \leq m \leq 55$ and put

$$H = \{p \mid p \text{ is an odd prime } < m\} \cup \{4\}.$$

Observe that by Lemma 5.4 there exists a set S_m for which P_2 does not hold if and only if $[1, m]$ has an H -covering. We begin with $m = 17$, when $H = \{3, 4, 5, 7, 11, 13\}$. By the Covering Algorithm we find that $[1, m]$ has no H -covering. Thus P_2 holds for any S_{17} and hence $G(2) \geq g(2) > 17$. We carry out this checking for $18 \leq m \leq 24$ and find that no H -coverings exist. Let $m = 25$. Then we get an H -covering given by

$$\begin{aligned} f(3) = 1, \quad f(4) = 3, \quad f(5) = 2, \quad f(7) = 7, \quad f(11) = 9, \\ f(13) = 5, \quad f(17) = 8, \quad f(19) = 6, \quad f(23) = 1. \end{aligned}$$

Thus P_2 does not hold for some S_{25} and we get

$$g(2) = 25.$$

To find $G(2)$, we need to check for $26 \leq m \leq 55$. For this purpose, we continue using the Covering Algorithm for $26 \leq m \leq 40$ and find that for all such m there exists an H -covering. Now for $41 \leq m \leq 48$, we apply the Weighted Algorithm with weights $(\alpha, \beta) = (.7, .15)$, and for the remaining m -values $49 \leq m \leq 55$, we apply the Weighted Algorithm with $(\alpha, \beta) = (.6, .25)$. We find for each of the m -values considered that the algorithm

provides an H -covering for $[1, m]$. Altogether this gives

$$G(2) = 25.$$

We now turn to the calculation of $g(3)$ and $G(3)$. By Table 1, $g(3) \leq 151$, $G(3) \leq 239$. By computing L_3 , we get $G(3) \leq 100$. For fixed m we take

$$H = \{p \mid p \text{ is a prime with } 3 < p < m\} \cup \{4, 6, 9\}.$$

We use the modified version of Lemma 5.4 as explained in Remark 5.5. We fix $f(6)$ subject to (14), that is, satisfying the conditions $1 \leq f(6) \leq 6$, $f(6) \equiv f(4) \pmod{2}$ and $f(6) \equiv f(9) \pmod{3}$. Then we see that property P_3 does not hold for some S_m if and only if $[1, m]$ has such an H -covering. For $17 \leq m \leq 48$ we do not find such an H -covering. When $m = 49$, we get the following covering:

$$\begin{aligned} f(4) &= 3, f(5) = 3, f(6) = 1, f(7) = 6, f(9) = 4, f(11) = 10, \\ f(13) &= 3, f(17) = 9, f(19) = 17, f(23) = 1, f(29) = 1, f(31) = 14, \\ f(37) &= 12, f(41) = 5, f(43) = 1, f(47) = 2. \end{aligned}$$

Thus $g(3) = 49$. Repeated use of the Covering Algorithm reveals that $[1, m]$ has no such H -covering for $m = 50, 51, 52$ but such coverings exist for $53 \leq m \leq 59$. Such a covering for $m = 59$ is given by

$$\begin{aligned} f(4) &= 1, f(5) = 1, f(6) = 5, f(7) = 6, f(9) = 5, f(11) = 8, \\ f(13) &= 2, f(17) = 5, f(19) = 5, f(23) = 12, f(29) = 18, f(31) = 7, \\ f(37) &= 3, f(41) = 1, f(43) = 1, f(47) = 10, f(53) = 4. \end{aligned}$$

Then for all $60 \leq m \leq 77$ this f can be extended to an H -covering of $[1, m]$, by defining the following values:

$$\begin{aligned} f(59) &= 1 \ (m \geq 60), & f(61) &= 3 \ (m \geq 64), & f(67) &= 3 \ (m \geq 70), \\ f(71) &= 1 \ (m \geq 72), & f(73) &= 2 \ (m \geq 75). \end{aligned}$$

Then we apply the Weighted Algorithm with weights $(\alpha, \beta) = (.3, .05)$ to get an H -covering of $[1, m]$ for $m = 78$, given by

$$\begin{aligned} f(4) &= 2, f(5) = 3, f(6) = 4, f(7) = 2, f(9) = 4, f(11) = 3, \\ f(13) &= 6, f(17) = 7, f(19) = 1, f(23) = 12, f(29) = 27, \\ f(31) &= 29, f(37) = 24, f(41) = 18, f(43) = 14, f(47) = 8, \\ f(53) &= 21, f(59) = 15, f(61) = 17, f(67) = 11, f(73) = 5. \end{aligned}$$

Here the prime 71 is a spared element. We define the values

$$\begin{aligned} f(71) &= 16 \ (m \geq 87), & f(79) &= 10 \ (m \geq 89), & f(83) &= 12 \ (m \geq 95), \\ f(89) &= 10 \ (m = 99) \end{aligned}$$

to get H -coverings for all $78 \leq m \leq 99$ with 97 as a spared element. Summarizing the above facts we obtain $G(3) = 53$, and the statement follows. ■

