On a problem of R. L. Graham

by

R. D. Boyle (Heslington)

O. 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.**

$$\max_{1 \leq i < j \leq n} \frac{a_j}{a_i} \geq n \quad \text{for any} \ S, \text{any} \ n \geq 2.$$

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 $p | a_i$ for some $i$, and $p$ is prime, $p \leq n$ (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 $p | a_i$ for some $i$, then

$$p \leq (n-1)/2.$$  

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

$$n = gp + t, \quad 1 \leq t \leq p,$$

(8) $p | a_i$ for some $i$,

(9) $n$ is sufficiently large depending on $g$.  

Postulated 21. 5. 1976  

(551)
then
\[ p \leq (n-1)/3 \quad \text{(i.e. } q \geq 3). \]

If \( (n-1)/4 < p \leq (n-1)/3 \), so \( q = 3 \), then
\[ S = \{2p\} \cup M \]
for some \( M \), where \( m \in M \) implies \( m \equiv 0 \pmod{p} \). If \( q \leq 4 \) and we define
\[ Q = \{1, 2, \ldots, q\}, \]
the \( \text{l.c.m.} \) of the first \( q \) natural numbers and
\[ \nu(q) = \sum_{r \mid Q} \frac{\nu^2(r/\nu^2)}{Q} \]
then either
\( q < (2p+1)/2 \) multiples of \( p \) in \( S \)
or
\( q > n-(2p+1)/2 \) multiples of \( p \) in \( S \).

Further, if (14) holds, then
\[ (a_i, Q) \geq 2 \quad \text{when } p \mid a_i. \]

Theorem 3. If \( n = p^a \) for \( p \) prime, \( a \geq 2 \), and \( S \) is good for \( n \), then
\[ S = (p^{a-1}K_{a-1}) \cup (p^{a-2}K_{a-2}) \cup \ldots \cup (p^1K_1) \cup (K_0) \]
where the (not necessarily non-empty) sets \( K \) are such that
\[ k \in K_i \Rightarrow k \equiv 0 \pmod{p}, \]
\[ k, l \in K_i \Rightarrow k \equiv l \pmod{p}, \]
\[ k \in K_i, l \in K_j \Rightarrow k \equiv l \pmod{p^a.} \]

As a corollary to Theorem 3, we can deduce that there are no good \( S \) for \( n = p^a \), \( p \) 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
\[ S^{-1} = \left[ \frac{s^*}{a_1}, \ldots, \frac{s^*}{a_n} \right]. \]

Lemma 1. The ratios of \( S^{-1} \) coincide with those of \( S \), and so \( S \) is good for \( n \) if \( S^{-1} \) is good for \( n \).

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

We will assume throughout that
\[ \varphi(a_i) \leq n-1, \quad 1 \leq i, j \leq n \]
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 \( n \),
\[ \frac{a_i}{(a_i, a_j)} \leq n-2, \quad 1 \leq i, j \leq n \]
and equality gives \( (n-1)a_i \). Suppose there are no multiples of \( n-1 \) in \( S \). Then
\[ \frac{a_i}{(a_i, a_j)} \leq n-1, \quad 1 \leq i, j \leq n \]
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 \( S \), \( a_i \), say. Then
\[ \frac{a_i}{(a_i, a_j)} \leq n-1, \quad 1 \leq i, j \leq n \]
and
\[ \frac{a_i}{(a_i, a_j)} \leq n-2, \quad i \neq r, \quad 1 \leq i, j \leq n. \]

Hence \( S \setminus \{a_i\} \) 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
\[ (k_i, t) = 1, \quad 1 \leq i \leq a. \]

Then if \( k^* = \text{l.c.m.} [k_1, \ldots, k_a] \), we have
\[ \frac{k^*}{k_1} > \frac{\alpha}{\varphi(t)} - 1. \]

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 \( 1 \leq q_i < q_{i+1} < \ldots < q_i \)
and
\[ (q_i, t) = 1, \quad 1 \leq i \leq a. \]

Suppose \( \alpha = \varphi(t) + \mu, \quad 1 \leq \mu \leq \varphi(t). \)
Now in any block of \( t \) consecutive integers, there can be at most \( q(t) \) primes. Hence
\[
q_1 \geq \frac{2t + \mu}{\mu} \geq \left( \frac{\alpha}{\frac{1}{p(t)}} - 1 \right) t.
\]

