Цитированная литература

[1] E. Hecke, *Über Dirichlet-Reihen mit Funktionalgleichung und ihre Nullstellen auf der Mittelgeraden*, Mathematische Werke, Zweite Auflage, Göttingen, 1970, стр. 708–730.

[2] — *Analytische Arithmetik der positiven quadratischen Formen*, ibid., стр. 789–918.

[3] B. W. Jones and G. Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. 70 (1938), стр. 165–191.

[4] H. D. Kloosterman, *The behaviour of general theta-functions under the modular group and the characters of binary modular congruence groups. I*, Ann. of Math. 47 (1946), стр. 317–375.

[5] Л. А. Коган, *О представлении чисел некоторыми квадратичными формами с тремя переменными*, Известия Академии Наук Узбекской ССР, серия физ.-мат. наук, 4 (1963), стр. 13–22.

[6] — *О представлении чисел некоторыми тернарными квадратичными формами*, Ученые записки Ташкентского педагогического института 61 (1966), стр. 10–19.

[7] Г. А. Ломадзе, *О числе представлений чисел формами* $x^2+3y^2+36z^2$ *и* $x^2+12y^2+36z^2$, Сообщения Академии Наук Грузинской ССР 51 (1968), стр. 25–30.

[8] — *О числе представлений чисел квадратичными формами с четырьмя переменными*, Труды Тбилисского математического института им. А. М. Размадзе 40 (1971), стр. 106–139.

[9] — *О представлении чисел положительными тернарными диагональными квадратичными формами*, Acta Arith. 19 (1971), стр. 267–305; 387–407.

[10] G. Pall, *Representation by quadratic forms*, Canad. Journ. Math. 1 (1949), стр. 344–364.

Поступило 21. 5. 1976 (851

ACTA ARITHMETICA
XXXIV (1978)

On a problem of R. L. Graham

by

R. D. Boyle (Heslington)

0. Introduction. Let S be a set of distinct positive integers

$$S = \{a_1, a_2, \ldots, a_n\} \quad \text{where} \quad a_1 < a_2 < \ldots < a_n.$$

Then Graham [1] has made the following:

Conjecture.

$$\max_{1\leqslant i,j\leqslant n} \frac{a_i}{(a_i, a_j)} \geqslant n \quad \text{for any } S, \text{ any } n \geqslant 2.$$

Supposing the conjecture false, we will call any counter example a *good set for n*. If S is good for n, it has been shown that:

(1) Not all the a_i are square free (Marica and Schönheim [2]).

(2) a_1 is not a prime (Winterle [3]).

(3) n is not a prime (Szemerédi [1]).

(4) $n-1$ is not a prime (Vélez [4]).

(5) If $p \mid a_i$ for some i, and p is prime, $p \leqslant n$ (Vélez [4]).

Vélez also considers in [4] the nature of sets with maximum ratio equal to n.

In this paper we shall show:

Theorem 1. *If S is good for n, p is a prime, and $p \mid a_i$ for some i, then*

$$p \leqslant (n-1)/2. \tag{6}$$

An immediate corollary to this theorem is Vélez' result that $n-1$ is not a prime; it further enables us to show that $n-2$ and $n-3$ must be composite also.

Theorem 2. *If p is a prime, and S is good for n, where*

$$n = qp+t, \quad 1 \leqslant t \leqslant p, \tag{7}$$

$$p \mid a_i \quad \textit{for some } i, \tag{8}$$

$$n \textit{ is sufficiently large depending on } q, \tag{9}$$

then

$$p \leqslant (n-1)/3 \quad (\text{i.e. } q \geqslant 3). \tag{10}$$

If $(n-1)/4 < p \leqslant (n-1)/3$, *so* $q = 3$, *then*

$$S = \{6p\} \cup M \tag{11}$$

for some M, *where* $m \in M$ *implies* $m \not\equiv 0 \pmod p$. *If* $q \geqslant 4$ *and we define*

(12) $Q = [1, 2, \ldots, q]$, *the l.c.m. of the first* q *natural numbers*

and

$$\psi(q) = \sum_{r|Q} \frac{r^2 \varphi(Q/r)}{Q} \tag{13}$$

then either

(14) *there are* $< (2\psi+1)/2$ *multiples of* p *in* S

or

(15) *there are* $> n-(2\psi+1)/2$ *multiples of* p *in* S.

