PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 63, Number 1, March 1977

ON A CONJECTURE OF GRAHAM CONCERNING GREATEST COMMON DIVISORS

GERALD WEINSTEIN

ABSTRACT. Let $a_1 < a_2 < \cdots < a_n$ be a finite sequence of positive integers. R. L. Graham has conjectured that $\max_{i,j}\{a_i/(a_i, a_j)\} \geqslant n$. The following are proved:

(1) If $a_l = p$, a prime, for some l and $p \neq (a_i + a_j)/2$, $1 \leqslant i < j \leqslant n$, then the conjecture holds.

(2) Given a finite sequence of positive integers $k_1 < k_2 < \cdots < k_m$, where $k_I = p$, a prime, for some I and $k_m < n$, consider the set of all positive integral multiples of $k_1, k_2, \ldots, k_m$ which are $< n$. Denote these multiples by $a_1 < a_2 < \cdots < a_q$. Define P_n to be a set consisting of the integers $a_1 < a_2 < \cdots < a_q < a_{q+1} < \cdots < a_{q+r}$ where r is maximal, such that $n \leqslant a_{q+1}$ and $\max_{i,j}\{a_i/(a_i, a_j)\} < n$. Thus

$$P_n = P_n(k_1, k_2, \ldots, k_m).$$

Then

(a) $|P_n| \geqslant n$ for at most finitely many n.

(b) If $|P_n| < n$ for $n <$ l.c.m.$\{k_1, k_2, \ldots, k_m\}$ then $|P_n| < n$ for all positive integers n.

In this note we consider the following conjecture of R. L. Graham [1]. Let $a_1 < a_2 < \cdots < a_n$ be a finite sequence of positive integers. Then $\max_{i,j}\{a_i/(a_i, a_j)\} \geqslant n$.

This conjecture has attracted many investigators and has been verified in the following special cases:

(a) a_i is square-free for all i (Marica and Schönheim [2]).

(b) a_1 is prime (Winterle [3]).

(c) n is prime (Szemerédi [4]).

(d) $n - 1$ is prime (Vélez [4]).

Vélez [4] also considers another conjecture of Graham as to the form of those sequences for which equality is achieved and shows that this second conjecture implies the title conjecture.

Here we prove two generalizations of Winterle's result (b).

Part I.

THEOREM 1. *If A is the sequence $a_1 < a_2 < \cdots < a_n$, where $a_k = p$, a prime, for some k and $p \neq (a_i + a_j)/2$, $1 \leqslant i < j \leqslant n$, then*

$$\max_{i,j}\{a_i/(a_i, a_j)\} \geqslant n.$$

Received by the editors January 19, 1976.
AMS (MOS) subject classifications (1970). Primary 10A05.

PROOF. We assume that $\max_{i,j}\{a_i/(a_i, a_j)\} < n$ so that

$$a_n \leqslant (n-1)(a_n, p) \leqslant (n-1)p.$$

Let B be the subsequence $b_1 < b_2 < \cdots < b_r$ consisting of all terms in A not divisible by p. Since we may assume that the g.c.d. of the terms of A is 1, B is not empty and $b_r \leqslant n-1$. We define a mapping T by $T(b_i) = p^h|b_i - p|$, where h is the largest nonnegative integer such that $p^h|b_i - p| \leqslant (n-1)p$. Since $|b_i - p| < n-1$, h is always positive, hence $p|T(b_i)$ for all b_i. Since $(p, b_i) = 1$ and $(|b_i - p|, b_i) = 1$, we have $(b_i, T(b_i)) = 1$ for all b_i. Also, if $T(b_i) \leqslant n-1$, then $pT(b_i) \leqslant (n-1)p$, which contradicts the definition of $T(b_i)$. Thus $T(b_i) \geqslant n$ for all b_i. These two results imply that $T(b_i)$ is never a term of the sequence A.

Now assume that $T(b_i) = T(b_j)$. Then $p^h|b_i - p| = p^k|b_j - p|$ for some h and k. Since p does not divide either $|b_i - p|$ or $|b_j - p|$, we see that $h = k$ and so $b_i - p = \pm(b_j - p)$. Since the minus sign contradicts the hypothesis, we must have $b_i = b_j$.

We now define $F(a_i)$, for each $a_i \in A$, as follows:

$$F(a_i) = a_i \qquad \text{if } p|a_i,$$

$$F(a_i) = T(a_i) \quad \text{if } a_i \in B.$$

Then $p|F(a_i) \leqslant (n-1)p$ for all $a_i \in A$. Also, since T is 1-1 and never maps b_i into $A - B$, it follows that F is 1-1. Hence $|A| \leqslant n-1$; this contradicts the fact that $|A| = n$ and so completes the proof.