Note that \( t = 1 \) always satisfies the requirements of the lemma, whence
\[
\frac{k_*}{k_1} = q_1 > a - 1 \Rightarrow \frac{k_*}{k_1} \geq a.
\]

\[ (20) \]

2. Proof of Theorem 1. Suppose \( S \) is good for \( n \), and
\[
S = (pK) \cup L, \quad \text{where} \quad l \in L \iff l \equiv 0 \pmod{p}.
\]

We suppose \( K \neq \emptyset \), whence (18) gives \( L \neq \emptyset \). We also suppose (6) does not hold, so \( \frac{n - 1}{p} = 1 \) by (3) and (5). Let \( k \in K, \ l \in L; \) then
\[
\frac{kp}{(k, l)} = k < \frac{n - 1}{p} < 2p = \frac{k}{(k, l)} < 2 \Rightarrow k | l \forall k \in K, \ l \in L.
\]

So \( k_* \) is the I.C.M. of the elements of \( K \), we have
\[
S = (pK) \cup (k_*M) \quad \text{for some} \quad M.
\]

Let \( |K| = c, \) then \( |M| = |L| = n - c. \)

Let \( m_1 = \max(m \in M) \), so \( m_1 \geq n - c. \)

Let \( k_0 = \min(k \in K) \); then \( k_* \geq ck_0 \) by (20).

Now we know that
\[
\frac{m_1 k_*}{(m_1 k_*; k_0)} \leq n - 1
\]

and so
\[
\frac{m_1 k_*}{k_0} \leq n - 1
\]

\[ = (n - 1) \leq n - 1 \]

\[ = c \leq n - 1. \]

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 \( k_0 | a_k \) for each \( k, \) so from (18) \( k_0 = 1 \) and \( pK = \{p\}. \) Also \( m_1 \geq n \) since \( |M| = n - 1, \)

\[ p \leq n - 1 \] and we cannot have \( p \in M. \) Then
\[
\frac{m_1}{(m_1, p)} m_1 \geq n
\]
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 \( p \geq 3 \) so we cannot have \( 3 \) distinct elements \( a_1, a_2, a_3 \in S \) with \( i > j > k \) and \( a_i = a_j (\mod p); \ a_k = a_j + rp, \) say, for some \( r > 0. \) Then
\[
\begin{align*}
\frac{a_i}{(a_i, a_j)} &= \frac{a_j + rp}{(r, a_j)} &= \frac{a_i}{(r, a_j)} \frac{r}{(r, a_j)} p \\
&\leq p + 1 \quad \text{as} \ S \text{ is good for } p + 2.
\end{align*}
\]

Hence \( r = a_j, \) so \( a_i = a_j(p + 1). \) Then
\[
\frac{a_i}{a_j} \geq \frac{a_i}{a_k} = \frac{a_j}{a_k} (p + 1) > p + 1
\]

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 \( n \geq 6, \) so \( n - 3 > (n - 1)/2, \) and hence there are no multiples of \( p \) in \( S. \) We consider possible congruent pairs \( \mod p \) in \( S. \) Suppose
\[
a_i = a_j (\mod p),
\]

\[ a_i = a_j + rp, \quad r > 0, \quad \text{say}. \]

Then
\[
\begin{align*}
\frac{a_i}{a_j} &= \frac{a_j}{a_j} + \frac{r}{(a_j, r)} p \leq p + 2.
\end{align*}
\]

So \( r | a_j, \) and either \( a_j = r \) or \( a_j = 2r. \) Thus either
\[
\begin{align*}
a_i &= a_j(p + 1) \quad \text{or} \quad a_i = \frac{a_j}{2} (p + 2).
\end{align*}
\]
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

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

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

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

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

Then

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

Hence

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

Thus

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

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

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

But then

$$\frac{(p+1) a_i}{a_i, a_l} = \frac{(p+1)^2}{[(p+1) a_i, (p+1) a_k]} = (p+1)^2 > p+2.$$ 

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

Case B. Suppose we have $a_s, a_i, a_k, a_j \in S$, $t > s$ and

$$a_s = \frac{a_s}{2} (p+2), \quad a_i = \frac{a_i}{2} (p+2).$$

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

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

Thus

$$d \geq \frac{a_i}{2} \geq \frac{a_i}{2} \geq d = a_s, \quad \text{since } d | a_s.$$ 