Further, if (14) *holds, then*

$$(a_i, Q) \geqslant 2 \quad \text{when} \quad p \mid a_i. \tag{16}$$

THEOREM 3. *If* $n = p^a$ *for* p *prime,* $a \geqslant 2$, *and* S *is good for* n, *then*

$$S = (p^{a-1}K_{a-1}) \cup (p^{a-2}K_{a-2}) \cup \ldots \cup (pK_1) \cup (K_0) \tag{17}$$

where the (not necessarily non-empty) sets K_i *are such that*

$$k \in K_i \Rightarrow k \not\equiv 0 \pmod p,$$
$$k, l \in K_i \Rightarrow k \not\equiv l \pmod{p^a},$$
$$k \in K_i,\ l \in K_j,\ k \equiv l \pmod{p^a} \Rightarrow k = l.$$

As a corollary to Theorem 3, we can deduce that there are no good S for $n = p^2$, p any prime.

1. Preliminaries. Throughout, the letters $S, S^{-1}, K, K_1, K_2, \ldots, L, M$ will denote sets of positive integers; all other letters will denote non-negative integers.

Let $s^* = \text{l.c.m.}[a_1, \ldots, a_n]$, and then define

$$S^{-1} = \left\{\frac{s^*}{a_n}, \ldots, \frac{s^*}{a_1}\right\}.$$

LEMMA 1. *The ratios of* S^{-1} *coincide with those of* S, *and so*

$$S \text{ is good for } n \Leftrightarrow S^{-1} \text{ is good for } n.$$

Proof. This result is due to Winterle in [3].

We will assume throughout that

$$\text{h.c.f.}(a_1, \ldots, a_n) = 1 \tag{18}$$

which is obviously no restriction.

LEMMA 2. *Suppose the conjecture is true for* $n-1$, *and that* S *is good for* n. *Then there are at least 2 multiples of* $n-1$ *in* S.

Proof. Since S is good for n,

$$\frac{a_i}{(a_i, a_j)} \leqslant n-1, \quad 1 \leqslant i, j \leqslant n$$

and equality gives $(n-1) \mid a_i$. Suppose there are no multiples of $n-1$ in S. Then

$$\frac{a_i}{(a_i, a_j)} \leqslant n-2, \quad 1 \leqslant i, j \leqslant n$$

and so $S \setminus \{a_i\}$ is good for $n-1$, for any $a_i \in S$, a contradiction.

Now suppose there is just one multiple of $n-1$ in S, a_r say. Then

$$\frac{a_r}{(a_r, a_i)} \leqslant n-1, \quad 1 \leqslant i \leqslant n$$

and

$$\frac{a_i}{(a_i, a_j)} \leqslant n-2, \quad i \neq r, \quad 1 \leqslant i, j \leqslant n.$$

Hence $S \setminus \{a_r\}$ is good for $n-1$, a contradiction.

LEMMA 3. *Let* $K = \{k_1, k_2, \ldots, k_a\}$, *where the* k_i *are in ascending order. Suppose there is a* t *such that*

$$(k_i, t) = 1, \quad 1 \leqslant i \leqslant a.$$

Then if $k^* = \text{l.c.m.}[k_1, \ldots, k_a]$, *we have*

$$\frac{k^*}{k_1} > t\left(\frac{a}{\varphi(t)} - 1\right). \tag{19}$$

Proof. It is easy to see that $(k^*, t) = 1$. Also

$$k_i = \frac{k^*}{q_i} \quad \text{for some } q_i, \quad i = 1, \ldots, a.$$

We have $1 \leqslant q_a < q_{a-1} < \ldots < q_1$ and

$$(q_i, t) = 1, \quad 1 \leqslant i \leqslant a.$$

Suppose $a = \lambda\varphi(t) + \mu$, $1 \leqslant \mu \leqslant \varphi(t)$.

Now in any block of t consecutive integers, there can be at most $\varphi(t)$ q's. Hence

$$q_1 \geqslant \lambda t + \mu > \lambda t \geqslant \left(\frac{a}{\varphi(t)} - 1\right)t.$$

Note that $t = 1$ always satisfies the requirements of the lemma, whence

(20) $$\frac{k^*}{k_1} = q_1 > a-1 \Rightarrow \frac{k^*}{k_1} \geqslant a.$$

2. Proof of Theorem 1. Suppose S is good for n, and

$$S = (pK) \cup L, \quad \text{where} \quad l \in L \Rightarrow l \not\equiv 0 \ (\mathrm{mod}\ p).$$

We suppose $K \neq \emptyset$, whence (18) gives $L \neq \emptyset$. We also suppose (6) does not hold, so $\left[\frac{n-1}{p}\right] = 1$ by (3) and (5). Let $k \in K$, $l \in L$; then

$$\frac{kp}{(kp, l)} = \frac{k}{(k, l)} p \leqslant n-1 < 2p \Rightarrow \frac{k}{(k, l)} < 2 \Rightarrow k \mid l \quad \forall k \in K, \ \forall l \in L.$$

