SETS OF INTEGERS WITH PAIRWISE COMMON DIVISOR AND A FACTOR FROM A SPECIFIED SET OF PRIMES

by

Rudolf Ahlswede and Levon H. Khachatrian

1. Introduction and main results

Whenever possible we keep the notation of [3]. $\mathbb{N}$ denotes the set of positive integers and $\mathbb{N}^*$ is the set of positive squarefree numbers. $\mathbb{P} = \{p_1, p_2, \dots\} = \{2, 3, 5, \dots\}$ denotes the set of primes and p_s denotes the s–th prime.

For two numbers $u, v \in \mathbb{N}$ we write $u|v$ (resp. $u \nmid v$) iff u divides v (resp. u does not divide v). $[u,v]$ stands for the least common multiple of u and v . (u,v) is the largest common divisor of u, v and we say that u and v have a common divisor if $(u,v) > 1$. $\langle u, v\rangle$ denotes the interval $\{x \in \mathbb{N} : u \leq x \leq v\}$ and $(u, v\rangle$ denotes the left–open interval $\{x \in \mathbb{N} : u < x \leq v\}$.

For any set $A \subset \mathbb{N}$ we introduce $A(n) = A \cap \langle 1, n\rangle$ and $|A|$ as cardinality of A . The set of multiples of A is

$$M(A) = \{m \in \mathbb{N} : a|m \text{ for some } a \in A\}.$$

For $u \in \mathbb{N}, u \neq 1, p^+(u)$ (resp. $p^-(u)$) denotes the largest (resp. the smallest) prime factor of u .

For any $y \in \mathbb{N}$, $\pi(y) = |\mathbb{P}(y)|$ denotes the counting function of primes. For any subset of primes $T \subset \mathbb{P}$, and $u \in \mathbb{R}^+$ we set

$$\phi(u,T) = \big\{x \in \mathbb{N}(u) : (x,p) = 1 \text{ for all } p \in T\big\}.$$

We note that always $\{1\} \in \phi(u,T)$ for all $T \subset \mathbb{P}$, $u \geq 1$.

Finally, for a set $A = \{a_1, \dots, a_m\}$ of ordered numbers $a_1 < a_2 < \dots < a_m$ we also just write $A = \{a_1 < a_2 < \dots < a_m\}$.

P. Erdös and R. Graham (see [1], [2]) posed the following problem:

Let $1 < a_1 < a_2 < \dots < a_k = n$, $(a_i, a_j) \neq 1$. What is the maximal value of k ? We denote it by $g(n)$.

While in [1] the problem was stated unfortunately with many confusing misprints, in [2] one can find the following conjecture: $g(n)$ equals either $\frac{n}{p^-(n)}$ or the number of integers of the form $2 \cdot t$, $t \leq \frac{1}{2}n$, $(t,n) \neq 1$.

However, it is easy to find a counterexample for this assertion and we informed Erdös about this during his visit in Bielefeld in the year 1992. He then came up with the following formulation:

Conjecture 1. Let $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \dots q_r^{\alpha_r}$, $\alpha_i \geq 1$, $q_i \in \mathbb{P}$, and $q_1 < q_2 < \dots < q_r$, then

$$g(n) = \max_{1 \leq j \leq r} |M(2q_1, 2q_2, \dots, 2q_j, q_1 \dots q_j) \cap \mathbb{N}(n)|.$$

We consider a more general and seemingly more natural problem:

Let $Q = \{q_1 < \dots < q_r\} \subset \mathbb{P}$ be any finite set of primes and let $A = \{a_1 < a_2 < \dots < a_k\} \subset \mathbb{N}(n)$, be a set such that for all $1 \leq i, j \leq k$

$$(a_i, a_j) \neq 1 \tag{1.1}$$

and

$$\left(a_i, \prod_{i=1}^{r} q_i\right) > 1. \tag{1.2}$$

$I(n,Q)$ denotes the set of all such sets. We are interested in the quantity

$$f(n,Q) = \max\bigl\{|A| : A \in I(n,Q)\bigr\}. \tag{1.3}$$

For special values of n, namely $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$ for some $\alpha_i \geq 1$, clearly $a_{f(n,Q)} = n$ and we get exactly the problem of Erdös–Graham.

Our problem can be viewed as being dual to that studied in [3], where a specified set of primes is *excluded* as factors.

Obviously, we can assume that $\{2\} \notin Q$, because otherwise $f(n,Q) = \lfloor \frac{n}{2} \rfloor$ is realized for the even numbers $\leq n$. Our main result is

Theorem 1. *For every finite* $Q = \{q_1 < q_2 < \dots < q_r\} \subset \mathbb{P}$ *and* $n \geq \prod_{i=1}^{r} q_i$

$$f(n,Q) = \max_{1 \leq j \leq r} |M(2q_1, 2q_2, \dots, 2q_j, q_1 \dots q_j) \cap \mathbb{N}(n)| \tag{1.4}$$

holds. In particular Conjecture 1 is true.

We will also show (see Section 6), that the restriction on n in Theorem 1 can not be ignored.

For given finite $Q = \{q_1 < \dots < q_r\} \subset \mathbb{P}$ let us look at our problem in the infinite case, i.e. $A = \{a_1 < a_2 < \dots\} \subset \mathbb{N}$ satisfies (1.1) and (1.2). What is maximal $\overline{d}_Q$ of the asymptotic (upper) density of such A? From Theorem 1 immediately follows:

Corollary. *For any finite* $Q = \{q_1 < \dots < q_r\} \subset \mathbb{P}$ *we have*

$$\overline{d}_Q = \max_{1 \leq j \leq r} \frac{1}{2} \left(1 - \prod_{i=1}^{j} \left(1 - \frac{1}{q_i}\right) + \frac{1}{q_1 \dots q_j}\right).$$

Moreover, this maximum is assumed for a set possessing an asymptotic density.

It is also natural to formulate the problem for the squarefree case. We define $f^*(n,Q)$ as the maximal cardinality of sets $A \subset \mathbb{N}^*(n)$ satisfying (1.1) and (1.2).

Theorem 2. *For any finite* $Q = \{q_1 < \dots q_r\} \subset \mathbb{P}$ *we have*

$$f^*(n,Q) = \max_{1 \leq j \leq r} |M(2q_1, \dots, 2q_j, q_1 \dots q_j) \cap \mathbb{N}^*(n)|.$$

We draw attention to the fact that here we have no restriction on n. The proof of Theorem 2 is much easier than that of Theorem 1.

Moreover, Theorem 2 can easily be extended to much more general objects, namely to squarefree quasi–numbers (see [3]).

Sections 2,3, and 4 provide auxiliary results for the proof of Theorem 1 (and sketch of proof of Theorem 2) in Section 5. We draw especially attention to an auxiliary result in Section 3, which is stated as Theorem 3, because it is of independent interest.

Finally, an example in Section 6 shows that (1.4) does not hold without any condition on n . The reader is advised to look first at this example.

2. An auxiliary result for "left compressed sets", "upsets", and "downsets"

Let $\mathcal{O}(n,Q)$ denote the set of all optimal sets of $I(n,Q)$, i.e.

$$\mathcal{O}(n,Q) = \big\{A \in I(n,Q) : |A| = f(n,Q)\big\} \quad \text{(see (1.3))}.$$

For any $p_s, p_t \in \mathbb{P}$, $p_s < p_t$, we define the operation "left pushing" $L_{s,t}$ on subsets of $\mathbb{N}$. For $B \subset \mathbb{N}$ let

$$B_1 = \big\{b \in B : b = b_1 \cdot p_t^\alpha, (b_1, p_s \cdot p_t) = 1, \alpha \geq 1, (b_1 \cdot p_s^\alpha) \notin B\big\}.$$

Then

$$L_{s,t}(B) = (B \setminus B_1) \,\dot\cup\, B_2,$$

where $B_2 = \big\{c \in \mathbb{N} : c = c_1 \cdot p_s^\beta, (c_1, p_s \cdot p_t) = 1, \beta \geq 1, (c_1 \cdot p_t^\beta) \in B_1\big\}$.