Hence

$$2a_s \geq a_i.$$ 

Now suppose $2^e | a_s$, i.e. $a_s = 2^e a_e$, with $a_e$ odd. Then $2^e+1 | a_i$ since

$$\frac{a_i}{2} (p+2), \quad \text{and } p+2 \text{ is odd. This gives}$$

$$\frac{d'}{d'} = \frac{a_e}{2} \frac{a_i}{a_i} = \frac{a_e}{2} (p+2) \leq p+2 \quad \text{as } S \text{ is good for } p+3.$$ 

Thus $d' \geq a_e/2$, and so by (23)

$$\frac{a_s}{2} \leq \frac{a_i}{4}.$$ 

(24) and (22) now give

$$a_i = 2a_e,$$ 

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

$$a_s, \quad 2a_e, \quad \frac{a_e}{2} (p+2), \quad a_e (p+2) \in S.$$ 

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 $n = q + h$, $h \geq 4$. 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 $n = q + t,$
$1 \leq t \leq p,$ and

$$S = (pK) \cup L.$$
where \( K \neq \emptyset, L \neq \emptyset \) and \( l \in L \Rightarrow l \equiv 0 \pmod{p} \). \( Q \) and \( \psi(q) \) are as at (12) and (13), and we define

\[
u_1(q) = q^2 + q + 1, \quad \text{so} \quad n \geq n_1(q) \Rightarrow p > q,
\]

\[
u_1(q) = 2(p^2 - 1)Q(p + Q) + Q + 1.
\]

\( n_2(q) \) is such that

\[
\forall \geq n_2(q) = \pi(n) - \pi\left(\frac{n-1}{2}\right) + q > \frac{2\psi(q) + 1}{2}.
\]

Then by "sufficiently large depending on \( q \)" we shall mean

\[
\forall \geq \max\{n_1(q), n_2(q), n_3(q)\}.
\]

Suppose \( k \in K \) and \( l \in L \); then

\[
\frac{k}{(k, l)} \leq q.
\]

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

\[
\frac{k}{z} \leq q \quad \text{by (25)},
\]

so

\[
k \leq \frac{Q}{z} = \frac{k}{z} \quad \text{by (26)},
\]

Now for each \( r \mid Q \) we define the (possibly empty) set \( K_r \) by

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

Also, put

\[
k^* = \begin{cases} \text{l.c.m.} \left[ \frac{k}{r} : k \in K_r \right] & \text{if } K_r \neq \emptyset, \\ 1 & \text{if } K_r = \emptyset,
\]

and

\[
k^* = \text{l.c.m.}[k^*_1, \ldots, k^*_n].
\]

Then (26) tells us that \( k^* \mid l \) 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 \( n_2 = \max\{m \in M\} \), so \( m_4 \geq n - c\); let \( k_0^* = \min\{k \in K_r\} \).

Now \( k \in K_r \) implies \((k, Q, r) = 1\), and so by Lemma 3,

\[
\frac{k^*}{k_0^*} \geq \frac{k^*}{k_0^*} > r, \quad \frac{|K_r|}{\varphi(Q, r)} - 1.
\]

We know that \( S \) is good for \( n \), and so

\[
\frac{m_2 k^*}{(m_1 k^* r^k_0^*, p)} \leq n - 1 \quad \text{(when } K_r \neq \emptyset)\]

\[
= \frac{m_2}{(m_1 k^* r^k_0^*, p)} \leq n - 1
\]

\[
\frac{n_2^* k^*}{r^k_0^*} \leq n - 1
\]

\[
\frac{(n - c) Q}{\varphi(Q, r)} \left( \frac{|K_r|}{\psi(Q, r)} - 1\right)
\]

\[
\leq n - 1
\]

\[
= \left( r^2 + Q \right) \frac{n - (r^2 + cQ)}{Q(n - c)}
\]

