COMBINATORICA 6 (1) (1986) 67—71

# THE SOLUTION OF GRAHAM'S GREATEST COMMON DIVISOR PROBLEM

M. SZEGEDY

*Received 2 May 1985*

The following conjecture of R. L. Graham is verified: If $n \geqq n_0$, where $n_0$ is an explicitly computable constant, then for any $n$ distinct positive integers $a_1, a_2, \ldots, a_n$ we have $\max_{i,j} a_i/(a_i, a_j) \geqq n$, and equality holds only in two trivial cases. Here $(a_i, a_j)$ stands for the greatest cnmmon divisor of $a_i$ and $a_j$.

R. L. Graham asked the following question in [2]: *Is it true that if* $a_1, a_2, \ldots, a_n$ *are distinct positive integers, then* $\max_{i,j} \frac{a_i}{(a_i, a_j)} \geqq n$. (Parentheses will denote g. c. d. throughout the paper.)

For a relatively complete history of the problem see [1], pages 78—79.

If $a_1, a_2, \ldots, a_n$ were a counterexample for the conjecture, then each $a_i/a_j$ could be written in the form $s/t$ where $s = a_i/(a_i, a_j)$, $t = a_j/(a_i, a_j)$, and $s, t < n$. So in fact we are interested only in the ratios of the $a_i$, $a_j$ pairs. This idea gives us a second version of Graham's conjecture:

*If we have n distinct positive rational numbers* $r_1, r_2, \ldots, r_n$, *we can choose two of them* $r_i$ *and* $r_j$ *so that* $r_i/r_j = s/t$ *where* $(s, t) = 1$ *and* $s \geqq n$.

From this version immediately follows the fact, that each prime greater than $n-1$ has to be in the same power in each $a_i$ in a counterexample. We can extend this statement to the primes greater than $n/2$:

**Lemma.** *Let* $a_1, a_2, \ldots, a_n$ *be distinct positive integers so that* $p | a_1$, $p \nmid a_n$ *for a prime* $p > n/2$. *Then*

(i) $\max_{i,j} \frac{a_i}{(a_i, a_j)} \geqq n$;

(ii) *if* $\max_{i,j} \frac{a_i}{(a_i, a_j)} = n$ *holds, then either* $\{a_1, \ldots, a_n\} = \{k, 2k, \ldots, nk\}$ *or* $\{a_1, a_2, \ldots, a_n\} = \left\{\frac{k}{1}, \frac{k}{2}, \ldots, \frac{k}{n}\right\}$ *for some integer* $k$, *or* $n = 4$ *and* $\{a_1, a_2, a_3, a_4\} = \{2k, 3k, 4k, 6k\}$.

AMS subject classification (1980): 10 A 05, 10 A 25

**Proof.** $a_1/(a_1, a_n) \geqq p$ gives the result in the case when $p > n$. So we may assume $p \leqq n$. Without loss of generality we may assume also, that $p \mid (a_1, a_2, \ldots, a_s)$ but $p \nmid a_{s+1} \cdot \ldots \cdot a_n$. We are done again if for some $1 \leqq i \leqq s$, $s+1 \leqq j \leqq n$ $a_i/p \nmid a_j$ since then

$$\frac{a_i}{(a_i, a_j)} = p \frac{\frac{a_i}{p}}{\left(\frac{a_i}{p}, a_j\right)} \geqq 2p > n.$$

Otherwise we obtain the following divisibility relation, where brackets denote l. c. m.

$$B = [b_1, b_2, \ldots, b_s] \mid A = (a_{s+1}, \ldots, a_n), \quad \text{where} \quad b_i = a_i/p \quad (1 \leqq i \leqq s).$$

For $\dfrac{B}{b_k} = \max\limits_{1 \leqq i \leqq s} \dfrac{B}{b_i}$ we have $\dfrac{B}{b_k} \geqq s$, since $b_i \neq b_j$ whenever $i \neq j$. For $\dfrac{a_t}{A} = \max\limits_{s+1 \leqq j \leqq n} \dfrac{a_j}{A}$ we have $\dfrac{a_t}{A} \geqq n-s$ since $a_i \neq a_j$ if $i \neq j$.