Clearly

$$|L_{s,t}(B) \cap \mathbb{N}(n)| \geq |B(n)| \quad \text{for every} \quad s,t; s<t; \quad \text{and} \quad n \in \mathbb{N}. \tag{2.1}$$

For $Q \subset \mathbb{P}$ the set $B \subset \mathbb{N}$ is said to be *left compressed with respect to* Q , if

$$L_{s,t}(B) = B \quad \text{for all} \quad s,t,s<t,p_t \in \mathbb{P} \setminus Q \tag{2.2}$$

and

$$L_{s,t}(B) = B \quad \text{for all} \quad s,t,s<t,p_s,p_t \in Q. \tag{2.3}$$

For given $Q \subset \mathbb{P}$, we denote by $\mathcal{C}(Q)$ the set of all subsets of $\mathbb{N}$, which are left compressed with respect to Q .

Every finite set $B \subset \mathbb{N}$ can be transformed by finitely many operations $L_{s,t}$; $s<t$; of the types (2.2) and (2.3) into a member of $\mathcal{C}(Q)$. Since these operations preserve (1.1) and (1.2), we get with (2.1) the following result.

Lemma 1. *For any* $Q \subset \mathbb{P}$ *and* $n \in \mathbb{N}$

$$\mathcal{O}(n,Q) \cap \mathcal{C}(Q) \neq \varnothing.$$

Clearly any $A \in \mathcal{O}(n,Q)$ is an "upset":

$$A = M(A) \cap \mathbb{N}(n), \tag{2.4}$$

and it is also a "downset" in the following sense:

$$\text{for } \ a \in A, a = p_{i_1}^{\alpha_1} \dots p_{i_t}^{\alpha_t}, \alpha_i \geq 1 \ \text{ also } \ p_{i_1} \dots p_{i_t} \in A. \tag{2.5}$$

For every $B \subset \mathbb{N}$ we introduce the unique primitive subset $P(B)$, $P(B) \subset B$, which has the properties

$$b_1, b_2 \in P(B), b_1 \neq b_2, \ \text{ implies } \ b_1 \nmid b_2 \ \text{ and } \ B \subset M\big(P(B)\big). \tag{2.6}$$

We know from (2.5) that for any $A \in \mathcal{O}(n,Q)$ $P(A)$ consists only of squarefree numbers and that by (2.4)

$$A = M\big(P(A)\big) \cap \mathbb{N}(n). \tag{2.7}$$

3. Auxiliary inequalities for sets of numbers with forbidden prime factors

Let $T \subset \mathbb{P}, T = T_1 \,\dot{\cup}\, T_2$, where

$$T_1 \subset \{p_1, \dots, p_{s-1}\}, T_2 = \{p_{j_1}, \dots, p_{j_r}\}; p_s < p_{j_1} < \dots < p_{j_r}.$$

The sets T_1 and T_2 can be empty.

Lemma 2. *Let* $s > 1$ *and suppose that*

$$r \leq \pi(p_{s+\ell-1} \cdot p_s) - s - 2\ell + 1 \ \textit{ for all } \ \ell \geq 1, \tag{3.1}$$

then

$$2 \cdot |\phi(u,T)| \leq |\phi(u \cdot p_s, T)| \ \textit{ for all } \ u \in \mathbb{R}^+. \tag{3.2}$$

Remark 1: A more special form of the Lemma was proved (although it was not stated explicitly) in our paper [3]. Actually, in [3] we proved (3.2), if $T_2 = \varnothing$. In this case we have $r = 0$ and the condition (3.1)

$$0 \leq \pi(p_{s+\ell-1} \cdot p_s) - s - 2\ell + 1 \ \text{ for all } \ \ell \geq 1$$

always holds.

Indeed, since $s > 1$ we have $p_s \geq 3$ and thus the first inequality in $\pi(p_{s+\ell-1} \cdot p_s) \geq \pi(3\ p_{s+\ell-1}) \geq 2\pi(p_{s+\ell-1})$, where the last inequality folows from $\pi(3x) \geq 2\pi(x)$, which was shown in [3]. Thus for the quantity in question

$$\pi(p_{s+\ell-1} \cdot p_s) - s - 2\ell + 1 \geq 2\pi(p_{s+\ell-1}) - s - 2\ell + 1 = 2(s + \ell - 1) - s - 2\ell + 1 = s - 1 > 0.$$

Proof: Equivalent to (3.2) is

$$|\phi(u, T)| \leq |\phi'(u \cdot p_s, T), \tag{3.3}$$

where $\phi'(u \cdot p_s, T) = \phi(u \cdot p_s, T) \cap (u, u \cdot p_s\rangle$.

We introduce

$$\Psi(u, T) = \{a \in \phi(u, T) : p^+(a) < p_s \text{ or } a = 1\}$$

and for $a \in \Psi(u, T)$

$$D(a) = \{b \in \phi(u, T) : b = a \cdot d, p^-(d) \geq p_s \text{ or } d = 1\}.$$

With these sets we can write $\phi(u, T)$ as a disjoint union

$$\phi(u, T) = \dot{\bigcup_{a \in \Psi(u,T)}} D(a).$$

Next we introduce for $a \in \Psi(u,T)$

$$D'(a) = \big\{c \in \phi'(u \cdot p_s, T) : c = a \cdot d^*, p^-(d^*) \geq p_s\big\}.$$

Clearly these sets are disjoint and

$$\phi'(u\ p_s, T) \supset \dot{\bigcup_{a \in \Psi(u,T)}} D'(a).$$

Sufficient for (3.3) is

$$|D'(a)| \geq |D(a)| \ \text{ for all } \ a \in \Psi(u,T). \tag{3.4}$$

From the definition of the sets $D(a)$ and $D'(a)$ it follows that for

$$T^* = \{p_1, \dots, p_{s-1}\} \cup T_2$$

$$|D(a)| = \phi\left(\frac{u}{a}, T^*\right), |D'(a)| = |\phi'\left(\frac{u\ p_s}{a}, T^*\right), \quad \text{and}$$

$$\phi'\left(\frac{u\ p_s}{a}, T^*\right) = \phi\left(\frac{u\ p_s}{a}, T^*\right) \smallsetminus \phi\left(\frac{u}{a}, T^*\right) = \phi\left(\frac{u\ p_s}{a}, T^*\right) \cap \left(\frac{u}{a}, \frac{u\ p_s}{a}\right\rangle.$$

Thus we arrived at the following sufficient condition for (3.4):

$$|\phi(v,T^*)| \leq |\phi'(v \cdot p_s, T^*)| = |\phi(v \cdot p_s, T^*) \smallsetminus \phi(v, T^*)| \ \text{ for all } \ v \in \mathbb{R}^+. \tag{3.5}$$

We avoid the trivial cases $v < 1$ for which $\phi(v,T^*) = \varnothing$ and $1 \leq v < p_s$, for which $|\phi(v,T^*)| = 1$ and $p_s \in \phi'(v \cdot p_s, T^*)$. Hence we assume $v \geq p_s$ and introduce

$$F(v,T^*) = \big\{b \in \phi(v,T^*), b \neq 1 : b \cdot p^+(b) \leq v\big\} \cup \{1\}.$$

Then $\phi(v,T^*)$ is a disjoint union

$$\phi(v,T^*) = \dot{\bigcup_{b \in F(v,T^*)}} \tau(b) \cup \{1\},$$

where

$$\tau(b) = \left\{m \in \mathbb{N} : m = p \cdot b; p \in \mathbb{P} \smallsetminus T^*; p^+(b) \leq p \leq \frac{v}{b}\right\}.$$

Hence for all $b \in F(v,T^*)$

$$|\tau(b)| = \left|\left\{p \in \mathbb{P} \smallsetminus T^* : p^+(b) \leq p \leq \frac{v}{b}\right\}\right| \ \text{ and} \tag{3.6}$$

$$|\phi(v,T^*)| = \sum_{b \in F(v,T^*)} |\tau(b)| + 1, \tag{3.7}$$

where integer 1 in (3.7) stands to account for the element $\{1\} \in \phi(v,T^*)$.