So if k^* is the l.c.m. of the elements of K, we have

$$S = (pK) \cup (k^* M) \quad \text{for some } M.$$

Let $|K| = c$; then $|M| = |L| = n-c$.
Let $m_1 = \max(m \in M)$, so $m_1 \geqslant n-c$.
Let $k_0 = \min(k \in K)$; then $k^* \geqslant ck_0$ by (20).
Now we know that

$$\frac{m_1 k^*}{(m_1 k^*, k_0 p)} \leqslant n-1$$

and so

$$\frac{m_1 k^*}{k_0} \leqslant n-1$$
$$\Rightarrow (n-c)c \leqslant n-1$$
$$\Rightarrow c^2 - nc + n - 1 \geqslant 0$$
$$\Rightarrow c \leqslant 1 \text{ or } c \geqslant n-1.$$

Hence $c = 1$ or $c = n-1$. By Lemma 1, if S is good for n with $c = n-1$, then S^{-1} is good for n with $c = 1$, so it suffices to show that $c = 1$ is impossible. Hence suppose $c = 1$; i.e. $K = \{k_0\}$, $k^* = k_0$. Then $k_0 \mid a_i$ for each i, so from (18) $k_0 = 1$ and $pK = \{p\}$. Also $m_1 \geqslant n$ since $|M| = n-1$, $p \leqslant n-1$ and we cannot have $p \in M$. Then

$$\frac{m_1}{(m_1, p)} = m_1 \geqslant n$$

a contradiction, so $c = 1$ is impossible.

Corollary 1. *The conjecture is true for $n = p+1$, p any prime.*

Proof. We know from [1] that it is true for p, so by Lemma 2, any S that is good for $p+1$ must have at least 2 multiples of p in it, whence $n = p+1$ contradicts (6).

Corollary 2. *The conjecture is true for $n = p+2$, p any prime.*

Proof. Suppose S is good for $p+2$. By Theorem 1 there are no multiples of p in S (provided $n-2 > (n-1)/2$, which is implied by $p \geqslant 3$) so we must have 3 distinct elements $a_i, a_j, a_k \in S$ with $i > j > k$ and $a_i \equiv a_j \ (\mathrm{mod}\ p)$; $a_i = a_j + rp$, say, for some $r > 0$. Then

$$\frac{a_i}{(a_i, a_j)} = \frac{a_j + rp}{(a_j + rp, a_j)} = \frac{a_j}{(r, a_j)} + \frac{r}{(r, a_j)} p$$
$$\leqslant p+1 \quad \text{as } S \text{ is good for } p+2.$$

Hence $r = a_j$, so $a_i = a_j(p+1)$. Then

$$\frac{a_i}{(a_i, a_k)} \geqslant \frac{a_i}{a_k} = \frac{a_j}{a_k}(p+1) > p+1$$

which provides a contradiction.

Corollary 3. *The conjecture is true for $n = p+3$, p any prime.*

Proof. Suppose S is good for $n = p+3$. We may take $n \geqslant 6$, so $n-3 > (n-1)/2$, and hence there are no multiples of p in S. We consider possible congruent pairs $(\mathrm{mod}\ p)$ in S. Suppose

$$a_i \equiv a_j \ (\mathrm{mod}\ p),$$
$$a_i = a_j + rp, \quad r > 0, \quad \text{say}.$$

Then

$$\frac{a_i}{(a_i, a_j)} = \frac{a_j}{(a_j, r)} + \frac{r}{(a_j, r)} p \leqslant p+2.$$

So $r \mid a_j$, and either $a_j = r$ or $a_j = 2r$. Thus either

(21) $$a_i = a_j(p+1) \quad \text{or} \quad a_i = \frac{a_j}{2}(p+2).$$

We see now that there cannot be as many as 3 elements of S in one residue class, for if there were, then by (21) they would be of the form

$$a_r,\ \frac{a_r}{2}(p+2),\ a_r(p+1)\quad \text{for some } a_r \in S.$$

But then, writing $a_j = \frac{a_r}{2}(p+2)$ and $a_i = a_r(p+1)$, (21) would not be satisfied.