Now

$$\frac{a_t}{(a_t, a_k)} = \frac{a_t}{(a_t, b_k)} = \frac{a_t}{b_k} = \frac{a_t}{A} \frac{B}{b_k} \frac{A}{B} \geqq s(n-s) \frac{A}{B}.$$

We are done if the right hand side is greater than $n$. Consider the cases when

$$s(n-s) \frac{A}{B} \leqq n.$$

*1.* $s=1$, $n-s=n-1$, $A=B$. In this case $\{a_2, a_3, \ldots, a_{n-1}\} = \{A, 2A, \ldots, nA\} \setminus \{pA\}$, $a_1 = pB = pA$ so we get a system described in (ii).

*2.* $s=n-1$, $n-s=1$, $A=B$. Now $a_n = A = B$, $\{a_1, \ldots, a_{n-1}\} = \left\{\dfrac{Bp}{1}, \dfrac{Bp}{2}, \ldots, \dfrac{Bp}{n}\right\} \setminus \{B\}$, so we get the other type of system described in (ii).

*3.* $n=4$, $s=n-s=2$, $A=B$ will give the third possible system in (ii). ∎

Now our main idea will be presented in

**Theorem 1.** *If the interval $[2n-\sqrt{n}+1, 2n]$ contains a prime $p$ then an arbitrary system $a_1, a_2, \ldots, a_n$ of distinct positive integers contains two elements $a_i$ and $a_j$ such that $a_i/(a_i, a_j) \geqq n$.*

**Proof.** We may assume that $(a_1, a_2, \ldots, a_n) = 1$. If for some $i$ we have $p \mid a_i$, we are done by Lemma 1.

We are finished also if $a_i \equiv a_j \pmod{p}$ for some $a_i > a_j$, since then $a_i/(a_i, a_j) \geqq \geqq a_i((a_i - a_j)/p)^{-1} > p > n$. These facts mean that considering the set $a_1, a_2, \ldots, a_n$, $-a_1, -a_2, \ldots, -a_n \pmod{p}$ we may assume that each residue class contains at most two of these elements.

If a class contains two elements, they are $a_i$ and $-a_j$ where $i \neq j$. We can divide the congruence $a_i \equiv -a_j (p)$ by $(a_i, a_j)$ $((a_i, p) = 1)$, and we get $a_i' \equiv -a_j' \pmod{p}$ where $a_i' = a_i/(a_i, a_j)$, $a_j' = a_j/(a_i, a_j)$.

Define a function $\varphi$ on the congruent pairs $\langle a_i, -a_j\rangle$ by $\varphi\langle a_i, -a_j\rangle = a_i/(a_i, a_j) = a_i'$. If $a_i'$ or $a_j'$ is greater than or equal to $n$, we are done. If $a_i' < n$, $a_j' < n$, then from the congruence $a_i' \equiv -a_j' \pmod p$ we get $p-n < a_i' < n$, $p-n < a_j' < n$. In this case the image of $\varphi$ is contained in the set $\{p-n+1, \ldots, n-1\}$, which has $2n-p-1$ elements.

Since the number of congruent pairs is at least $2n-(p-1) = 2n-p+1$, there are at least two congruent pairs $\langle a_i, a_j\rangle$ and $\langle a_k, a_t\rangle$ such that $\varphi\langle a_i, -a_j\rangle = \varphi\langle a_k, -a_t\rangle = \vartheta$. We have the equalities

$$\frac{a_i}{a_j} = \frac{a_i'}{a_j'} = \frac{\vartheta}{p-\vartheta} \quad \text{and} \quad \frac{a_k}{a_t} = \frac{a_k'}{a_t'} = \frac{\vartheta}{p-\vartheta}.$$

Let us define the positive integers $X$, $Y$, $X'$ and $Y'$ by $XY^{-1} = a_t a_i^{-1}$ where $(X, Y) = 1$ and $X'Y'^{-1} = a_k a_j^{-1}$ where $(X', Y') = 1$. From the second version of the conjecture we are done if $\max(X, X', Y, Y') \geqq n$. Otherwise consider the equality

$$\frac{X'}{Y'} = \frac{X}{Y}\frac{\vartheta^2}{(p-\vartheta)^2}, \quad \text{obtained from} \quad \frac{a_k}{a_j} = \frac{a_k}{a_t}\frac{a_t}{a_i}\frac{a_i}{a_j}.$$