On the other hand we have

$$\phi'(v \cdot p_s, T^*) \supset \dot{\bigcup_{b \in F(v,T^*)}} \tau_1(b) \cup \{p_s^k\},$$

where $\tau_1(b) = \{m_1 \in \mathbb{N} : m_1 = p \cdot b, p \in \mathbb{P} \setminus T^*, \frac{v}{b} < p \le \frac{v \cdot p_s}{b}\}$ and p_s^k satisfies $v < p_s^k \le v \cdot p_s$ for some $k \in \mathbb{N}$.

It is easy to see, that the sets $\{\tau_1(b)\}, b \in F(v, T^*)$, are disjoint and that the element $\{p_s^k\}$ does not belong to any of them.

We have

$$|\tau_1(b)| = \left|\left\{p \in \mathbb{P} \setminus T^* : \frac{v}{b} < p \le \frac{v \cdot p_s}{b}\right\}\right| \tag{3.8}$$

for all $b \in F(v, T^*)$ and

$$|\phi'(v \cdot p_s, T^*)| \ge \sum_{b \in F(v,T^*)} |\tau_1(b)| + 1, \tag{3.9}$$

where integer 1 in (3.9) stands to account for the element $\{p_s^k\}$.

From (3.7) and (3.9) it follows that sufficient for (3.5) is

$$|\tau_1(b)| \ge |\tau(b)| \text{ for all } b \in F(v, T^*).$$

Let $p_{s+\ell-1} \le \frac{v}{b} < p_{s+\ell}$ for some $\ell \ge 1$.

Then, from (3.6) and (3.8), we have

$$|\tau(b)| = \left|\left\{p \in \mathbb{P} \setminus T^* : p^+(b) \le p \le \frac{v}{b}\right\}\right| \le |\{p \in \mathbb{P} : p_s \le p \le p_{s+\ell-1}\}| = \ell$$

and

$$|\tau_1(b)| = \left|\left\{p \in \mathbb{P} \setminus T^* : \frac{v}{b} < p \le \frac{v \cdot p_s}{b}\right\}\right| \ge$$
$$|\{p \in \mathbb{P} \setminus T^* : p_{s+\ell-1} < p \le p_{s+\ell-1} \cdot p_s\}| = \pi(p_{s+\ell-1} \cdot p_s) - (s + \ell - 1) - r_1,$$

where r_1 is the number of primes from T_2 in the interval $\langle p_{s+\ell}, p_{s+\ell-1} \cdot p_s \rangle$. Since $r_1 \le r = |T_2|$ we have

$$|\tau_1(b)| \ge \pi(p_{s+\ell-1} \cdot p_s) - (s + \ell - 1) - r.$$

Finally, using condition (3.1) we have established the sufficient condition

$$|\tau_1(b)| \ge \pi(p_{s+\ell-1} \cdot p_s) - (s + \ell - 1) - r \ge \ell \ge |\tau(b)|.$$

Remark 2: Perhaps one can try to simplify condition (3.1) in Lemma 2 by finding

$$\min_{\ell \in \mathbb{N}} \left(\pi(p_{s+\ell-1} \cdot p_s) - 2\ell\right) \text{ for } s \ge 2.$$

However, if the minimum is achieved for $\ell = 1$ (which seems the most likely), then one has at least to prove, that between p_s^2 and $p_s \cdot p_{s+1}$ there are at least two primes, which seems hopeless. For comparison let us recall that in 1904 Brocard conjectured that between p_s^2 and p_{s+1}^2 , there are at least 4 primes and this remains unsolved (see [5]).

We need the folowing result, which is probably known to the experts (in fact, it is an easy consequence of known results), but we could not find in the literature.

Lemma 3.

$$p_s \cdot p_t > p_{s\cdot t}$$

for all $s, t \in \mathbb{N}$ *expect for two cases, namely,* $s = 3$, $t = 4$, *for which* $p_3 \cdot p_4 = 5 \cdot 7 = 35 < p_{12} = 37$, *and* $s = t = 4$, *for which* $p_4 \cdot p_4 = 7 \cdot 7 = 49 < p_{16} = 53$ *.*

Proof: We use very sharp estimates of the size of primes, which are due to Rosser and Schoenfeld [4]:

$$\begin{aligned} &p_n < n\left(\log n + \log\log n - \frac{1}{2}\right) \quad \text{for} \quad n \geq 20, \\ &p_n > n \log n \quad \text{for} \quad n \geq 1. \end{aligned} \tag{3.10}$$

Using (3.10) one gets

$$p_s \cdot p_t > p_{s\cdot t} \quad \text{for all} \quad t \geq s \geq 12.$$

For every $s \leq 11$, we take the exact value of p_s and estimate, using (3.10), only primes p_t and p_{st} . For example let $s = 4$, $p_4 = 7$, $t \geq 5$. Since $s \cdot t \geq 20$ we can use (3.10) to get

$$p_{4t} < 4t\left(\log 4t + \log\log 4t - \frac{1}{2}\right) \quad \text{and} \quad p_4 \cdot p_t = 7 \cdot p_t > 7 \cdot t \log t. \tag{3.11}$$

From (3.11) we have $7 \cdot p_t > p_{4\cdot t}$ for all $t \geq 25$ and this cases $5 \leq t \leq 24$ are verified by inspection using the list of primes.

In the case $s = t = 4$ we have the opposite inequality and this is one of the two exceptions specified in the Lemma. For other values of $s \leq 11$ we have similar calculations.

We recall the definitions of the sets T_1, T_2, T in Lemma 2:

$$T_1 \subset \{p_1, \ldots, p_{s-1}\}, T_2 = \{p_{j_1}, \ldots, p_{j_r}\}; p_s < p_{j_1} < \cdots < p_{j_r};$$

and $s > 1$. We introduce

$$T_3 = \big(\{p_1, \ldots, p_{s-1}\} \smallsetminus T_1\big) \cup \{p_s\} = \{p_{i_1}, \ldots, p_{i_t}\}, p_{i_1} < \cdots < p_{i_t} = p_s.$$

Theorem 3. *Let* $s > 1$ *and the sets of primes* T_1, T_2, T_3 , $T = T_1 \cup T_2$ *as described above. Then for every* $u \in \mathbb{R}^+$ *with*

$$u \geq \frac{\prod_{p\in T_2} p}{\prod_{p\in T_3} p} \tag{3.12}$$

$$2|\phi(u, T)| \leq |\phi(u \cdot p_s, T)| \quad \textit{holds.} \tag{3.13}$$

Proof: In the light of Lemma 2 we can assume

$$r > \pi(p_{s+\ell-1} \cdot p_s) - s - 2\ell + 1 \quad \text{for some} \quad \ell \geq 1. \tag{3.14}$$

At first let us show that from (3.14) one can get

$$r > (s-1)^2. \tag{3.15}$$

Indeed from Lemma 3 we know

$$p_{s+\ell-1} \cdot p_s > p_{(s+\ell-1)s} \quad \text{for all} \quad s, \ell \quad \text{except} \quad s=3, \ell=2 \quad \text{and} \quad s=4, \ell=1.$$

