ON A CONJECTURE OF GRAHAM

J. W. SANDER

(Communicated by Larry T. Goldstein)

Abstract. Let \(a_1 < a_2 < \cdots < a_n\) be a finite sequence of positive integers containing a prime power \(p^d\) with the property: \(a_i \neq p^k a_j\) for all \(i, j\) and \(k > 0\). Then \(\max_{i,j} a_i/(a_i, a_j) \geq n\).

In [4] R. L. Graham asks if the following is true: Let \(A\) be a finite sequence of \(n\) positive integers \(a_1 < a_2 < \cdots < a_n\). Then \(\max_{i,j} a_i/(a_i, a_j) \geq n\).

Several partial results have been obtained (see the references), particularly for the case where one of the \(a_i\)'s is prime. The proofs for the latter follow similar lines, E. Z. Chein [2] and R. Klein [5] use G. Weinstein's improvement [9] upon R. Winterle's earlier result [10] while R. J. Simpson [7] can do without. In this paper we use refinements of the methods of Winterle [10] and Klein [5] to prove the following theorem. The sequence \(A\) is said to be \(p\)-simple for a prime \(p\) if \(a_i \neq p^k a_j\) for \(1 \leq i, j \leq n, k > 0\).

**THEOREM.** Let \(A\) be \(p\)-simple for a prime \(p \neq 2\) and let \(A\) contain a prime power \(a_k = p^d\) \((d \geq 0)\). Then
\[
\max_{1 \leq i, j \leq n} \frac{a_i}{(a_i, a_j)} \geq n.
\]

In order to prove the theorem we first consider the case where \(a_1\) is the required prime power. For a given sequence \(A\) let \(A = \{a_1, \ldots, a_n\}\).

**LEMMA.** Let \(A\) be \(p\)-simple with \(a_1 = p^d\) \((d \geq 0)\). Then
\[
\max_{i,j} \frac{a_i}{(a_i, a_j)} \geq n.
\]

**PROOF.** We may assume \(d > 0\), since the lemma is trivial for \(a_1 = 1\). We suppose
\[
(1) \quad \max_{i,j} \frac{a_i}{(a_i, a_j)} \leq n - 1.
\]
This implies
\[
(2) \quad a_n \leq (n - 1)(a_n, a_1) \leq (n - 1)p^d.
\]
For \(k = 0, 1, \ldots, d - 1\) define
\[
B_k = \{a_i \in A : p^k \| a_i\}, \quad \text{and} \quad B = A \setminus \bigcup_{k=0}^{d-1} B_k.
\]
Furthermore, for \( k = 0, 1, \ldots, d - 1 \) and each \( a_i \in B_k \) define
\[
T_k(a_i) = p^{h_{i,k}}(a_i - p^{k+1})
\]
such that \( h_{i,k} \) is maximal with
\[
T_k(a_i) \leq (n - 1)p^d.
\]
Obviously, \( T_k(a_i) > 0 \) and the maximality of \( h_{i,k} \) gives
\[
T_k(a_i) > (n - 1)p^{d-1}.
\]
We have for \( a_i \in B_k \)
\[
a_i \leq (n - 1)p^k;
\]
otherwise \( a_i = p^ka_i' \) with \( a_i' \geq n, p \nmid a_i' \). This yields \( a_i/(a_i, a_1) = p^ka_{i}'/p^k = a_i' \geq n \) which contradicts (1). By (3), (4) and (6) we have \( h_{i,k} \geq d - k \) which implies
\[
p^d|T_k(a_i).
\]
Since \( (a_i, a_i - p^{k+1}) = (a_i, p^{k+1}) = p^k \) for \( a_i \in B_k \), we get
\[
(a_i, T_k(a_i)) = p^k.
\]
We claim for \( a_i \in B_k, a_j \in B, \)
\[
T_k(a_i) \neq a_j;
\]
otherwise by (5) and (8)
\[
a_j/(a_j, a_i) = T_k(a_i)/(T_k(a_i), a_i) > n - 1
\]
which contradicts (1).

We claim for \( a_i \in B_{k1}, a_j \in B_{k2}, a_i \neq a_j, \)
\[
T_{k_1}(a_i) \neq T_{k_2}(a_j);
\]
otherwise
\[
p^{h_{i,k_1}}(a_i - p^{k_1+1}) = p^{h_{i,k_2}}(a_j - p^{k_2+1}),
\]
and hence
\[
a_i/p^{k_1} - p = a_j/p^{k_2} - p
\]
which contradicts the \( p \)-simplicity of \( A \).

Now define the following function \( F: A \to \mathbb{N} \) by
\[
F(a_i) = \begin{cases} 
T_k(a_i) & \text{for } a_i \in B_k, \\
\frac{a_i}{a_i} & \text{for } a_i \in B.
\end{cases}
\]
By (9) and (10) \( F \) is 1-1. By (2), (4) and (7) we have for all \( i = 1, \ldots, n \)
\[
0 < F(a_i) \leq (n - 1)p^d \quad \text{and} \quad p^d|F(a_i).
\]
This contradiction proves the lemma.