Case A. Suppose we have $a_i, a_j, a_k, a_l \in S$, $j > l$ and

$$a_i = a_j(p+1),\quad a_k = a_l(p+1).$$

Then

$$\frac{a_i}{(a_i, a_l)} \geqslant \frac{a_i}{a_l} = \frac{a_j}{a_l}(p+1) > p+1.$$

Hence

$$\frac{a_i}{(a_i, a_l)} = p+2 \quad \text{as } S \text{ is good for } p+3.$$

Thus

$$a_j = \frac{p+2}{p+1}a_l.$$

So there are at most 2 congruent pairs of this type, and if there were 2 such, we would have

$$a_l,\ \frac{p+2}{p+1}a_l,\ (p+1)a_l,\ (p+2)a_l \in S.$$

But then

$$\frac{(p+1)a_l}{\left((p+1)a_l, \left(\frac{p+2}{p+1}\right)a_l\right)} = \frac{(p+1)^2}{((p+1)^2, p+2)} = (p+1)^2 > p+2.$$

Hence we see that there is at most one pair of the first type at (21).

Case B. Suppose we have $a_s, a_t, a_u, a_v \in S$, $t > v$ and

$$a_s = \frac{a_t}{2}(p+2),\quad a_u = \frac{a_v}{2}(p+2).$$

Let $d = (a_s, a_v)$, and so

$$\frac{a_s}{(a_s, a_v)} = \frac{a_t}{2d}(p+2) \leqslant p+2 \quad \text{as } S \text{ is good for } p+3.$$

Thus

$$d \geqslant \frac{a_t}{2} > \frac{a_v}{2} \Rightarrow d = a_v,\quad \text{since}\quad d \mid a_v.$$

Hence

$$(22)\qquad 2a_v \geqslant a_t.$$

Now suppose $2^x \| a_v$; i.e. $a_v = 2^x a_v'$, with a_v' odd. Then $2^{x+1} \mid a_t$ since $a_v \left| \frac{a_t}{2}(p+2)\right.$, and $p+2$ is odd. This gives

$$(23)\qquad d' = \left(\frac{a_v}{2}(p+2), a_t\right) \leqslant \frac{a_t}{4}.$$

Now

$$\frac{a_u}{(a_u, a_t)} = \frac{a_u}{d'} = \frac{a_v}{2d'}(p+2) \leqslant p+2 \quad \text{as } S \text{ is good for } p+3.$$

Thus $d' \geqslant a_v/2$, and so by (23)

$$(24)\qquad \frac{a_v}{2} \leqslant \frac{a_t}{4}.$$

(24) and (22) now give

$$a_t = 2a_v,$$

so we see that there are at most 2 congruent pairs of this type, and if there were 2 such, we would have

$$a_v,\ 2a_v,\ \frac{a_v}{2}(p+2),\ a_v(p+2) \in S.$$

Now there are $p+3$ numbers in S, which occupy $p-1$ residue classes. Thus either one residue class contains at least 3 elements of S, or at least 4 residue classes contain 2 or more elements of S. The argument after (21) rules out the first possibility, and the conclusions of cases A and B do not allow the second. Hence we cannot find an S that is good for $n = p+3$.

Unfortunately it does not seem immediately possible to extend the above ideas to $n = p+h$, $h \geqslant 4$. Obviously, if this could be done for general $h < p$, Bertrand's postulate would then prove the conjecture.

3. Proof of Theorem 2. We suppose that S is good for $n = qp+t$, $1 \leqslant t \leqslant p$, and

$$S = (pK) \cup L$$

where $K \neq \emptyset$, $L \neq \emptyset$ and $l \in L \Rightarrow l \not\equiv 0 \pmod p$. Q and $\psi(q)$ are as at (12) and (13), and we define

$$n_1(q) = q^2+q+1, \quad \text{so} \quad n \geqslant n_1(q) \Rightarrow p > q,$$
$$n_2(q) = 2\big(\psi(q)\big)^2+2Q\psi(q)+Q+1,$$

$n_3(q)$ is such that

$$n \geqslant n_3(q) \Rightarrow \pi(n)-\pi\left(\frac{n-1}{2}\right)+q \geqslant \frac{2\psi(q)+1}{2}.$$

Then by "sufficiently large depending on q" we shall mean

$$n \geqslant \max\big(n_1(q), n_2(q), n_3(q)\big).$$

Suppose $k \in K$ and $l \in L$; then

$$\frac{kp}{(kp, l)} \leqslant n-1$$

so

$$\frac{k}{(k, l)}p \leqslant qp \Rightarrow \frac{k}{(k, l)} \leqslant q. \tag{25}$$

Let $(k, Q) = y$ and $(k, l) = z$; then

$$\frac{k}{z} \leqslant q \quad \text{by} \quad (25),$$

so

$$\frac{k}{z}\Big| Q \Rightarrow \frac{k}{z}\Big| y \Rightarrow \frac{k}{y}\Big| z \Rightarrow \frac{k}{y}\Big| l. \tag{26}$$