Hence

$$\pi(p_{s+\ell-1} \cdot p_s) \geq \pi(p_{(s+\ell-1)\cdot s}) = s(s+\ell-1)$$

for all s, ℓ with the exceptions mentioned above.
Therefore

$$r > \pi(p_{s+\ell-1} \cdot p_s) - s - 2\ell + 1 \geq s(s+\ell-1) - s - 2\ell + 1 \geq (s-1)^2.$$

since $s > 1$. For $s = 3$, $\ell = 2$ and $s = 4$, $\ell = 1$ we verify (3.15) by inspection.
Now, for every $u \in \mathbb{R}^+$ by the inclusion–exclusion principle we have

$$|\phi(u,T)| = \lfloor u \rfloor - \sum_{p \in T} \left\lfloor \frac{u}{p} \right\rfloor + \sum_{\substack{p<q \\ p,q \in T}} \left\lfloor \frac{u}{p \cdot q} \right\rfloor \cdots \leq u \cdot \prod_{p \in T} \left(1 - \frac{1}{p}\right) + 2^{|T|-1}$$

and

$$|\phi(u \cdot p_s), T| \geq u \cdot p_s \cdot \prod_{p \in T} \left(1 - \frac{1}{p}\right) - 2^{|T|-1}.$$

Hence, sufficient for (3.13) is

$$u(p_s - 2) \cdot \prod_{p \in T} \left(1 - \frac{1}{p}\right) \geq 3 \cdot 2^{|T|-1} \quad \text{for all} \quad u \geq \frac{\prod_{p \in T_2} p}{\prod_{p \in T_3} p}. \tag{3.16}$$

Since $|T| = s - t + r$, equivalent to (3.16) is

$$(p_s - 2) \cdot \frac{\prod_{p \in T_2} p}{\prod_{p \in T_3} p} \cdot \prod_{p \in T_1 \cup T_2} \left(1 - \frac{1}{p}\right) = (p_s - 2) \cdot \frac{\prod_{p \in T_2} (p-1)}{\prod_{i=1}^{s} p_i} \cdot \prod_{p \in T_1} (p-1) \geq 3 \cdot 2^r \cdot 2^{s-t-1}. \tag{3.17}$$

Since $|T_1| = s - t$, we observe that

$$\prod_{p \in T_1} (p-1) \geq 2^{s-t-1}$$

and sufficient for (3.17) is

$$(p_s - 2) \cdot \frac{\prod_{p \in T_2} (p-1)}{\prod_{i=1}^{s} p_i} \geq 3 \cdot 2^r. \tag{3.18}$$

Now, if $s \geq 3$, then

$$(p_s - 2) \cdot \frac{\prod_{p \in T_2}(p-1)}{\prod_{i=1}^{s} p_i} = (p_s - 2)\frac{(p_{j_1}-1)\dots(p_{j_r}-1)}{p_1 \dots p_s} >$$
$$(p_s - 2)(p_{j_{s+1}}-1)\dots(p_{j_r}-1) > (p_s-2)\cdot(p_{j_{s+1}}-1)^{r-s} \geq (p_s-2)\cdot 16^{r-s} > 3\cdot 2^r,$$

since $p_{j_1} \geq 7, p_{j_{s+1}} \geq 17$ and we know that $r \geq (s-1)^2+1$ (see (3.15)).

So, it remains to show the validity of (3.13) only for the case $s = 2$. From (3.15) we know that $r \geq 2$ and, if $r > 2$, we have in (3.18)

$$\frac{(p_{j_1}-1)(p_{j_2}-1)\dots(p_{j_r}-1)}{2\cdot 3} \geq \frac{(5-1)(7-1)(11-1)\dots(p_{j_r}-1)}{6} \geq 3\cdot 2^r.$$

Hence, we can assume $r = 2$. However the formula (3.18) does not hold in this case for instance for $p_{j_1} = 5$, $p_{j_2} = 7$:

$$\frac{(5-1)(7-1)}{6} \not\geq 3\cdot 2^2 = 12.$$

In the case $s = r = 2$ we have to estimate the quantities $|\phi(u,T)|$ and $|\phi(3u,T)|$ more accurately.

We have to consider two cases: $t = 1$ and $t = 2$, where $t = |T_3|$. We are going to prove (3.13) only for $t = 1$ (the case $t = 2$ is similar, actually even simpler).

We have to prove that for q_1, q_2 , $5 \leq q_1 < q_2$; $T = \{2, q, q_2\}$

$2|\phi(u,T)| < |\phi(3u,T)|$ holds provided that $u \geq \frac{q_1\cdot q_2}{3}$. We have

$$|\phi(3u,T)| - 2|\phi(u,T)| = \lfloor 3u\rfloor - \left\lfloor \tfrac{3u}{2}\right\rfloor - \left\lfloor \tfrac{3u}{q_1}\right\rfloor - \left\lfloor \tfrac{3u}{q_2}\right\rfloor + \left\lfloor \tfrac{3u}{2q_1}\right\rfloor + \left\lfloor \tfrac{3u}{2q_2}\right\rfloor + \left\lfloor \tfrac{3u}{q_1q_2}\right\rfloor - \left\lfloor \tfrac{3u}{2q_1q_2}\right\rfloor -$$
$$2\lfloor u\rfloor + 2\left\lfloor \tfrac{u}{2}\right\rfloor + 2\left\lfloor \tfrac{u}{q_1}\right\rfloor + 2\left\lfloor \tfrac{u}{q_2}\right\rfloor - 2\left\lfloor \tfrac{u}{2q_1}\right\rfloor - 2\left\lfloor \tfrac{u}{2q_2}\right\rfloor - 2\left\lfloor \tfrac{u}{q_1q_2}\right\rfloor + 2\left\lfloor \tfrac{u}{2q_1q_2}\right\rfloor =$$
$$\left(\lfloor 3u\rfloor - \left\lfloor \tfrac{3u}{2}\right\rfloor - 2\lfloor u\rfloor + 2\left\lfloor \tfrac{u}{2}\right\rfloor\right) - \left(\left\lfloor \tfrac{3u}{q_1}\right\rfloor - \left\lfloor \tfrac{3u}{2q_1}\right\rfloor - 2\left\lfloor \tfrac{u}{q_1}\right\rfloor + 2\left\lfloor \tfrac{u}{2q_1}\right\rfloor\right) -$$
$$\left(\left\lfloor \tfrac{3u}{q_2}\right\rfloor - \left\lfloor \tfrac{3u}{2q_2}\right\rfloor - 2\left\lfloor \tfrac{u}{q_2}\right\rfloor + 2\left\lfloor \tfrac{u}{2q_2}\right\rfloor\right) + \left(\left\lfloor \tfrac{3u}{q_1q_2}\right\rfloor - \left\lfloor \tfrac{3u}{2q_1q_2}\right\rfloor - 2\left\lfloor \tfrac{u}{q_1q_2}\right\rfloor + 2\left\lfloor \tfrac{u}{2q_1q_2}\right\rfloor\right).$$

Now we use the following inequalities (which can be easily verified).

$x - 1 < x - \frac{5}{6} < \lfloor 6x\rfloor - \lfloor 3x\rfloor - 2\lfloor 2x\rfloor + 2\lfloor x\rfloor \leq x + \frac{5}{6} < x + 1$ for all $x \in \mathbb{R}^+$ to get

$$|\phi(3u,T)| - 2|\phi(u,T)| > u\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{q_1}\right)\left(1-\tfrac{1}{q_2}\right) - 4 =$$

$= \frac{u(q_1-1)(q_2-1)}{2q_1q_2} - 4 \geq \frac{(q_1-1)(q_2-1)}{6} - 4 \geq 0$, since $u \geq \frac{q_1q_2}{3}$ and $5 \leq q_1 < q_2$.

Remarks:

3. We note that (3.13) does not always hold, if we ignore the restriction on u . For example for $T = \{2, 5, 7\}$, $s = 2$, $u = 3$ we have

   $2|\phi(3,T)| = 2\cdot|\{1,3\}| = 4 \not\leq |\phi(p_2\cdot 3, T)| = |\phi(9,T)| = |\{1,3,9\}| = 3$.

4. If u is sufficiently large, $u > u(\varepsilon)$, then the coefficient 2 in (3.13) of the Theorem (in Lemma 2 as well), clearly can be changed to $(p_s - \varepsilon)$, for any $\varepsilon > 0$.