**Proof of the Theorem.** We may assume that \( A \) is proper, i.e. the g.c.d. of the \( a_i \)'s is 1. We may also assume that \( p^d \) is the lowest \( p \)-power in \( A \) and \( d > 0 \). We suppose
\[
\max_{i,j} \frac{a_i}{(a_i, a_j)} \leq n - 1.
\]

Define $B_0 = \{1, 2, \ldots, n-1\} \setminus \{p, p^2, \ldots, p^{d-1}\}$ and $B_d = \{lp^d : \lfloor n/p^d \rfloor \leq l \leq n-2\}$; for $h = 1, 2, \ldots, d-1$ let

$$B_h = \{lp^h : \lfloor n/p^h \rfloor \leq l \leq n-1, (l, p) = 1\}.$$ 

Obviously, $B_0, \ldots, B_d$ are pairwise disjoint.

We claim

$$A \subseteq \bigcup_{h=0}^{d} B_h;$$

therefore, let $a_i \in A$. If $a_i \leq n-1$ then $a_i \in B_0$ since $p^d$ is the lowest $p$-power in $A$. If $a_i \geq n$ then $p|a_i$, for otherwise $a_i/(a_i, a_k) = a_i/(a_i, p^d) = a_i \geq n$, contradicting (11). Now we distinguish between two cases:

Case 1. $p^h|a_i$ for some $h$, $1 \leq h \leq d-1$. Then $a_i = p^h a_i'$, $(a_i', p) = 1$, say. Hence $a_i' \geq \lfloor n/p^h \rfloor$ and by (11)

$$p^h a_i' = a_i \leq (n-1)(a_i, a_k) = (n-1)(a_i, p^d) = (n-1)p^h,$$

thus $a_i' \leq n-1$, so $a_i \in B_h$.

Case 2. $p^d|a_i$. Then $a_i = p^d a_i'$, say. Hence $a_i' \geq \lfloor n/p^d \rfloor$ and by the lemma

$$a_i < a_k = p^d,$$

and by (11)

$$p^d a_i' = a_i \leq (n-1)(a_i, a_k) = (n-1)(a_i, p^d) = (n-1)p^d,$$

thus $a_i' \leq n-1$, so $a_i \in B_d$.

This proves the claim (12).

We define for $h = 1, \ldots, d$

$$C_h = B_h \cap A, \quad C'_h = C_h \setminus \{(n-1)p^h\}, \quad C' = \bigcup_{h=1}^{d} C'_h.$$ 

Let $B'_0 = \{b \in B_0 : p \nmid b\}$. Define a function $f : C' \rightarrow B'_0$ in the following way:

$$x' \in C', \quad x = p^t b \ (p \nmid b, \ b \leq n-2) \text{ say}; \quad \text{then } f(x) = b.$$ 

The function $f$ is 1-1. Otherwise we have $b = b'$ for $x = p^t b$ and $x' = p^t b' \ (p \nmid bb')$. This implies $p^t x = p^t x'$ which contradicts the $p$-simplicity of $A$.

For $b \in B'_0$ there is $r$ with $1 \leq r \leq p-1$ and $b \equiv r \mod p$. Define a function $g : f(C') \rightarrow B'_0$ by

$$g(b) = \begin{cases} 
 b + 1 & \text{for } 2 \nmid r, \\
 b - 1 & \text{for } 2 \mid r.
\end{cases}$$ 

Since $2|(p-1)$ and $b \leq n-2$ in (13) we have indeed

$$g(f(C')) \subseteq B'_0.$$ 

It is easily seen that $g$ is 1-1:

The only interesting case is $g(b) = b + 1$, $g(b') = b' - 1$, $g(b) = g(b')$. This implies $b = sp + r, b' = s'p + r'$ with $2 \nmid r, 2|r'$, for some $s, s'$, and $b + 2 = b'$. Hence $(s' - s)p = r - r' + 2$. Since $|r - r'| \leq p - 2$ we can have $p|(r - r' + 2)$ only for $r - r' + 2 = 0$ or $r - r' + 2 = p$. The former gives $r \equiv r' \mod 2$, the latter $r = p - 1 \equiv 0 \mod 2$, both contradicting the conditions on $r$ and $r'$. 


For $C = \bigcup_{h=1}^{d} C_h$ and $B = \{1, 2, \ldots, n - 1\}$ define the function $F : C \to B$ as follows:

$$F(x) = \begin{cases} g(f(x)) & \text{for } x \in C', \\ p^h & \text{for } x = (n-1)p^h (p \nmid (n-1), 1 \leq h \leq p-1). \end{cases}$$

Indeed, $p^h \in B$, because $p^d \in B$; otherwise, since the g.c.d. of the $a_i$'s is 1, there is $a_m$ with $p \nmid a_m$; thus $a_k/(a_k,a_m) = p^d \geq n$ which contradicts (11). By (14) $F$ is 1-1.

For $x \in C'$, $x = p^tb$ (if $b$), say, we have $p \nmid F(x)$, so $(x,F(x)) = (p^tb,b\pm1) = 1$. Since $x \in A$, $F(x)$ cannot belong to $A$, because $x/(x,F(x)) \geq n$ again contradicts (11). Also, the numbers $p^h$ ($1 \leq h \leq d-1$) do not belong to $A$, because $p^d$ is the lowest $p$-power in $A$.

Thus we have found a 1-1 function $F : C \to B$ with $\text{card}(F(C) \cup (A \cap B)) = n$; but $F(C) \cup (A \cap B) \subseteq B$. This contradiction proves the theorem.

REFERENCES


INSTITUT FÜR MATHEMATIK, UNIVERSITÄT HANNOVER, WELFENGARTEN 1, 3000 HANNOVER 1, FEDERAL REPUBLIC OF GERMANY