Some remarks on a number theoretic problem of Graham

by

WILLIAM YSILAS VÁLÉZ (Murray Hill, N. J. and Tucson, Ariz.)

In considering generalizations of van der Waerden's theorem, R. L. Graham [1] was led to consider finite sequences of positive integers $a_1 < a_2 < \ldots < a_n$ and certain ratios, namely, $a_i/(a_1, a_2)$ where $(x, y)$ denotes the g.c.d. of $x$ and $y$. He proposed the following conjecture.

**Conjecture I.** If $0 < a_1 < a_2 < \ldots < a_n$, then
\[
\max_{i \neq j} \left\{ a_i/(a_1, a_2) \right\} \geq n.
\]

The conjecture has been verified in some special cases:
(a) $a_i$ is square-free for all $i$ (Marica and Schönheim [2]),
(b) $a_1$ is prime (Winterle [4]),
(c) $n$ is prime (Szemerédi [3]).

One of the results of this note is to prove Conjecture I when $n-1$ is prime.

A natural question to ask is: For what sequences is equality achieved? Before going into this question we make some remarks.

1. If we multiply a sequence by a constant we obtain the same set of ratios, so we may assume g.c.d. $(a_1, a_2, \ldots, a_n) = 1$.

2. Given a sequence $\mathcal{Q} = (a_1, a_2, \ldots, a_n)$, let $\mathcal{A} = \text{l.c.m.} \{a_1, a_2, \ldots, a_n\}$ and form $\mathcal{Q}' = (\mathcal{A}/a_n, \mathcal{A}/a_{n-1}, \ldots, \mathcal{A}/a_1)$.

It is easy to show that $\mathcal{Q}$ and $\mathcal{Q}'$ have the same set of ratios.

**Notation.** Let $\mathcal{M}_n = \text{l.c.m.} \{1, 2, \ldots, n\}$ and $b_i^{(n)} = \mathcal{M}_n/(n-i+1)$, so $b_1^{(n)} = \mathcal{M}_n/(n-1) < \ldots < \mathcal{M}_n/2 < \mathcal{M}_n/1$ is the “inverse” of $\{1, 2, \ldots, n\}$.

**Definition.** Given a sequence $a_1 < a_2 < \ldots < a_n$, we say it is a standard sequence if it is a multiple of $\{1 < 2 < \ldots < n\}$ or of $\{b_1^{(n)} < b_2^{(n)} < \ldots < b_n^{(n)}\}$. That is, either $a_i = ki$ for all $i$. 

Received on 24. 3. 1975 (691)
or

\[ a_i = k b_i^{(a)} \] for all \( i \).

Graham also made the following conjecture.

**Conjecture II. Assume**

\[
g.c.d. (a_1, a_2, \ldots, a_n) = 1 \quad \text{and} \quad \max_{1 \leq i < j \leq n} \{ a_i / (a_i, a_j) \} = n.
\]

Then the sequence is a standard sequence except for \( n = 4 \), where we have the additional sequence \( \{ 2, 3, 4 \} \).

The reason for this exceptional sequence is perhaps explained by the following theorem.

**Theorem 1.** Let \( \mathcal{Q} = \{ a_2 = \ldots = a_n \} \) be a standard sequence and \( b \) any integer such that \( b \neq a_i \) for any \( i \) and \( g.c.d. (a_1, a_2, \ldots, a_n, b) = 1 \).

Form the new sequence \( \mathcal{Q}' = \{ a_1 < a_2 < \ldots < a_n, b \} \) (where \( b \) is inserted in the appropriate place). Then if \( \mathcal{Q}' \) is not a standard \( n + 1 \) sequence, we have

\[
\max_{1 \leq i < j \leq n} \{ a_i / (a_i, a_j), b / (a_i, b), a_i / (a_i, b) \} > n + 1,
\]

except possibly when \( n = 4 \).

For \( n = 4 \) we have the only exception to the assertion of the theorem, namely, \( \mathcal{Q} = \{ 2, 3, 4 \} \), \( b = 3 \), i.e., \( \{ 2, 3, 4 \} \).

**Proof.** We first note that \( g.c.d. (a_1, a_2, \ldots, a_n, b) = 1 \) is no restriction.

Assume \( a_i = k b_i^{(a)} \). Let \( a = \text{lcm.} \{ a_1, a_2, \ldots, a_n, b \} \) and form the new sequence

\[
\{ a/a_n < a/a_{n-1} < \ldots < a/a_1, b \}.
\]

Hence we have the new sequence

\[
\mathcal{Q}' = \{ k < 2k < 3k < \ldots < nk, b' \} \quad \text{with} \quad (b', k) = 1.
\]

We will prove the theorem for this sequence.

We assume that \( \mathcal{Q}' \) is not a standard sequence.