4. Further preparations: Lemmas 4, 5, 6

For given $Q \subset \mathbb{P}$ and any $b \in \mathbb{N}$ let $p^+(b,Q)$ denote the maximal prime from $\mathbb{P} \setminus Q$ which occurs in the prime decomposition of b (in the case $Q = \varnothing$ we always have $p^+(b,\phi) = p^+(b)$).

If b is completely composed from the primes Q or $b = 1$, then $p^+(b,Q) = 1$.

Further, let $A \subset \mathbb{N}(n)$ be such that $P(A)$, the primitive subset of A , consists only of squarefree numbers and let $A = M\big(P(A)\big) \cap \mathbb{N}(n)$.

For given $Q \subset \mathbb{P}$, we define

$$p^+\big(P(A),Q\big) = \max_{a \in P(A)} p^+(a,Q). \tag{4.1}$$

We consider $L_{i,j}(A) = A'$, where $i < j$ and $p_j \in Q$ implies $p_i \in Q$.

One can easily verify the following statement.

Lemma 4.

$$p^+\big(P(A),Q\big) \geq p^+\big(P(A'),Q\big).$$

Let $A \in \mathcal{O}(n,Q) \cap C(Q)$ for some $Q = \{q_1, q_2, \ldots, q_r\}$, $2 < q_1 < \cdots < q_r$ and $n \in \mathbb{N}$.

We know (see Lemma 1), that such a set A always exists. Let $P(A)$ be the primitive subset of A and $p^+\big(P(A),Q\big) = p_s$ for some $p_s \in (\mathbb{P} \setminus Q) \cup \{1\}$.

We write $P(A)$ in the form $P(A) = R_0 \,\dot\cup\, R_1 \,\dot\cup \ldots \dot\cup\, R_s$, where

$$R_0 = \big\{a \in P(A) : p^+(a,Q) = 1\big\} \tag{4.2}$$

and

$$R_i = \big\{a \in P(A) : p^+(a,Q) = p_i\big\}, 1 \leq i \leq s.$$

We note that some of the R_i can be empty, but not R_s .

Since A is optimal, we know that $A = M\big(P(A)\big) \cap \mathbb{N}(n)$, which can be written in the form

$$A = M\big(P(A)\big) \cap \mathbb{N}(n) = \big(M(R_0 \,\dot\cup \ldots \dot\cup\, R_{s-1}) \,\dot\cup\, K(R_s)\big) \cap \mathbb{N}(n),$$

where $K(R_s) = \big(M(R_s) \setminus M(R_0 \cup \cdots \cup R_{s-1})\big) \cap \mathbb{N}(n)$, i.e. $K(R_s)$ is the set of those elements of A , which are not divisible by any $b, b \in R_0 \cup \cdots \cup R_{s-1}$.

Let $s > 1$, $R_s = R_s^0 \,\dot\cup\, R_s^1$, where

$$R_s^0 = \{b \in R_s : 2 \mid b\}, R_s^1 = R_s \setminus R_s^0 \tag{4.3}$$

and $K(R_s) = K^0(R_s) \,\dot\cup\, K^1(R_s)$, where

$$K^0(R_s) = \big\{a \in K(R_s) : 2 \mid a\big\}, K^1(R_s) = K(R_s) \setminus K^0(R_s). \tag{4.4}$$

Finally, let

$$G_s^i = \{m \in \mathbb{N} : m \cdot p_s \in R_s^i\}, i = 0, 1. \tag{4.5}$$

Lemma 5. *Let* $A \in \mathcal{O}(n,Q) \cap C(Q)$ *, let the sets* $K^i(R_s), R_s^i, G_s^i$ *,* $i = 0,1$ *, be defined as above, and let* $s > 1$ *. Then*

(1) $b \nmid a$ *for all* $b \in R_s^i$ *,* $a \in K^{1-i}(R_s)$ *,* $i = 0,1$

(2) $K^i(R_s) = M(R_s^i) \setminus M(R_0 \cup \dots \cup R_{s-1})$ *,* $i = 0,1$

(3) $G_s^i \in I(n,Q)$ *,* $i = 0,1$ *. (defined in the Introduction)*

(4) $(R_0 \cup \dots \cup R_{s-1} \cup G_s^i) \in I(n,Q)$ *,* $i = 0,1$ *.*

Proof: (1) Obviously, $b \nmid a$ for all $b \in R_s^0$, $a \in K^1(R_s)$. Suppose $b \mid a$ for some $b \in R_s^1$, $a \in K^0(R_s)$. Then $\frac{b}{p_s} \cdot 2 \mid a$ as well, because $2 \nmid b$ and $2 \mid a$. However $\frac{b}{p_s} \cdot 2 \in A$, because A is left compressed with respect to Q and $p_s \notin Q$, $p_s > 2, 2 \nmid b$. Hence $\frac{b}{p_s} \cdot 2 \in M(R_0 \cup \dots \cup R_{s-1})$, because $p_s \nmid \frac{b}{p_s} \cdot 2$. Therefore $a \notin K(R_s)$, becuase $\frac{b}{p_s} \cdot 2 \mid a$. This is a contradiction.

(2) follows from (1).

(3) Clearly $G_s^0 \in I(n,Q)$, because all elements of G_s^0 are even and prime $p_s \notin Q$. Let us show that $G_s^1 \in I(n,Q)$ as well. Suppose to the opposite, there exist $b_1, b_2 \in G_s^1$ with $(b_1, b_2) = 1$.

We have $b_1 \cdot p_s, b_2 \cdot p_s \in R_s^1$ (see definition of G_s^1 and R_s^1).

However, since $R_s^1 \subset A$, A is left compressed with respect to Q and $p_s \notin Q$, $p_s > 2$, $2 \nmid b_1$, $2 \nmid b_2$, we conclude $2 \cdot b_1 \in A$ as well. Hence the elements $2 \cdot b_1$, $p_s \cdot b_2 \in A$ and at the same time $(2 \cdot b_1, p_s \cdot b_2) = 1$, which is a contradiction.

(4) This is trivial.

Finally we need an auxiliary result concerning the set $K(R_s)$. Let a be any element of $K(R_s)$. This element uniquely can be written in the forms

$$a = p_{i_1}^{\alpha_1} \cdot \ldots \cdot p_{i_t}^{\alpha_t} \cdot q_{j_1}^{\beta_1} \ldots q_{j_\ell}^{\beta_\ell} \cdot a_3, \quad \text{where} \tag{4.6}$$

$p_{i_1} < p_{i_2} < \dots < p_{i_t} = p_s < q_{j_1} < \dots < q_{j_\ell}$; $\alpha_i, \beta_i \geq 1$, $q_{j_i} \in Q$, $p^-(a_3) > p_s$, $p \mid a_3$ implies $p \in \mathbb{P} \setminus Q$ or $a_3 = 1$.

We note, that $\{q_{j_1}, \dots, q_{j_\ell}\} = \varnothing$ is also possible.

Lemma 6. *Let* $A \in \mathcal{O}(n,Q) \cap C(Q)$ *,* $p^+\big(p(A), Q\big) = p_s$ *,* $s > 1$ *and let* $a \in K(R_s)$ *be an element of the form (4.6), then*

(1) $a' = p_{i_1}^{\alpha_1'} \ldots p_{i_t}^{\alpha_t'} \cdot q_{j_1}^{\beta_1'} \ldots q_{j_\ell}^{\beta_\ell'} \cdot a_3' \in K(R_s)$ *for all* $\alpha_i' \geq 1$ *,* $\beta_i' \geq 1$ *,* $p^-(a_3') > p_s$ *,* $p \mid a_3'$ *implies* $p \in \mathbb{P} \setminus Q$ *, or* $a_3' = 1$ *, provided that* $a' \leq n$ *.*

(2) *For every integer* $b \in \mathbb{N}$ *of the form* $b = p_{i_1}^{\gamma_1} \ldots p_{i_{t-1}}^{\gamma_{t-1}} \cdot q_{j_1}^{\delta_1} \ldots q_{j_\ell}^{\delta_\ell} \cdot b', \gamma_i \geq 0, \delta_i \geq 0,$ $p^-(b') > p_s$ *,* $p \mid b'$ *implies* $p \in \mathbb{P} \setminus Q$ *or* $b' = 1$ *, we have* $b \notin A$ *.*

Proof: (1) Since $a \in K(R_s) \subset A$, we have $m \mid a$ for some $m \in P(A)$ and hence $m \mid p_{i_1} \ldots p_{i_t} \cdot q_{j_1} \ldots q_{j_\ell}$, because $p^+\big(P(A), Q\big) = p_s$ and $m \in P(A)$ implies $m \in \mathbb{N}^*$. Therefore all integers of the form in (1) belong to our set A . However, every $m \in P(A)$

with $m \mid a$ must belong to the set R_s , otherwise $a \notin K(R_s)$ and this completes the proof of (1).