COROLLARY 1 (WINTERLE). *Given the sequence* $a_1 < a_2 < \cdots < a_n$, *where* $a_1 = p$, *a prime, then* $\max_{i,j}\{a_i/(a_i, a_j)\} \geqslant n$.

COROLLARY 2. *Given the sequence* $a_1 < a_2 < \cdots < a_n$, *where* $a_k = p$ *and* $a_{k+1} \geqslant 2p$, *for some* k, p *a prime, then* $\max_{i,j}\{a_i/(a_i, a_j)\} \geqslant n$.

PROOF. In both corollaries it is clear that $p \neq (a_i + a_j)/2$ for $1 \leqslant i < j \leqslant n$.

Part II. If we omit the condition of Theorem 1 that $p \neq (a_i + a_j)/2$, $1 \leqslant i < j \leqslant n$, we can still show that the conjecture is "ultimately" true in the following sense.

Given a finite sequence of positive integers $k_1 < k_2 < \cdots < k_m$ where $k_I = p$, a prime, for some I and $k_m < n$, consider the set of all positive integral multiples of $k_1, k_2, \ldots, k_m$ which are $< n$. Denote these multiples by $a_1 < a_2 < \cdots < a_q$. Define P_n to be a set consisting of the integers $a_1 < a_2 < \cdots < a_q < a_{q+1} < \cdots < a_{q+r}$, where r is maximal such that $n \leqslant a_{q+1}$ and $\max_{i,j}\{a_i/(a_i, a_j)\} < n$. Thus $P_n = P_n(k_1, k_2, \ldots, k_m)$. Then we have

THEOREM 2. (a) $|P_n| \geqslant n$ *for at most finitely many* n.

(b) *If* $|P_n| < n$ *for* $n <$ l.c.m.$\{k_1, k_2, \ldots, k_m\}$ *then* $|P_n| < n$ *for all positive integers* n.

Several remarks are necessary before proceeding to the proof.

(1) We use the following notation:

$[k_i, k_j]$: the least common multiple of k_i and k_j;

$\phi(n)$: the number of positive integers less than, and relatively prime to, n.

(2) We say that $k_1 < k_2 < \cdots < k_m$ is a basis which generates P_n.

(3) Define $I_n^j = \{x \in P_n, (j-1)n \leqslant x < jn\}, j = 1, 2, \ldots, a_1\ (a_1 = k_1)$. Thus $P_n = \bigcup_{j=1}^{a_1} I_n^j$.

(4) There is no loss in generality if we choose $(k_j, p) = 1$ for $k_j \neq p$.

(5) The number of elements in I_n^1 is given by

$$|I_n^1| = \left[\frac{n}{k_1}\right] + \cdots + \left[\frac{n}{k_m}\right] - \left(\left[\frac{n}{[k_1, k_2]}\right] + \cdots + \left[\frac{n}{[k_i, k_j]}\right] + \ldots\right)$$
$$+ \left[\frac{n}{[k_i, k_j, k_l]}\right] + \cdots + (-1)^{m+1}\left[\frac{n}{[k_1, \ldots, k_m]}\right].$$

Define

$$d(I_n^1) = \frac{1}{k_1} + \cdots + \frac{1}{k_m} - \left(\frac{1}{[k_1, k_2]} + \cdots + \frac{1}{[k_i, k_j]} + \ldots\right)$$
$$+ \frac{1}{[k_i, k_j, k_l]} + \cdots + \frac{(-1)^{m+1}}{[k_1, \ldots, k_m]},$$

and

$$d(I_n^2) = 1 - \left(\frac{\phi(k_1)}{k_1} + \cdots + \frac{\phi(k_m)}{k_m}\right)$$
$$+ \left(\frac{\phi([k_1, k_2])}{[k_1, k_2]} + \cdots + \frac{\phi([k_i, k_j])}{[k_i, k_j]} + \ldots\right)$$
$$- \left(\ldots + \frac{\phi([k_i, k_j, k_l])}{[k_i, k_j, k_l]} + \ldots\right) + (-1)^m \frac{\phi([k_1, \ldots, k_m])}{[k_1, \ldots, k_m]}.$$

Then,

$$\frac{1}{n}|I_n^1| \leqslant \frac{1}{n}\left\{\frac{n}{k_1} + \cdots + \frac{n}{k_m} - \left(\frac{n}{[k_1, k_2]} + \cdots + \frac{n}{[k_i, k_j]} + \ldots\right)\right.$$
$$\left. + \frac{n}{[k_i, k_j, k_l]} + \cdots + (-1)^{m+1}\frac{n}{[k_1, \ldots, k_m]} + 2^{m-1}\right\}$$
$$= d(I_n^1) + \frac{2^{m-1}}{n}.$$