Now clearly

\[
\sum_{r \mid Q} |K_r| = c.
\]

hence

\[
\sum_{r \mid Q} \frac{Q}{r} \left( \frac{(r^2 + Q)n - (r^2 + cQ)}{Q(n - c)} \right)
\]

\[
= nc - c^2 < (n - c) \sum_{r \mid Q} \psi(Q) + (n - 1) \sum_{r \mid Q} r^2 \varphi(Q, r)
\]

\[
> nc - c^2 < (n - c)Q + (n - 1)\psi(Q)
\]

\[
\Rightarrow c^2 > (n + Q) + n(Q + \psi(Q)) - \psi(Q) > 0.
\]

Note that \( n \geq n_2(q) \) implies

\[
(n + Q)^2 - 4[n(Q + \psi(q)) - \psi(q)] \geq (n - (Q + 2\psi(q) + 1))^2
\]

\[
\Rightarrow n - (Q + 2\psi(q) + 1) 1
\]

\[
\Rightarrow 6 - \text{Acta Arithmetica} \ XXXIV, 2
\]
and so $n \geq n_4(q)$ must imply
\[ c < Q + \varphi(q) + \frac{1}{2} < \frac{2n}{3} \quad \text{or} \quad \frac{2\varphi(q) + 1}{2} \leq c < Q + \frac{2\varphi(q) + 1}{2}, \]
by locating the roots of the expression on the left-hand side of (27). Suppose
\[ \frac{2\varphi(q) + 1}{2} \leq c < Q + \frac{2\varphi(q) + 1}{2}, \]
then $S^{-1}$ would contain $c' = c - c$ multiples of $p$, and $c'$ could not satisfy either of the inequalities at (28). Hence we see
\begin{align*}
(29(i)) & \quad c < \frac{2\varphi(q) + 1}{2} \quad \text{or} \\
(29(ii)) & \quad c > n - \frac{2\varphi(q) - 1}{2}.
\end{align*}
This proves (14) and (15).

Now $|M| = n - c$; also $m \in M$, implies $m \equiv 0 \pmod{p}$, and, by Theorem 1, $m \in M$ implies $m \equiv 0 \pmod{p'}$ where $p'$ is any prime greater than $(n-1)/2$. Hence we see that
\[ n \geq n_4(q) = m_3 \geq n \quad \text{if} \quad c < (2\varphi(q) + 1)/2. \]
Now suppose $K_r \neq \emptyset$, let $k_r \in K_r$. Then
\[ \frac{m_3 k^*}{(m_3 k^*, r k_p, p)} \leq (n-1) = \frac{n k^*}{r k_p} \leq u - 1 = \frac{k^*}{k_r} \leq r - 1 \]
\[ \Rightarrow |K_r| < r - 1 \quad \text{by (20)}. \]
Hence $|K_r| = 0$, so $K_r = \emptyset$, and (16) is proved. Note that $|K_{r+1}| \leq r - 1$ gives
\[ c \leq \sum_{r=0}^{n-2} (r-1) \]
\[ \Rightarrow \quad \begin{cases} c \leq \sigma(Q) - \sigma(Q) \text{ if (29(i)) holds or} \\ c \geq n - \sigma(Q) - \sigma(Q) \text{ if (29(ii)) holds} \end{cases} \]
by considering $S^{-1}$ in the latter case.

To prove (10) we need to show $q = 2$ is impossible. If $q = 2$, then $Q = 2$, $\varphi(2) = 1$, so
\[ n_4(2) = \frac{51}{2}, \quad n_4(2) = 2. \]
Thus the result will be valid for all $n \geq 26$. We suppose that
\[ S = (p M) \cup (M') \]
is good for $n = 2p + t \leq t \leq p$, so
\[ K = K_1 \cup (2K_1). \]
By (31), we see that, if $n \geq 26$, $|K| = 1$ or $|K| = 1$; 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 (3). 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 $n = 3p + t (1 \leq t \leq p)$, and
\[ S = (p M) \cup (M') \]
where $K = K_1 \cup (2K_1) \cup (3K_1) \cup (6K_1) \neq \emptyset$.