Now for each $r|Q$ we define the (possibly empty) set K_r by

$$K_r = \left\{\frac{k}{r}:\ k \in K, (k, Q) = r\right\}.$$

Also, put

$$k_r^* = \begin{cases} \text{l.c.m.}\left[\dfrac{k}{r} \in K_r\right] & \text{if} \quad K_r \neq \emptyset, \\ 1 & \text{if} \quad K_r = \emptyset \end{cases}$$

and

$$k^* = \text{l.c.m.}\,[k_1^*, \ldots, k_Q^*].$$

Then (26) tells us that $k^*|l$ for each $l \in L$, and so we have

$$S = (pK) \cup (k^*M) \quad \text{for some } M.$$

Let $|K| = c$; then $|L| = |M| = n-c$;
Let $m_1 = \max(m \in M)$, so $m_1 \geqslant n-c$;
Let $k_r^{(0)} = \min(k \in K_r)$.
Now $k \in K_r$ implies $(k, Q/r) = 1$, and so by Lemma 3,

$$\frac{k^*}{k_r^{(0)}} \geqslant \frac{k_r^*}{k_r^{(0)}} > \frac{Q}{r}\left(\frac{|K_r|}{\varphi(Q/r)}-1\right).$$

We know that S is good for n, and so

$$\frac{m_1 k^*}{(m_1 k^*, rk_r^{(0)}p)} \leqslant n-1 \quad (\text{when } K_r \neq \emptyset)$$
$$\Rightarrow \frac{m_1 \dfrac{k^*}{k_r^{(0)}}}{\left(m_1 \dfrac{k^*}{k_r^{(0)}}, r\right)} \leqslant n-1$$
$$\Rightarrow \frac{m_1 k^*}{rk_r^{(0)}} \leqslant n-1$$
$$\Rightarrow \frac{(n-c)\dfrac{Q}{r}\left(\dfrac{|K_r|}{\varphi(Q/r)}-1\right)}{r} < n-1$$
$$\Rightarrow |K_r| < \varphi\left(\frac{Q}{r}\right)\left[\frac{(r^2+Q)n-(r^2+cQ)}{Q(n-c)}\right].$$

Now clearly

$$\sum_{r|Q} |K_r| = c,$$

hence

$$c < \sum_{r|Q} \varphi\left(\frac{Q}{r}\right)\left[\frac{(r^2+Q)n-(r^2+cQ)}{Q(n-c)}\right] \tag{27}$$
$$\Rightarrow nc-c^2 < (n-c)\sum_{r|Q}\varphi\left(\frac{Q}{r}\right)+(n-1)\sum_{r|Q}\frac{r^2\varphi(Q/r)}{Q}$$
$$\Rightarrow nc-c^2 < (n-c)Q+(n-1)\psi(q)$$
$$\Rightarrow c^2-c(n+Q)+n\big(Q+\psi(q)\big)-\psi(q) > 0.$$

Note that $n \geqslant n_2(q)$ implies

$$(n+Q)^2-4\big(n(Q+\psi(q))-\psi(q)\big) \geqslant \big(n-(Q+2\psi(q)+1)\big)^2$$

and so $n \geqslant n_2(q)$ must imply

$$c < Q+\psi(q)+\frac{1}{2} < \frac{n}{2} \quad \text{or}$$

(28)

$$c > n-\left(\frac{2\psi(q)+1}{2}\right) > \frac{n}{2}$$

by locating the roots of the expression on the left-hand side of (27). Suppose

$$\frac{2\psi(q)+1}{2} \leqslant c < Q+\frac{2\psi(q)+1}{2},$$

then S^{-1} would contain $c' = n-c$ multiples of p, and c' could not satisfy either of the inequalities at (28). Hence we see

(29(i)) $$c < \frac{2\psi(q)+1}{2} \quad \text{or}$$

(29(ii)) $$c > n-\frac{2\psi(q)+1}{2}.$$

This proves (14) and (15).