Here $\vartheta^2 = a_i'^2 > (p-n)^2 \geqq (n-\sqrt{n}+1)^2 > n^2/2$ and

$$n > X' = \frac{X}{(X, (p-\vartheta)^2)}\frac{\vartheta^2}{(\vartheta^2, Y)} \quad \text{imply} \quad \frac{X}{(X, (p-\vartheta)^2)}\frac{1}{(\vartheta^2, Y)} < \frac{2}{n}$$

so $X|(p-\vartheta)^2$, $Y|\vartheta^2$, i.e. $XY' = (p-\vartheta)^2$, $YX' = \vartheta^2$. Define $\lambda$ and $\mu$ by $\lambda/\mu = \vartheta/Y$, $(\lambda, \mu) = 1$. Clearly $\lambda|\vartheta$. But from $Y|\vartheta^2$ we have that $\vartheta^2/Y = \vartheta(Y/\vartheta)^{-1} = \vartheta(\mu/\lambda)^{-1} = \vartheta\lambda/\mu$ is an integer, $(\mu, \lambda) = 1$, so $\mu|\vartheta$. This means that $\vartheta$ can be written in the form $\vartheta = \vartheta_1\lambda\mu$, hence $\min(\lambda, \mu) < \sqrt{n}$. We also have the inequality, $Y = \vartheta^2/X' \geqq \vartheta^2/n$. Now we distinguish three cases:

*1.* $Y > \vartheta$. In this case, using $\mu > \lambda$, $\lambda < \sqrt{n}$, $\vartheta > n-\sqrt{n}+1$, and $Y < n$ we obtain

$$\frac{1}{\sqrt{n}} < \frac{\mu-\lambda}{\lambda} = \frac{Y-\vartheta}{\vartheta} < \frac{\sqrt{n}-1}{n-\sqrt{n}} = \frac{1}{\sqrt{n}},$$

which is a contradiction.

*2.* $\vartheta > Y$. Now $\lambda > \mu$, $\mu < \sqrt{n}$, $Y > \vartheta^2/n$ and $\vartheta > n-\sqrt{n}+1$, imply

$$\frac{1}{\sqrt{n}} < \frac{\lambda-\mu}{\mu} = \frac{\vartheta-Y}{Y} < \frac{\vartheta-(\vartheta^2/n)}{\vartheta^2/n} = \frac{n-\vartheta}{\vartheta} < \frac{\sqrt{n}-1}{n-\sqrt{n}} = \frac{1}{\sqrt{n}},$$

which is a contradiction again.

*3.* We can argue similarly using $p-\vartheta$ and $X$ instead of $\vartheta$ and $Y$. So the only case left is $Y = \vartheta$ and $X = p-\vartheta$. From these two facts we obtain

$$\frac{a_t}{a_j} = \frac{a_i}{a_j}\frac{a_t}{a_i} = \frac{\vartheta}{p-\vartheta}\frac{X}{Y} = 1,$$

but this is impossible because $a_t \neq a_j$.

The idea of the following extension is due to E. Szemerédi:

**Theorem 2.** *There exists an effectively computable $n_0$ with the following properties:*

(i) *If $n \geqq n_0$ and $a_1, a_2, \ldots, a_n$ are distinct natural numbers then* $\max_{i,j} \frac{a_i}{(a_i, a_j)} \geqq \geqq n$.

(ii) *If equality holds then the system $\{a_1, a_2, \ldots, a_n\}$ is either of the type $\{k, 2k, \ldots, nk\}$ or of the type $\left\{\frac{k}{1}, \frac{k}{2}, \ldots, \frac{k}{n}\right\}$ for some $k$.*

**Proof of Theorem 2.** If $n$ is large enough then the interval $[2n-n^{1/2+1/7}, 2n-1/2\,n^{1/2+1/7}]$ contains a prime $p$ by Ingham's theorem. Just as in the proof of Theorem 1, we may assume $p \nmid a_i$ and $a_i \not\equiv a_j \pmod p$. Using the notations of Theorem 1, define $\alpha(\vartheta) = \left|\{\langle a_i, -a_j\rangle | \varphi\langle a_i, -a_j\rangle = \vartheta\}\right|$. Clearly

$$2n-p+1 \leqq \text{the number of congruent pairs} = \sum_{\vartheta} \alpha(\vartheta) =$$

$$= \sum_{\alpha(\vartheta)=1} 1 + \sum_{\alpha(\vartheta)>1} \alpha(\vartheta) = \Sigma_1 + \Sigma_2.$$

We shall give an upper bound for $\Sigma_2$. Clearly

$$\Sigma_2 \leqq \left(\max_{\vartheta} \alpha(\vartheta)\right) \sum_{\alpha(\vartheta)>1} 1 = AB.$$