We take a large enough to be able to assume, by considering $S^{-1}$ if necessary, that
\[ |K| < \frac{2\varphi(3) + 1}{2} = 9 \frac{2}{3} \quad \text{and} \quad K_1 = \emptyset. \]
We consider possible elements of $K$, remembering, as at (30), that
\[ |K_1| < r - 1. \]
Case A: $K_1 = \emptyset$. By (30), we have $|K_1| = 1$ and so $K_1 = \{k_2\}$ 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): $K_2 \neq \emptyset$. Now $k_2 \in K_2 = \{k_2\}$, so $k_2$ and consequently $k^*_2$ are odd. By (30),
\[ \frac{k^*_2}{k_2} = \frac{k^*_2}{k_2} \]
\[ = \frac{k^*_2}{k_2} = 1 \quad \text{since} \ k^*_2 \text{ is odd}, \]
\[ = K_2 = \{k_2\} \quad \text{where either} \ k_2 = k_2 \text{ or} \ 2k_2 = k_2. \]
Suppose \( K_4 = \emptyset \). If \( k_2 = k_4 \), then \( k_4 \mid a_i \) 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 \( k_2 = 2k_4 \), then similarly, \( k_2 = 1 \) and so \( 3p, 4p \in S \). Now \( k^* = 2 \) and so \( a_1 \mid k^* \) implies \( 2 \mid a_i \). Also, \( a_1 \mid n \) implies \( 3 \mid a_i \), since \( a_i/(a_i, 3p) \leq n - 1 \). Together we see this gives \( a_1 > 3n \), and so \( a_i/(a_i, 3p) > n \), providing a contradiction.

Thus, suppose \( K_4 \neq \emptyset \). We must have \( k_0 \in K_4 \) such that

(i) If \( k_0 = k_4 \), then \( k_0 \nmid 6k_3 \);

(ii) If \( 2k_3 = k_4 \), then \( k_0 \nmid 6k_3 \);

or the argument above would apply again, since in each case \( k_3 = 1 \), and in (i), \( k_3 \nmid k_4 \) implies \( k_4 = 1 \). Now we know that \( k^* \mid k_0 \); \( k_0 \leq 5 \); and \( k_3 \) is odd. Also \( k_0 = 2k_3 \); \( 3 \mid k_3 \); and \( k_3 = 5 \);, so in each case we must have \( k_0 = 5 \in K_4 \).

Then:

if \( k_3 = k_2 = k_4 \); \( k_0 = 1 \);, and so \( 10p, 15p, 6p \in S \); and \( k^* = 5 \).

Since \( 6p \in S \), and \( 6p < n \leq 4p \), we must have \( n \geq 2 \) for each \( m \in M \).

Now \( |K| \leq 4 \), so \( |M| \geq n - 4 \), and hence \( M = \max(m \in M) \) must be at least \( 6(n - 4)/4 \) (by similar reasoning to Lemma 3). Then

\[
\frac{5m_1}{(5m_1, 6p)} > \frac{5m_1}{6} > n - 1 \quad \text{whenever} \quad n \geq 32,
\]

which is true by (9).

Thus we have \( 2k_3 = k_4 \); then \( k_3 = 1 \);, and \( 20p, 15p, 12p \in S \). We get a similar contradiction to the above by considering \( 12p \).

Thus we must have \( K_4 = \emptyset \).

Subcase A(ii): \( K_4 = \emptyset \). Now necessarily \( k_2 \) is odd, or we have \( 2 \mid a_i \) for each \( i \). Thus the only possible elements of \( K_4 \) are \( k_4 \) or \( k_4/5 \).

If \( k_4 \mid k_4 \) then \( k_4 = 1 \); \( S = \{2p, 6p \} \cup M \) and \( \{S \setminus \{2p\} \} \cup \{2\} \)

is good for \( n \), contradicting (2).

Hence \( k_4/5 \in K_4 \), and so \( k_4 = 5 \);, and \( k^* = 5 \), giving a contradiction as above. Thus \( K_4 = \emptyset \).

Subcase A(iii): \( k_1 = k_4 \). Then \( k_1 = 1 \); \( S = \{2p \} \cup M \)

contradicting (2) as above.

Thus \( K_4 = \emptyset \)

Case B: \( K_4 \neq \emptyset \). By (30),

\[
2 \geq \frac{k^*}{k_3} \geq \frac{k^*}{k_0} \quad \text{for all} \quad k_0 \in K_4,
\]

Hence \( K_4 = \{k_0\} \), and either \( k^* = k_0 \) or \( k^* = 2k_3 \) (since \( (k_3, 2) = 1 \)).

Subcase B(i): \( k^* = k_0 \). Now \( 3 \mid 3 \) and \( 3 \mid 6 \), so necessarily \( 3 \mid k^* \) by (18); also \( k_3 \) is odd.