Also,

$$\frac{1}{n}|I_n^2| \leqslant \frac{1}{n}\left\{ n - \left(\frac{n}{k_1}\phi(k_1) + \cdots + \frac{n}{k_m}\phi(k_m)\right)\right.$$

$$+ \left(\frac{n}{[k_1, k_2]}\phi([k_1, k_2]) + \cdots + \frac{n}{[k_i, k_j]}\phi([k_i, k_j]) + \ldots \right)$$

$$+ \cdots + (-1)^m \frac{n}{[k_1, \ldots, k_m]}\phi([k_1, \ldots, k_m])$$

$$+ \sum_{i=1}^{m}\phi(k_i) + \sum_{i,j}^{m}\phi([k_i, k_j])$$

$$\left. + \sum_{i,j,l}^{m}\phi([k_i, k_j, k_l]) + \cdots + \phi([k_1, \ldots, k_m])\right\}$$

$$\leqslant d(I_n^2) + (k_1 k_2 \cdots k_m)/n.$$

Note. This implies $n^{-1}|I_n^j| \leqslant d(I_n^2) + (k_1 k_2 \cdots k_m)/n$, $2 \leqslant j \leqslant k_1$.
We need four lemmas.

LEMMA 1. *Let* $2 < b_1 < b_2 < \cdots < b_r$ *be integers. Then*

$$1/b_1 + 1/b_2 + \cdots + 1/b_r - \left(1/[b_1, b_2] + \cdots + 1/[b_i, b_j] + \ldots\right)$$
$$+ \cdots + 1/[b_i, b_j, b_k] + \cdots + (-1)^{r+1}/[b_1, \ldots, b_r]$$
$$< \phi(b_1)/b_1 + \phi(b_2)/b_2 + \cdots + \phi(b_r)/b_r$$
$$- \left(\phi([b_1, b_2])/[b_1, b_2] + \cdots + \phi([b_i, b_j])/[b_i, b_j] + \cdots\right) + \cdots$$
$$+ \phi([b_i, b_j, b_k])/[b_i, b_j, b_k] + \cdots$$
$$+ (-1)^{r+1}\Phi([b_1, \ldots, b_r])/[b_1, \ldots, b_r].$$

PROOF. Define $L = [b_1, b_2, \ldots, b_r]$. Let M be the set of all multiples of b_1, $b_2, \ldots, b_r$ which are less than or equal to L. Let N be the set of all numbers which are relatively prime to at least one of $b_1, b_2, \ldots, b_r$ and less than or equal to L. Then the inequality is equivalent to the statement $|M| < |N|$. To see that the latter is true, define

$$A_i = \bigcup_{k=0}^{(L/b_i)-1} (b_i - 1) + kb_i \quad \text{and} \quad S = \bigcup_{i=1}^{r} A_i.$$

Then $S \subset N$ and $|S| = |M|$. But $1 \in (N - S)$ implies $|S| < |N|$ and so $|M| < |N|$.

LEMMA 2. *Let* k *and* p *be integers,* A *and* B *real numbers, such that* $1 \leqslant k < p$ *and* $0 < A < B < 1$. *Then* $A + (1 - A)/p + k(1 - B)/p < 1$.

PROOF. Equivalently, we must show $p^{-1}((p-1)A + 1 + k - kB) < 1$. If we define $\varepsilon = B - A > 0$ this becomes $(p-k-1)A + k(1-\varepsilon) + 1 < p$. But

$$\begin{aligned}(p-k-1)A + k(1-\varepsilon) + 1 &\leqslant p - k - 1 + k - \varepsilon k + 1\\ &= p - \varepsilon k < p.\end{aligned}$$

LEMMA 3. *Let A be a basis consisting of the positive integers $k_1 < \cdots < k_m$ and let $B = A \cup \{p\}$ be another basis where p is a prime which does not divide any k_j. Let $d(I_n^1)_A$ denote this previously defined function on the basis A. Similarly we define $d(I_n^1)_B$, $d(I_n^2)_A$, and $d(I_n^2)_B$. Then*

$$d(I_n^1)_B = d(I_n^1)_A + p^{-1}\left(1 - d(I_n^1)_A\right), \tag{1}$$

$$d(I_n^2)_B = d(I_n^2)_A - (\phi(p)/p)d(I_n^2) = p^{-1}d(I_n^2)_A. \tag{2}$$

PROOF. (1) Regroup terms of $d(I_n^1)_B$, taking first those without p, then those with p. Since p is relatively prime to all k_j, $1/p$ may be factored from each term in the second group to leave a term identical to one in the first group but with opposite signs except for the first term.

(2) Regroup as above. This time $\phi(p)/p$ may be factored from each term in the second group.