(2) If for some $b \in \mathbb{N}$ of the form in (2) we have $b \in A$, then $m' \mid b$ for some $m' \in R_0 \cup \cdots \cup R_{s-1}$ ($m' \notin R_s$, because $p_s \nmid b$). Since A is a "downset", $p^+(R_0 \cup \cdots \cup R_{s-1}, Q) \leq s-1$ and since $p^-(b') > p_s$, $p \mid b'$ implies $p \in \mathbb{P} \setminus Q$ or $b' = 1$, we have $m' \mid p_{i_1} \dots p_{i_{t-1}} q_{j_1} \dots q_{j_\ell}$ as well, and hence $m' \mid a$, which is a contradiction to $a \in K(R_s)$.

□

Let

$$Z = \{a^* \in K(R_s) \cap \mathbb{N}^* : a^* = p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell}, p_{i_1} < \cdots < p_{i_t} = p_s < q_{j_1} < \cdots < q_{j_\ell}, q_{j_i} \in Q\}$$

and let for $a^* \in Z, E(a^*)$ denotes the set of all integers a' of the form (1) in Lemma 6 with $a' \leq n$.

From Lemma 6 (1) immediately follows

$$K(R_s) = \dot{\bigcup_{a^* \in Z}} E(a^*). \tag{4.7}$$

Finally, from Lemma 5 (1) and (4.7) we have

$$K^i(R_s) = \bigcup_{a^* \in Z^i} E(a^*), i = 0, 1, \tag{4.8}$$

where $Z^i = Z \cap K^i(R_s), i = 0, 1$.

5. Proof of Theorem 1

Let $Q = \{q_1, q_2, \dots, q_r\}$, $2 < q_1 < \cdots < q_r$, $n \in \mathbb{N}$, $n \geq \prod_{i=1}^r q_i$ and let $\mathcal{O}(n, Q)$ be the set of all optimal sets. For every $B \in \mathcal{O}(n, Q)$ we consider $P(B)$ the primitive, generating subset of B : $B = M\big(P(B)\big) \cap \mathbb{N}(n)$.

Let

$$p_s = \min_{B \in \mathcal{O}(n,Q)} p^+\big(P(B), Q\big),$$

where $p^+\big(P(B), Q\big)$ is defined in (4.1), and $p_s \in (\mathbb{P} \setminus Q) \cup \{1\}$.

Let $\mathcal{O}_1(n, Q) = \{B \in \mathcal{O}(n, Q) : p^+\big(P(B), Q\big) = p_s\}$. Our first step is to prove

$$p_s \leq 2. \tag{5.1}$$

From Lemma 1 and 4 it follows that

$$\mathcal{O}_1(n, Q) \cap C(Q) \neq \varnothing.$$

Let $A \in \mathcal{O}_1(n,Q) \cap C(Q)$ and suppose to the opposite of (5.1) that $p_s \geq 3$, i.e. $s \geq 2$.

Let $P(A) = R_0 \cup R_1 \cup \cdots \cup R_s$, where the R_{i-s} are described in (4.2).

We also recall the definitions of the sets $R_s^i, G_s^i, K^i(R_s)$ (see (4.3), (4.4)). We consider the following two sets:

$$A^i = M(R_0 \cup \cdots \cup R_{s-1} \cup G_s^i) \cap \mathbb{N}(n), i = 0, 1.$$

From Lemma 5 we know that $A^0, A^1 \in I(n,Q)$ and we are going to prove, that at least one of the following inequalities $|A^0| \geq |A|, |A^1| \geq |A|$ holds. Suppose

$$|K^1(R_s) \cap \mathbb{N}(n)| \geq |K^0(R_s) \cap \mathbb{N}(n)| \tag{5.2}$$

(the opposite case is symmetrically the same), and let us prove that

$$|A^1| = |M(R_0 \cup \cdots \cup R_{s-1} \cup G_s^1) \cap \mathbb{N}(n)| \geq |A|. \tag{5.3}$$

Let

$$K^* \big(M(G_s^1) \smallsetminus M(R_0 \cup \cdots \cup R_{s-1})\big) \cap \mathbb{N}(n).$$

In the light of (5.2), sufficient for (5.3) is

$$|K^*| \geq 2|K^1(R_s)|. \tag{5.4}$$

From (4.8) we know that

$$K^1(R_s) = \bigcup_{a^* \in Z^1} E(a^*), \quad \text{where} \tag{5.5}$$

$$Z^1 = \{a^* \in K^1(R_s) \cap \mathbb{N}^* : a^* = p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell}, p_{j_1} < \dots < p_{i_t} = p_s < q_{j_1} < \dots < q_{j_\ell}, q_{j_i} \in Q\}$$

and

$$E(a^*) = \{a \leq n : a = p_{i_1}^{\alpha_1} \dots p_{i_t}^{\alpha_t} \cdot q_{j_1}^{\beta_1} \dots q_{j_\ell}^{\beta_\ell} \cdot a_3, \alpha_i \geq 1, \beta_i \geq 1, p^-(a_3) > p_s, p \mid a_3 \Rightarrow p \in \mathbb{P} \smallsetminus Q$$
$$\text{or } \ a_3 = 1, \ \text{ and } \ a^* = p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell} \in Z^1\}.$$

It is easy to see that one can write the set $E(a^*)$ in the following form:

$$E(a^*) = \left\{a \leq n : a = a^* \cdot a_3', a_3' \in \phi\left(\frac{n}{a^*}, T\right)\right\}, \tag{5.6}$$

where $T = \big(\{p_1, \dots, p_s) \smallsetminus \{p_{i_1}, \dots, p_{i_t}\}\big) \cup \big(\{q \in Q : q > p_s\} \smallsetminus \{q_{j_1}, \dots, q_{j_\ell}\}\big)$.

Hence

$$|E(a^*)| = \left|\phi\left(\frac{n}{a^*}, T\right)\right| \tag{5.7}$$

for every $a^* \in Z^1$ and $T = T(a^*)$, as described in (5.6).

Now, for any $a^* \in Z^1$, $a^* = p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell}$, $p_{i_1} < \dots < p_{i_t} = p_s < q_{j_1} < \dots < q_{j_\ell}; q_{j_i} \in Q$ we consider the integer $b^* = \frac{a^*}{p_s} = p_{i_1} \dots p_{i_{t-1}} \cdot q_{j_1} \dots q_{j_\ell}$ and the set

$E^*(b^*) = \{b \le n : b = p_{i_1}^{\gamma_1} \dots p_{i_{t-1}}^{\gamma_{t-1}} \cdot q_{j_1}^{\delta_1} \dots q_{j_\ell}^{\delta_\ell} \cdot b_3, \gamma_i, \delta_i \ge 1, p^-(b_3) \ge p_s, p \mid b_3 \Rightarrow p \in \mathbb{P} \setminus Q$ or $b_3 = 1\}$.

One can write the set $E^*(b^*)$ in the form:

$$E^*(b^*) = \left\{b \le n : b = b^* \cdot b_3', b_3' \in \phi\left(\frac{n}{b^*}, T\right)\right\},$$

where the set T is the same as in (5.6).