Proof of Theorem 2.8. Since the proof runs along the same lines as the proof of Theorem 2.7, we only give the essential details. For fixed p and m we take the set

$$H = \{q \mid q \text{ is a prime } < m\} \setminus \{p\}.$$

By Corollary 2.2 and Remark 2.3, we have $G(T_p) \leq G_0$ where G_0 is given by (4) for $p \neq 2$ and $G(T_2) \leq 384$. Brauer's result [1] immediately gives $g(T_p) = G(T_p) = 17$ for $p > 425$. In the case of $p < 425$ we run our algorithms for $17 \leq m < G_0$ to get Table 3. In the case of $p = 2, 3$ it took about three weeks altogether (using an average PC) to find the exact values of $g(T_p)$ and $G(T_p)$. The hard task is to find the values of $g(T_p)$, and to check whether there is an H -covering for $m = g(T_p) + i$ for some small values of i (say with $1 \leq i \leq 20$). From that point on the Weighted Algorithm starts working effectively, and easily provides all the necessary coverings. We typically used the weights

$$\alpha \in \{.3, .4, .5, .6, .7, .8, .9\}, \quad \beta \in \{.05, .1, .15, .2, .25, .3\}.$$

For example, when $p = 2$ (besides getting H -coverings for $m = 86$ and 87) for $m = 88$ we find the covering

$$\begin{aligned} f(3) &= 1, & f(5) &= 4, & f(7) &= 1, & f(11) &= 9, & f(13) &= 12, & f(17) &= 11, \\ f(19) &= 3, & f(23) &= 10, & f(29) &= 18, & f(31) &= 1, & f(37) &= 35, & f(41) &= 27, \\ f(43) &= 23, & f(47) &= 1, & f(53) &= 30, & f(59) &= 6, & f(61) &= 26, \\ f(67) &= 21, & f(71) &= 17, & f(73) &= 7, & f(79) &= 2, & f(83) &= 5. \end{aligned}$$

Then, defining the following f -values:

$$\begin{aligned} f(89) &= 4 \ (m \geq 93), & f(97) &= 4 \ (m \geq 101), & f(101) &= 6 \ (m \geq 107), \\ f(103) &= 7 \ (m \geq 110), & f(107) &= 4 \ (m \geq 111), \\ f(109) &= 13 \ (m \geq 122), & f(113) &= 10 \ (m \geq 123), \end{aligned}$$

we get H -coverings for $m \leq 125$. From this point on, the Weighted Algorithm is applied to find coverings for all the values of $m \leq 383$. We applied a similar procedure to calculate the values of $g(T_3)$ and $G(T_3)$.

Let $5 \leq p < 425$. Then $17 \leq g(T_p) \leq G(T_p) \leq G_0$ with $G_0 = 431$ for $p = 5$ and $G_0 = 425$ otherwise. Thus we need to check the existence of an H -covering for $17 \leq m < G_0$. As in the case $p = 2$, we use the Covering Algorithm up to some value of m , say m_0 , to get an H -covering. For $m > m_0$, we apply the Weighted Algorithm with weights α, β as chosen earlier, to check the existence of an H -covering. As previously, this process is considerably speeded up by using the spared primes obtained at step (WA.2). We obtain the values of $g(T_p)$ and $G(T_p)$ as given in Table 3. See [6] for explicit H -coverings. ■

Acknowledgements. The authors are grateful to the referee for his/her useful and helpful remarks and suggestions.

Research of L. Hajdu was supported in part by the Hungarian Academy of Sciences, by the OTKA grants T48791, K67580, K75566 and by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

References

- [1] A. Brauer, *On a property of k consecutive integers*, Bull. Amer. Math. Soc. 47 (1941), 328–331.
- [2] Y. Caro, *On a division property of consecutive integers*, Israel J. Math. 33 (1979), 32–36.
- [3] P. Dusart, *Autour de la fonction qui compte le nombre de nombres premiers*, Ph.D. thesis, Univ. de Limoges, 1998.
- [4] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. 19 (1975), 292–301.
- [5] I. Gassko, *Stapled sequences and stapling coverings of natural numbers*, Electron. J. Combin. 3 (1996), no. 1, #R33.
- [6] L. Hajdu and N. Saradha, *Examples for sets S_m not having property $P(T)$* , www.math.klte.hu/~hajdul/Tables.pdf.
- [7] M. Ohtomo and F. Tamari, *On relative prime number in a sequence of positive integers*, J. Statist. Plann. Inference 106 (2002), 509–515.
- [8] S. S. Pillai, *On m consecutive integers I*, Proc. Indian Acad. Sci. Sect. A 11 (1940), 6–12.
- [9] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
- [10] N. Saradha and R. Thangadurai, *Pillai's problem on consecutive integers*, in: Number Theory and Applications, Hindustan Book Agency, New Delhi, 2009, 175–188.

L. Hajdu
 Institute of Mathematics
 University of Debrecen
 and
 the Number Theory Research Group
 of the Hungarian Academy of Sciences
 P.O. Box 12
 H-4010 Debrecen, Hungary
 E-mail: hajdul@math.klte.hu

N. Saradha
 School of Mathematics
 Tata Institute of Fundamental Research
 Dr. Homibhabha Road
 Colaba, Mumbai, India
 E-mail: saradha@math.tifr.res.in

Received on 16.4.2009
 and in revised form on 8.2.2010

(6003)