Now $|M| = n-c$; also $m \in M$ implies $m \not\equiv 0 \pmod{p}$, and, by Theorem 1, $m \in M$ implies $m \not\equiv 0 \pmod{p'}$ where p' is any prime greater than $(n-1)/2$. Hence we see that

$$n \geqslant n_3(q) \Rightarrow m_1 \geqslant n \quad \text{if} \quad c < \big(2\psi(q)+1\big)/2.$$

Now suppose $K_r \neq \emptyset$, $k_r \in K_r$. Then

$$\frac{m_1 k^*}{(m_1 k^*, rk_r p)} \leqslant (n-1) \Rightarrow \frac{nk^*}{rk_r} \leqslant n-1 \Rightarrow \frac{k^*}{k_r} \leqslant r-1$$

(30) $$\Rightarrow |K_r| \leqslant r-1 \quad \text{by} \quad (20).$$

Hence $|K_1| = 0$, so $K_1 = \emptyset$, and (16) is proved. Note that $|K_r| \leqslant r-1$ gives

(31) $$c \leqslant \sum_{r|Q} (r-1)$$

$$\Rightarrow \begin{cases} c \leqslant \sigma(Q)-d(Q) & \text{if (29(i)) holds or} \\ c \geqslant n-\big(\sigma(Q)-d(Q)\big) & \text{if (29(ii)) holds} \end{cases}$$

by considering S^{-1} in the latter case.

To prove (10) we need to show $q = 2$ is impossible. If $q = 2$ then $Q = 2$, $\psi(2) = \frac{5}{2}$, so

$$n_1(2) = 7, \quad n_2(2) = \frac{51}{2}, \quad n_3(2) = 2.$$

Thus the result will be valid for all $n \geqslant 26$. We suppose that

$$S = (pK) \cup (k^* M)$$

is good for $n = 2p+t$ $(1 \leqslant t \leqslant p)$, so

$$K = K_1 \cup (2K_2).$$

By (31), we see that, if $n \geqslant 26$, $|K| = 1$ or $n-1$; as in Theorem 1 it is sufficient to show $|K| = 1$ is impossible. In this case, by (16), we know $K_1 = \emptyset$, and so $K = \{2k\}$ for some number k, and $k^* = k$. By (18), we must have $k = 1$, and

$$S = \{2p\} \cup M.$$

Clearly $1 \notin S$, so $2 \notin S$ by (2). But then it is easy to see that

$$(S \setminus \{2p\}) \cup \{2\}$$

will form a good set for n, also contradicting (2). Thus we see $q = 2$ is impossible.

To prove (11) we need to show $q = 3$ is possible only in the stated case

$$S = \{6p\} \cup M.$$

We assume S is good for $n = 3p+t$ $(1 \leqslant t \leqslant p)$, and

$$S = (pK) \cup (k^* M)$$

where $K = K_1 \cup (2K_2) \cup (3K_3) \cup (6K_6) \neq \emptyset$.

We take n large enough to be able to assume, by considering S^{-1} if necessary, that

$$|K| < \frac{2\psi(3)+1}{2} = 9\frac{2}{3} \quad \text{and} \quad K_1 = \emptyset.$$

We consider possible elements of K, remembering, as at (30), that

$$|K_r| \leqslant r-1.$$

Case A: $K_2 \neq \emptyset$. By (30), we have $|K_2| = 1$ and so $K_2 = \{k_2\}$ for some k_2. In fact, by the statement preceding (30), we see $k^* = k_2$. Hence $(k^*, 3) = 1$ by definition of K_2.

Subcase A(i): $K_3 \neq \emptyset$. Now $k_3 \in K_3 \Rightarrow \left(k_3, \frac{6}{3}\right) = 1$ so k_3 and consequently k_3^* are odd. By (30),

$$2 \geqslant \frac{k^*}{k_3} \geqslant \frac{k_3^*}{k_3}$$

$$\Rightarrow \frac{k_3^*}{k_3} = 1 \quad \text{since } k_3^* \text{ is odd,}$$

$$\Rightarrow K_3 = \{k_3\} \quad \text{where either } k_3 = k_2 \text{ or } 2k_3 = k_2.$$

Suppose $K_6 = \emptyset$. If $k_2 = k_3$, then $k_2 | a_i$ for each i, and so $k_2 = 1$. Thus $2p, 3p \in S$, and so $(S \setminus \{2p\}) \cup \{2\}$ would also be good for n, contradicting (2).

If $k_2 = 2k_3$, then similarly, $k_3 = 1$ and so $3p, 4p \in S$. Now $k^* = 2$ and so $a_i \in k^* M$ implies $2 | a_i$. Also, $a_i \geqslant n$ implies $3 | a_i$, since $a_i/(a_i, 3p) \leqslant n-1$. Together we see this gives $a_n > 3n$, and so $a_n/(a_n, 3p) > n$, providing a contradiction.