Hence

$$|E^*(b^*)| = \left|\phi\left(\frac{n}{b^*}, T\right)\right| = \left|\left(\frac{n \cdot p_s}{a^*}, T\right)\right|. \tag{5.8}$$

From the definitions of the sets $E(a^*)$ and $E^*(b^*)$ we know for every $a^* \in Z^1$, $b^* = \frac{a^*}{p_s}$, that

$$E_0^*(b^*) = E(a^*), \tag{5.9}$$

where $E_0^*(b^*) = \{b \in E^*(b^*) : p_s \mid b\}$ and that (by Lemma 6 (2))

$$\left(E^*(b^*) \setminus E_0^*(b^*)\right) \cap A = \varnothing. \tag{5.10}$$

Hence, in the light of (5.5) – (5.10), sufficient for (5.4) is

$$|E^*(b^*)| \ge 2|E(a^*)| \text{ for every } a^* \in Z^1, b^* = \frac{a^*}{p_s}, \tag{5.11}$$

which by (5.7) and (5.8) is equivalent to

$$\left|\phi\left(\frac{n \cdot p_s}{a^*}, T\right)\right| \ge 2 \cdot \left|\phi\left(\frac{n}{a^*}, T\right)\right| \tag{5.12}$$

for $T = \left(\{p_1, \dots, p_s\} \setminus \{p_{i_1}, \dots, p_{i_t}\}\right) \cup \left(\{q \in Q : q > p_s\} \setminus \{q_{j_1}, \dots, q_{j_\ell}\}\right)$,
$a^* = p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell}; p_{i_1} < p_{i_2} < \dots < p_{i_t} = p_s < q_{j_1} < \dots < q_{j_\ell}, q_{j_i} \in Q$.

Now we are in the position to apply Theorem 3 to show the validity of (5.12). The sets of primes T_1, T_2, T_3 in Theorem 3 are now

$T_1 = \{p_1, \dots, p_s\} \setminus \{p_{i_1}, \dots, p_{i_t}\} = \{p_1, \dots, p_{s-1}\} \setminus \{p_{i_1}, \dots, p_{i_{t-1}}\}$, $(p_{i_t} = p_s)$

$T_2 = \{q \in Q : q > p_s\} \setminus \{q_{j_1}, \dots, q_{j_\ell}\}$, and $T_3 = \{p_{i_1}, \dots, p_{i_t}\}$.

The condition (3.12), i.e. $u \ge \frac{\prod_{p \in T_2} p}{\prod_{p \in T_3} p}$, also holds, because $n \ge \prod_{q \in Q} q$ yields

$$u = \frac{n}{a^*} = \frac{n}{p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell}} \ge \frac{\prod_{q \in Q} q}{p_{i_1} \dots p_{i_t} \cdot q_{j_1} \dots q_{j_\ell}} \ge \frac{\prod_{q \in T_2} q}{\prod_{p \in T_3} p}.$$

This proves (5.12) and consequently (5.3):

$$|A^1| = |M(R_0 \cup \dots \cup R_{s-1} \cup G_s^1) \cap \mathbb{N}(n)| \geq |A|.$$

Hence $A^1 \in \mathcal{O}(n,Q)$, because $A \in \mathcal{O}(n,Q)$ and $A^1 \in I(n,Q)$. Obviously, $P(A') \subset R_0 \cup \dots \cup R_{s-1} \cup G_s^1$. Therefore $p^+\big(P(A'),Q\big) < p_s$, which is a contradiction to the definition $p_s = \min\limits_{B \in \mathcal{O}(n,Q)} p^+\big(P(B),Q\big)$. This proves (5.1).

Since for every $B \in \mathcal{O}_1(n,Q)$ we have $b_i \in P(B)$ it follows that either

$$p \nmid b_i \quad \text{for all} \quad p \in \mathbb{P} \setminus Q$$

or

$$2 \mid b_i, \quad \text{but} \quad p \nmid b_i, p \in \mathbb{P} \setminus \big(Q \cup \{2\}\big).$$

Let

$$q_t = \min_{B \in \mathcal{O}_1(n,Q)} p^+\big(P(B),\phi\big),$$

and let

$$\mathcal{O}_2(n,Q) = \big\{B \in \mathcal{O}_1(n,Q) : p^+\big(P(B),\phi\big) = q_t\big\}.$$

Again, it is easy to see, that

$$\mathcal{O}_2(n,Q) \cap C(Q) \neq \varnothing.$$

Let

$$A \in \mathcal{O}_2(n,Q) \cap C(Q).$$

We write $P(A)$ in the form

$$P(A) = S_1 \,\dot\cup\, S_2 \,\dot\cup \dots \dot\cup\, S_t,$$

where $S_i = \big\{b \in p(A) : p^+(b) = q_i\big\}$, $1 \leq i \leq t \leq r$.

We are going to prove, that $P(A) = \{q_1\}$, if $t = 1$, and $P(A) = \{2q_1, \dots, 2q_t, q_1 \dots q_t\}$, if $t > 1$, and this is equivalent to the statement (1.4) of Theorem 1.

If $t = 1$, then clearly $P(A) = \{q_1\}$ and the Theorem is true. Hence we assume $t > 1$. We observe that $\{q_t\} \notin S_1$, because otherwise $\{q_1\} \in S_1$ as well, since $A \in C(Q)$ and hence $(q_t, q_1) = 1$ in contradiction to $A \in I(n,Q)$. Let us assume that

$$2 \cdot q_t \notin S_t. \tag{5.13}$$

Since $A \in \mathcal{O}_2(n,Q) \subset \mathcal{O}_1(n,Q)$, (5.13) means that every integer $a \in S_t$ has at least two different primes from the set Q in its prime decomposition (one of this primes is of course q_t).

Let us prove that the assumption (5.13) is false. For this we choose a similar approach as for proving (5.1). Let

$$S_t = S_t^0 \,\dot\cup\, S_t^1,$$

where $S_t^0 = \{a \in S_t : q_{t-1} \mid a\}$, $S_t^1 = S_t \setminus S_t^0$ and

$$V_t^i = \{m \in \mathbb{N} : m \cdot q_t \in S_t^i\}, i = 0, 1.$$

Under assumption (5.13) it can be shown that

$$A^i = M(S_1 \cup \cdots \cup S_{t-1} \cup V_t^i) \cap \mathbb{N}(n) \in I(n, Q), i = 0, 1.$$

Using the approach described in the first part of this paragraph it can be proved that at least one of the inequalities

$$|A^0| \geq |A|, |A^1| \geq |A| \text{ holds.} \tag{5.14}$$

We mention that only a very special case of Lemma 2 has been used and not Theorem 3. We also note that here we do not need a restriction on n like $n \geq \prod_{q \in Q} q$.

It can be seen that the fact (5.14) contradicts $A \in \mathcal{O}_2(n, Q)$ and hence the assumption (5.13) is false. Therefore $2 \cdot q_t \in S_t$ for $A \in \mathcal{O}_2(n, Q) \cap C(Q)$ and $P(A) = S_1 \cup \cdots \cup S_t$.

However, from $2 \cdot q_t \in S_t \subset A \in \mathcal{O}_2(n, Q) \cap C(Q)$ it follows that $2 \cdot q_1, \ldots, 2q_{t-1} \in A$ as well and that $q_i \notin A$ for all $q_i \in Q$. Hence $2q_1, 2q_2, \ldots, 2q_t \in P(A)$.

Let $a \in P(A)$ and $a \neq 2q_i$, $i = 1, \ldots, t$. Since $p^+(a) \leq q_t$ $\big(A \in \mathcal{O}_2(n, Q)\big)$, then $2 \nmid a$ for otherwise $2q_i \mid a$ for some $i \leq t$, which is impossible, because $P(A)$ is primitive.

Therefore $2 \nmid a$ and $a = q_1 \ldots q_t$, because otherwise $(a, 2q_i) = 1$ for some $i \leq t$. Hence $P(A) = \{2q_1, \ldots, 2q_t, q_1 \ldots q_t\}$ and Theorem 1 is proved.