If \( k^* = k^* \); Possible elements of \( K_4 \) are \( k_4 \) or \( k_0 \), and we obtain a contradiction as in A(ii) above.

If \( 2k^* = k^* \); Possible elements of \( K_4 \) are \( 3k_4, 3k_4/3 \) or \( 2k_4/3 \). If \( 2k^* \in K_4 \), then \( k_4 = 1 \); \( k = 2 \); and \( 3p \in S \), giving a contradiction as in A(i). If \( 2k^* \in K_4 \), then \( k_4 = 5 \) by (18). Then \( k^* = 5 \); and \( 12p \in S \), giving a contradiction as in A(i).

Thus \( K_4 = \emptyset \).

Subcase A(ii): \( K_4 = \emptyset \). Then \( k^* = k_4 \), so \( k_4 = 1 \), which means that \( \{S \setminus \{3p\} \} \cup \{3\} \) would be good for \( n \), contradicting (2).

Hence we must have:

Case C: \( K_1 = K_2 = K_4 = \emptyset \). We must have \( (k^*, 6) = 1 \); so possible elements of \( K_4 \) are \( k^*, k^*/5 \). If \( k^* \in K_4 \), then \( k^* = 5 \); and \( 6p \in S \), providing a contradiction as before. Thus we must have \( K_4 = \{k^* \} \), \( k^* = 1 \), and so

\[
S = \{6p \} \cup M, \quad m \in M = m \equiv 0 \pmod{p}.
\]

[Note that \( m_1(3) = 13 \); \( m_2(3) = 285 \); \( 1/18 \); and \( m_4(3) \) is such that \( n \equiv n_4(3) \)

implies \( n \leftarrow \pi \left( \frac{n - 1}{2} \right) \equiv 1 \). Evaluation of \( m_4(3) \) would give the range of validity of (11).]

4. Proof of Theorem 3. We suppose \( S \) is good for \( n = p^a, a \geq 2 \).

Suppose there is an \( a_j \) in \( S \) with \( a_j \equiv 0 \pmod{p^a} \); \( a_j = 1p^a \) say. By (18) there is an \( a_j \) such that \( a_j \not\equiv 0 \pmod{p} \), so

\[
a_j \equiv \frac{I}{(I, a_j)} p^a \equiv p^a.
\]

Hence there cannot be such an \( a_j \), and so

\[
S = (p^{a-1} K_{a-1}) \cup (p^{a-2} K_{a-2}) \cup \ldots \cup (p K_a) \cup (K_a)
\]

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

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

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

Then

\[
\frac{p^i k}{(p^i k, p^i l)} = \frac{k}{(k, l)} \left( \frac{l}{r} \right) > p^a.
\]

Thus we cannot have \( k \equiv l \pmod{p^a} \).
Suppose \( k \in K_1, \ l \in K_2, \ i \neq j \) and \( k = l \mod p^n \), so

\[
k = l + rp^n \quad \text{with} \quad r \geq 0, \ \text{say}.
\]

Then

\[
\frac{p^r k}{(p^r k, p^r l)} > \frac{k}{(k, l)}.
\]

If \( r = 0 \), then as above this is greater than \( p^n \). Hence we must have \( r = 0 \), so \( k = l \).

\textbf{Corollary.} The conjecture is true for \( n = p^2 \), \( p \) any prime.

\textbf{Proof.} Suppose \( S \) is good for \( p^2 \), so

\[
S = pK_1 \cup K_2.
\]

Within \( K_1 \) and \( K_2 \), 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

\[
J = \{ \lambda_1, \ldots, \lambda_n \} \quad \text{with} \quad \lambda_i \in K_2, \ \lambda_i \in K_1.
\]

Take any \( \lambda_i \in I, \ \lambda_j \in L \). 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 \( p\lambda_i \in S, \ \lambda_i \in S \), and so \( I \) is good for \( p \), contradicting (3).

5. \textbf{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, \ldots Using Lemma 2 and (10), we see that if \( n \geq 26 \) 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 \( n = 27 = 2\cdot13 + 1 \) and \( n = 35 = 2\cdot17 + 1 \), as for each of these, \( n - 1 \) is of the form \( p^2 + 3 \) 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.