Thus suppose $K_6 \neq \emptyset$. We must have a $k_6 \in K_6$ such that

(i) If $k_3 = k_2$, then $k_2 \nmid 6k_6$;

(ii) If $2k_3 = k_2$, then $k_3 \nmid 6k_6$;

or the argument above would apply again, since then in each case $k_3 = 1$, and in (i), $k_6 | k_2$ implies $k_6 = 1$. Now we know that $k^*/k_6 = k_2/k_6 \leqslant 5$; also k_3 is odd and $(k_2, 3) = 1$, so in each case we must have $k_2/5 \in K_6$. Then:

if $k_3 = k_2$: $k_2/5 = 1$ by (18), and so $10p, 15p, 6p \in S$ and $k^* = 5$. Since $6p \in S$, and $3p < n \leqslant 4p$, we must have $(m, 6) \geqslant 2$ for each $m \in M$. Now $|K| \leqslant 4$, so $|M| \geqslant n-4$ and hence $M_1 = \max(m \in M)$ must be at least $6(n-7)/4$ (by similar reasoning to Lemma 3). Then

$$\frac{5m_1}{(5m_1, 6p)} \geqslant \frac{5m_1}{6} > n-1 \quad \text{whenever} \quad n \geqslant 32,$$

which is true by (9).

Thus we have $2k_3 = k_2$: Then $k_2/10 = 1$ by (18), and $20p, 15p$ and $12p \in S$. We get a similar contradiction to the above by considering $12p$.

Thus we must have $K_3 = \emptyset$.

Subcase A(ii): $K_3 = \emptyset$, $K_6 \neq \emptyset$. Now necessarily k_2 is odd, or we have $2 | a_i$ for each i. Thus the only possible elements of K_6 are k_2 or $k_2/5$.

If $k_2/5 \notin K_6$ then $k_2 = 1$ by (18), $S = \{2p, 6p\} \cup M$ and $(S \setminus \{2p\}) \cup \{2\}$ is good for n, contradicting (2).

Hence $k_2/5 \in K_6$, and so $k_2 = 5$ by (18). But then $6p \in S$ and $k^* = 5$, giving a contradiction as above. Thus $K_6 = \emptyset$.

Subcase A(iii): $k_3 = k_6 = \emptyset$. Then $k_2 = 1$ by (18), so $S = \{2p\} \cup M$ contradicting (2) as above.

Thus $K_2 = \emptyset$.

Case B: $K_3 \neq \emptyset$. By (30),

$$2 \geqslant \frac{k^*}{k_3} \geqslant \frac{k_3^*}{k_3} \quad \text{for all } k_3 \in K_3.$$

Hence $K_3 = \{k_3\}$ and either $k^* = k_3$ or $k^* = 2k_3$ (since $(k_3, 2) = 1$).

Subcase B(i): $k_6 \neq \emptyset$. Now $3 | 3$ and $3 | 6$, so necessarily $3 \nmid k^*$ by (18); also k_3 is odd.

If $k_3 = k^*$: Possible elements of K_6 are k_3 or $k_3/5$, and we obtain a contradiction as in A(ii) above.

If $2k_3 = k^*$: Possible elements of K_6 are $2k_3$, $2k_3/2$ or $2k_3/5$. If $2k_3/5 \notin K_6$, then $k_3 = 1$, $k^* = 2$ and $3p \in S$, giving a contradiction as in A(i). If $2k_3/5 \in K_6$, then $k_3 = 5$ by (18). Then $k^* = 5$ and $12p \in S$, giving a contradiction as in A(i).

Thus $K_6 = \emptyset$.

Subcase B(ii): $K_6 = \emptyset$, $K_3 = \{k_3\}$. Then $k^* = k_3$ so $k_3 = 1$, which would mean that $(S \setminus \{3p\}) \cup \{3\}$ would be good for n, contradicting (2).

Hence we must have:

Case C: $K_1 = K_2 = K_3 = \emptyset$. We must have $(k^*, 6) = 1$ by (18), so possible elements of K_6 are k^*, $k^*/5$. If $k^*/5 \in K_6$, then $k^* = 5$ and $6p \in S$, providing a contradiction as before. Thus we must have $K_6 = \{k^*\}$, $k^* = 1$, and so

$$S = \{6p\} \cup M, \quad m \in M \Rightarrow m \not\equiv 0 \pmod{p}.$$

[Note that $n_1(3) = 13$, $n_2(3) = 285\frac{1}{18}$ and $n_3(3)$ is such that $n \geqslant n_3(3)$ implies $\pi(n) - \pi\left(\frac{n-1}{2}\right) \geqslant 7$. Evaluation of $n_3(3)$ would give the range of validity of (11).]