□

Proof of Theorem 2:

Since the proof is very similar (and much easier) than the proof of Theorem 1, we will give only a *sketch*.

We repeat all steps up to formula (5.4) (proof of which was the most difficult part of Theroem 1) and observe that (5.4) trivially holds for squarefree numbers without any restriction on n .

The situation is similar with formula (5.14) (which was the second main step in the proof of Theorem 1).

6. Example of $Q \subset \mathbb{P}$ and $n, n < \prod_{q \in Q} q$, for which the conclusion of Theorem 1 does not hold

We take $Q \subset \mathbb{P}$ as follows:

$$Q = \{q_1, q_2, \ldots, q_{r-1}, q_r\} = \{5, 7, \ldots, p_{r+1}, q_r\},$$

i.e. $q_i = p_{i+2}$, $i = 1, 2, \ldots, r-1$ and q_r is a prime specified in (6.3) below.
We also assume that

$$q_{r-1} = p_{r+1} > 1000. \tag{6.1}$$

Let

$$n = 2 \cdot 3 \cdot 11 \cdot \prod_{i=1}^{r-1} q_i. \tag{6.2}$$

Finally, as a $q_r \in \mathbb{P}$ we take any prime satisfying

$$\frac{n}{2000} < q_r < \frac{n}{1000}. \tag{6.3}$$

The existence of such primes follows from Bertrand's postulate. We use the abbreviation

$$H_j = M\{2q_1, 2q_2, \ldots, 2q_j, q_1 \ldots q_j\} \cap \mathbb{N}(n); j = 1, \ldots, r.$$

We are going to prove, that for the specified $Q \subset \mathbb{P}$ and n , the conclusion of Theorem 1 does not hold, i.e.

$$f(n, Q) > \max_{1 \le j \le r} |H_j|. \tag{6.4}$$

We show first that

$$\max_{1 \le j \le r} |H_j| = \max\bigl\{|H_{r-1}|, |H_r|\bigr\}. \tag{6.5}$$

Since $2 \cdot \prod_{i=1}^{r-1} q_i \mid n$, it is easy to see that

$$|H_j| = n \cdot \frac{1}{2} \left(1 - \prod_{i=1}^{j} \left(1 - \frac{1}{q_i}\right) + \frac{1}{q_1 \ldots q_j}\right) \quad \text{for all} \quad 1 \le j \le r-1$$

and that

$$|H_2| < |H_3| < |H_4| < \cdots < |H_{r-1}|.$$

This proves (6.5), because

$$|H_1| = \frac{1}{5} n < \frac{1063}{5005} n = |H_4|$$

and trivially $r - 1 \ge 4$ (see (6.1)).

Clearly, to prove (6.4), it is sufficient to find a set $A \in I(n, Q)$ for which

$$|A| > \max_{1 \le j \le r} |H_j| = \max\{|H_{r-1}|, |H_r|\}.$$

We choose A as follows:

$$A = M\{2q_1, 2q_2, \dots, 2 \cdot q_{r-1}, 2 \cdot 3 \cdot q_r, 3 \cdot q_1 \cdot \ldots \cdot q_{r-1}\} \cap \mathbb{N}(n).$$

Obviously, $A \in I(n, Q)$ and we have to show that both hold:

$$|A| > |H_{r-1}| \tag{6.6}$$

and

$$|A| > |H_r|. \tag{6.7}$$

We consider first the set $H_{r-1} \setminus A$. Since

$$H_{r-1} = M\{2q_1, \dots, 2q_{r-1}, q_1 q_2 \dots q_{r-1}\} \cap \mathbb{N}(n),$$

the set $H_{r-1} \setminus A$ consists only of integers of the form

$$a \cdot q_1 \cdot q_2 \dots q_{r-1} \le n = 2 \cdot 3 \cdot 11 \cdot q_1 \dots q_{r-1} = 66 q_1 \dots q_{r-1}$$

and $(a, 6) = 1$, because for $(a, 6) \ne 1$ we have $a \cdot q_1 \dots q_{r-1} \in A$. There are exactly 22 integers a with $a \le 66$, $(a, 6) = 1$. Hence

$$|H_{r-1} \setminus A| = 22.$$

Now we consider the set $A \setminus H_{r-1}$.

It is clear that all integers of the form $2^\alpha \cdot 3^\beta \cdot q_r \le n$, $\alpha \ge 1$, $\beta \ge 1$, are in the set $A \setminus H_{r-1}$. We verify that there are 24 integers of the form $2^\alpha \cdot 3^\beta < 1000$, $\alpha \ge 1$, $\beta \ge 1$ and since $1000 \cdot q_r < n$ (by (6.3)) we conclude that $|A \setminus H_{r-1}| \ge 24 > |H_{r-1} \setminus A| = 22$. This proves (6.6).

To prove (6.7) we compare the cardinalities of the sets $H_r \setminus A$ and $A \setminus H_r$. Since $H_r = M\{2q_1, 2q_2, \dots, 2q_{r-1}, 2q_r, q_1 \dots q_r\} \cap \mathbb{N}(n) = M\{2q_1, \dots, 2q_r\} \cap \mathbb{N}(n)$ (because $q_1 \dots q_r > n$), $H_r \setminus A$ consists only of integers of the form

$$2 \cdot q_r \cdot b \le n, \tag{6.8}$$

where b is not divisible by anyone of the primes $3, q_1, \dots, q_{r-1}$.

Since $q_r > \frac{n}{2000}$ (see (6.3)), we conclude from (6.8) that $b < 1000$. However, since $q_{r-1} > 1000$, (see (6.1)), we have $b \in \{1, 2, \dots, 2^9\}$ and hence

$$|H_r \setminus A| \le 10.$$

Now we consider the set $A \setminus H_r$.

This set consists of the integers of the form

$$3 \cdot q_1 \dots q_{r-1} \cdot c \le n = 66 q_1 \dots q_{r-1},$$

where $2 \nmid c$. There are exactly 11 such integers $c \le 22$. Hence

$$|A \setminus H_r| = 11 > 10 = |H_r \setminus A|$$

and this proves (6.7).

7. Directions of research

We think that our methods are applicable to other number theoretical extremal problems.

A first question is how $f(n,Q)$ can be characterized, if Q is an infinite set of primes.

Perhaps more demanding is the problem of finding a common generalisation of the problem analysed in this paper and its in dual in [3]:

For (finite) sets $Q_1, Q_2 \subset \mathbb{P}$, $Q_1 \cap Q_2 = \varnothing$, and $n \in \mathbb{N}$, what is the maximal cardinality k of sets $A = \{a_1 < \dots < a_k\} \subset \mathbb{N}(n)$ satisfying $(a_i, a_j) \neq 1$, $\left(a_i, \prod_{q \in Q_1} q\right) \neq 1$, and $\left(a_i, \prod_{q \in Q_2} q\right) = 1$ for all i, j ?

Instead of requiring that no two numbers of A are relatively prime one can require that no ℓ numbers are pairwise relatively prime.

References

[1] P. Erdös, “Problems and results in combinatorial number theory”, Chapt. 12 in: A Survey of Combinatorial Theory, J.N. Srivastava et al (eds.), North–Holland, 1973.

[2] P. Erdös, “A survey of problems in combinatorial number theory”, Ann. Discrete Math. 6, 89–115, 1980.

[3] R. Ahlswede and L.H. Khachatrian, “Sets of integers and quasi–integers with pairwise common divisor”, to appear in Acta Arithmetica.

[4] J.B. Rosser and L. Schoenfeld, “Approximate formulas for some functions of prime numbers”, Illinois J. Math. 6, 64–89, 1962.

[5] P. Ribenboim, “The little book of big primes”, Springer–Verlag 1991.

[6] R. Ahlswede and L.H. Khachatrian, “Maximal sets of numbers not containing $k+1$ pairwise coprime integers”, to appear in Acta Arithmetica.