From $Y|\vartheta^2$, $X|(p-\vartheta)^2$ we get that $A \leqq d(\vartheta^2)d((p-\vartheta)^2) = O(n^{\varepsilon})$ for arbitrary $\varepsilon>0$. To give an upper bound for $B$ we have to enumerate all values of $\vartheta$ for which either $Y$ may be different from $\vartheta$ or $X$ may be different from $p-\vartheta$. If $Y$ is different from $\vartheta$, $\vartheta$ can be written in the form $\vartheta = \vartheta_1\lambda\mu$ where $Y = \vartheta_1\mu^2 > \vartheta^2/n$. Similarly to Cases 1 and 2 in the proof of Theorem 1 we obtain now

$$\frac{1}{\lambda} \leqq \left|\frac{\lambda-\mu}{\lambda}\right| = \left|\frac{\vartheta - Y}{\vartheta}\right| \leqq \frac{2}{n^{1/2-1/7}},$$

hence $\lambda \geqq n^{1/2-1/7}/2$.

Since both $Y$ and $\vartheta$ are in the interval $[n-2n^{1/2+1/7}, n]$, and $Y/\vartheta = \mu/\lambda$ we obtain $\mu = \lambda Y/\vartheta \geqq n^{1/2-1/7}/4$. But then $\vartheta_1 = \vartheta(\lambda\mu)^{-1}$ implies

$$\vartheta_1 < 8n^{2/7}.$$

Define $K = \sqrt{n/\vartheta_1} - \mu$, $L = \sqrt{n/\vartheta_1} - \lambda$. From $n - n^{1/2+1/7} \leqq \vartheta = \vartheta_1\left(\sqrt{n/\vartheta_1} - K\right) \times \times \left(\sqrt{n/\vartheta_1} - L\right) = n - \sqrt{n\vartheta_1}(K+L) + KL\vartheta_1$ we get that $K+L = O(n^{1/7})$. From $n - O(n^{1/2+1/7}) < Y = \vartheta_1\left(\sqrt{n/\vartheta_1} - K\right)\left(\sqrt{n/\vartheta_1} - K\right) = n - \sqrt{n\vartheta_1}(2K) + K^2\vartheta_1$ we get that $2K = O(n^{1/7})$. Since $\vartheta$ is uniquely determined by $\vartheta_1$, $K+L$ and $2K$ we get that the number of possible choices of $\vartheta$ is at most $O(n^{2/7})O(n^{1/7})O(n^{1/7}) = O(n^{4/7})$. We have the same result for the number of possible values of $p-\vartheta$, as well. Thus we have an upper bound $\Sigma_2 \leqq AB = O(n^{\varepsilon}\, n^{4/7})$ for arbitrary $\varepsilon$ and hence

$$\Sigma_1 \geqq 2n-p+1-\Sigma_2 \geqq 2n-p+1-O(n^{4/7+1/15}).$$

Since we know (see [3]), that in the interval $[n-1/2n^{1/2+1/7}, n] \subseteqq [p-n, n]$ the number of primes is $\geqq cn^{1/2+1/7}/\log n$ for some positive constant $c$, we see that the set $\{\vartheta | p-n \leqq \vartheta \leqq n,\ \vartheta \text{ is not a prime}\}$ has at most $2n-p+1-cn^{1/2+1/7}/\log n$ elements.

Since $\Sigma_1$ is greater than this value (for $n > n_0$) we obtain, that there is a congruent pair $\langle a_i, -a_j\rangle$ so that $\varphi\langle a_i, -a_j\rangle$ is a prime $\pi > p-n > n/2$ and considering $a_i/(a_i, a_j) = \pi$ we are done by the Lemma. (To obtain (ii) we made use also of the fact, that $n$ can be replaced by $n+1$ in some of the arguments taken from the proof of Theorem 1.)

**Acknowledgements.** The author would like to express his thanks to E. Szemerédi for contributing a key idea to the proof of Theorem 2.

## References

[1] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Genève, 1980.

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

[3] D. R. Heat-Brown and H. Iwaniec, On the difference between consecutive primes, *Invent. Math.* **55** (1979), 49—69.

M. Szegedy

*Department of Algebra and Number Theory*
*Institute of Mathematics, L. Eötvös University*
*Budapest, 1088, Hungary*

*Current address:*

*Department of Computer Science*
*University of Chicago*
*1100 E 58th St.*
*Chicago, IL 60637, U.S.A.*