4. Proof of Theorem 3. We suppose S is good for $n = p^a$, $a \geqslant 2$. Suppose there is an a_i in S with $a_i \equiv 0 \pmod{p^a}$; $a_i = Ip^a$ say. By (18) there is an a_j such that $a_j \not\equiv 0 \pmod{p}$, so

$$\frac{a_i}{(a_i, a_j)} = \frac{I}{(I, a_j)} p^a \geqslant p^a.$$

Hence there cannot be such an a_i, and so

$$S = (p^{a-1}K_{a-1}) \cup (p^{a-2}K_{a-2}) \cup \ldots \cup (pK_1) \cup (K_0)$$

for some (possibly empty) sets K_i, where $k \in K_i \Rightarrow k \not\equiv 0 \pmod{p}$, $i = 0, 1, \ldots, a-1$.

Suppose $k \in K_i$, $l \in K_i$ and $k \equiv l \pmod{p^a}$, so

$$k = l + rp^a \quad \text{with} \quad r > 0, \text{ say}.$$

Then

$$\frac{p^i k}{(p^i k, p^i l)} = \frac{k}{(k, l)} = \frac{l}{(r, l)} + \frac{r}{(r, l)} p^a > p^a.$$

Thus we cannot have $k \equiv l \pmod{p^a}$.

Suppose $k \in K_i$, $l \in K_j$, $i \neq j$ and $k \equiv l \pmod{p^a}$, so

$$k = l + rp^a \quad \text{with} \quad r \geqslant 0, \text{ say.}$$

Then

$$\frac{p^i k}{(p^i k, p^j l)} \geqslant \frac{k}{(k, l)}.$$

If $r \neq 0$, then as above this is greater than p^a. Hence we must have $r = 0$, so $k = l$.

Corollary. *The conjecture is true for $n = p^2$, p any prime.*

Proof. Suppose S is good for p^2, so

$$S = pK_1 \cup K_0.$$

Within K_1 and K_0, all numbers are distinct (mod p^2), and are not divisible by p. Thus there are $p^2 - p$ residue classes in which to place p^2 numbers. There are at most 2 in any one class, and so there must be at least p congruent pairs, lying in different sets. By Theorem 3, they are in fact equal, so we can find

$$L = \{\lambda_1, \ldots, \lambda_p\} \quad \text{with} \quad \lambda_i \in K_0, \ \lambda_i \in K_1.$$

Take any $\lambda_i \in L$, $\lambda_j \in L$. Then $p\lambda_i \in S$, $\lambda_j \in S$ so

$$\frac{p\lambda_i}{(p\lambda_i, \lambda_j)} < p^2 \Rightarrow \frac{\lambda_i}{(\lambda_i, \lambda_j)} < p.$$

Similarly $\frac{\lambda_j}{(\lambda_i, \lambda_j)} < p$, as $p\lambda_j \in S$, $\lambda_i \in S$, and so L is good for p, contradicting (3).

5. Remark. Suppose n is such that there exists a good S for n. We know that n is not of the form p, $p+1$, $p+2$, $p+3$ or p^2 for any prime p: The first few such n are 27, 28, 35, 36, 51, 52, ... Using Lemma 2 and (10), we see that if $n \geqslant 26$ and $n = 2p+1$, and the conjecture has been proven true for $n = 2p$, then we can deduce it true for n: Thus the conjecture is true for $n = 27 = 2\cdot 13+1$ and $n = 35 = 2\cdot 17+1$, as for each of these, $n-1$ is of the form $p'+3$ for a prime p'. Similarly, using (11) and sufficiently high n, we can deal with $n = 3p+1$ if the result is known for $n-1$. So, in general, the conjecture is true for:

(a) $n = 2p+1 = p'+4$, p, p' prime,

and

(b) $n = 3p+1 = (2p'+1)+1 = (p''+4)+1$, p, p', p'' prime,

and n sufficiently large.

References

[1] P. Erdös, *Problems and results in Combinatorial Number Theory*, in *A survey of Combinatorial Theory*, North Holland Publishing Co., 1973.

[2] J. Marica and J. Schönheim, *Differences of sets and a problem of Graham*, Canad. Math. Bull. 12 (5) (1969), pp. 635–637.

[3] R. Winterle, *A problem of R. L. Graham in Combinatorial Number Theory*, Proceedings of the Louisiana Conference on Combinatorics, Louisiana State University, Baton Rouge, March 1–5, 1970, pp. 357–361.

[4] W. Y. Vélez, *Some remarks on a number theoretic problem of Graham*, Acta Arith. 32 (1977), pp. 233–238.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
Heslington, England

Received on 8. 6. 1976 (854)