LEMMA 4. *Consider again the basis B defined in Lemma 3, let $L = [k_1, k_2, \ldots, p, \ldots, k_m]$ and let P_n be the set generated by B. Then $|P_n|$ is a linear function on the set $r + kL$, $k = 0, 1, 2, \ldots$, for any integer $r \geqslant 0$.*

PROOF. Define

$$\begin{aligned}X(n; a_1, a_2, \ldots, a_N) &= [n/a_1] + \cdots + [n/a_N]\\ &\quad - \left([n/[a_1, a_2]] + \cdots + [n/[a_i, a_j]] + \ldots\right) + \ldots\\ &\quad + [n/[a_i, a_j, a_l]] + \ldots + (-1)^{N+1}[n/[a_1, \ldots, a_N]].\end{aligned}$$

Then

$$|I_n^1| = X(n; k_1, \ldots, p, \ldots, k_m),$$

$$|I_n^j| = X\left(jn; s_1^{(j)}, \ldots, s_{N_j}^{(j)}\right) - X\left((j-1)n; s_1^{(j)}, \ldots, s_{N_j}^{(j)}\right), \quad \text{if } 2 \leqslant j \leqslant k_1,$$

where $s_l^{(j)} | L$ and $(s_l^{(j)}, k_i) \geqslant j$ for every i. Thus

$$\begin{aligned}|P_n| &= \sum_{j=1}^{k_1} |I_n^j| = X(n; k_1, \ldots, p, \ldots, k_m)\\ &\quad + \sum_{j=2}^{k_1} X\left(jn; s_1^{(j)}, \ldots, s_{N_j}^{(j)}\right) - X\left((j-1)n; s_1^{(j)}, \ldots, s_{N_j}^{(j)}\right).\end{aligned}$$

Since every term in this sum is of the form $[jn/a]$, where $a | L$, and

$$[j(r + kL)/a] = [jr/a] + k[jL/a],$$

we have

$$|P_{r+kL}| = |P_r| + k|P_L|.$$

Now we may proceed directly to the

PROOF OF THEOREM 2. Let B denote the basis $k_1 < \cdots < k_i = p < \cdots < k_m$ and let A denote the basis $k_1 < \cdots < k_{i-1} < k_{i+1} < \cdots < k_m$. Remark (4) permits us to take p relatively prime to all other k_j without loss of generality. We wish to find an upper bound for $|P_n|$ when the basis is B.

$$\begin{aligned} n^{-1}|P_n| &= \frac{1}{n}\sum_{j=1}^{k_1} |I_n^j| \\ &\leqslant \left\{ d\left(I_n^1\right)_B + \frac{2^{m-1}}{n} + (k_1 - 1)\left(d\left(I_n^2\right)_B + \frac{k_1 k_2 \cdots k_m}{n} \right) \right\} \\ &= \left\{ d\left(I_n^1\right)_A + p^{-1}\left(1 - d\left(I_n^1\right)_A\right) + (k_1 - 1)(p^{-1}) d\left(I_n^2\right)_A \right\} \\ &\quad + \left(2^{m-1} + (k_1 - 1)k_1 \cdots k_m\right)/n, \quad \text{by Lemma 3.} \end{aligned}$$

By Lemma 1, $d(I_n^1)_A < 1 - d(I_n^2)_A$, and so Lemma 2 implies the last $\{\ \} < 1$. Hence if n is sufficiently large we have $n^{-1}|P_n| < 1$, which proves the first part of the theorem.

Let L denote the l.c.m. of the basis B and define $f(n) = |P_n| - n$. By Lemma 4, $f(n)$ is a linear function for $n = kL$, $k = 0, 1, 2, \ldots$, and, from what we have just shown, $f(n)$ is a nonincreasing linear function on these values of n. Hence $f(L) < 0$. But $f(n + kL) = f(n) + kf(L)$, so that $f(n) < 0$ implies $f(n + kL) < 0$. This proves the second part of the theorem.

REFERENCES

1. R. L. Graham, *Unsolved problem* 5749, Amer. Math. Monthly **77** (1970), 775.

P. Erdös, *Problems and results on combinatorial number theory*, A Survey of Combinatorial Theory, Chap. 12, North-Holland, Amsterdam, 1973. MR **50** #12957.

2. J. Marica and J. Schönheim, *Differences of sets and a problem of Graham*, Canad. Math. Bull. **12** (1969), 635–637. MR **40** #2633.

3. Riko Winterle, *A problem of R. L. Graham in combinatorial number theory*, Proc. Louisiana Conf. on Combinatorics, Graph Theory and Computing (Louisiana State Univ., Baton Rouge, La., 1970), Louisiana State Univ., Baton Rouge, La., 1970, pp. 357–361. MR **42** #3051.

4. W. Y. Vélez, *Some remarks on a number theoretic problem of Graham*, Acta Arith. (to appear).

DEPARTMENT OF MATHEMATICS, CITY COLLEGE, NEW YORK, NEW YORK 10031