If \( k = 1 \), then \( b' \neq n + 1 \), since \( \mathcal{Q}' \) is not a standard sequence. Hence \( b' > n + 1 \), but \( b' / (n, k) = b' > n + 1 \).

Hence, we may assume that \( k > 1 \).

If \( b' > n + 1 \), then \( b' / (n, k, b') = b' > n + 1 \).

If \( b' = n + 1 \), then \( k(n, b') = kn > n + 1 \).

If \( b' = n \), then \( k(n-1) / (k(n-1), b') = k(n-1) > n + 1 \) for \( k > 2 \) or \( n > 3 \). If \( k = 2, n = 3 \), then \( 2(3-1) = 3 + 1 \) and this gives the sequence \( \{ 2 < 4 < 3 \} \).

If \( b' = n - 1 \), then \( kn / (b', kn) = kn > n + 1 \).

Hence, we may assume that \( b' < n + 1 \), so \( b' + 1 < n \) and \( k(b' + 1) \) appears somewhere in the sequence \( \mathcal{Q}' \) and

\[
k(b' + 1) / (k(b' + 1), b') = k(b' + 1).
\]

If \( k(b' + 1) > n + 1 \), then we are done.

If not, then \( k(b' + 1) < b' + k \leq n + 1 \). Define \( i \) by

\[
k(b_i^{(a)} + 1) > n + 1;
\]

\[
k(k(b^{(i+1)} + 1)) < n + 1.
\]

Then \( l \geq 0 \) and we have that \( k^{l+1} b^{(i+1)} + 1 < k^{l+1} b^{(i+1)} + 1 \leq n + 1 \), \( k^{l+1} b^{(i+1)} + 1 \) appears somewhere in the sequence \( \mathcal{Q}' \), and

\[
k(k^{l+1} b^{(i+1)} + 1) / (k(k^{l+1} b^{(i+1)} + 1), b') = k(k^{l+1} b^{(i+1)} + 1) > n + 1.
\]

**Theorem 2.** Conjecture II implies Conjecture I.

**Proof.** The proof proceeds by induction on \( n \). Assume that Conjecture I is true for \( n \) and consider

\[
0 < a_1 < \ldots < a_n < a_{n+1}.
\]

We know by induction that

\[
\max_{1 \leq i < j \leq n} \{ a_i / (a_i, a_j) \} \geq n.
\]

If \( \max_{1 \leq i < j \leq n} \{ a_i / (a_i, a_j) \} > n \), then

\[
\max_{1 \leq i < j \leq n+1} \{ a_i / (a_i, a_j) \} \geq n + 1.
\]

Hence, we may assume that the max is exactly \( n \).

But by Conjecture II, the sequence is standard, i.e., \( a_1 < a_2 < \ldots < a_n \) is a standard sequence. Now by Theorem 1 we have

\[
\max_{1 \leq i < j \leq n+1} \{ a_i / (a_i, a_j) \} \geq n + 1.
\]

If we could show that Conjecture I implies Conjecture II, then we could show, using Theorem 1 and double induction, that both conjectures are true.

**Theorem 3 (Szemerédi).** Conjecture I is true for \( n = p, p \) a prime.

**Proof.** We may assume that \( g.c.d. (a_1, a_2, \ldots, a_p) = 1 \).

If \( a_i = a_j \equiv 0 (mod \ p), i > j \), then \( a_i = a_j + p \cdot r \). Let \( d = (a_i, a_j) \), then \( d = (a_i - a_j, d) \), so \( d \mid p \cdot r \), but \( d \mid p \cdot r \) is a unit. So we have that

\[
a_i / (a_i, a_j) = (a_i + r) / d = a_i / (a_i + p) / d > p.
\]

If we have that if two of the \( a_i \) are congruent modulo \( p \) to a unit, then

\[
\max_{1 \leq i < j \leq n} \{ a_i / (a_i, a_j) \} > p.
\]

Assume that \( a_i \equiv a_j (mod \ p) \), if \( a_i \equiv 0 (mod \ p), a_j \equiv 0 (mod \ p) \). Then since there are \( p \) \( a_i \) and only \( p - 1 \) units modulo \( p \), we must have at least one \( i \) for which \( p \mid a_i \). But \( g.c.d. (a_1, \ldots, a_p) = 1 \), so there is a \( j \) such that \( (a_i, j) = 1 \), hence \( p \mid a_j / (a_i, a_j) \), so \( a_j / (a_i, a_j) > p \).
From now on we will only consider sequences for which
\[ \max_{i,j} \{a_i(a_i, a_j)\} \leq n. \]

**Lemma 1.** If g.c.d. \(\{a_1, a_2, \ldots, a_n\} = 1\), then \(\max_{i,j} \{a_i(a_i, a_j)\} < n\) and \(p\) is a prime with \(p \mid a_i\), for some \(i\), then \(p < n\).

**Proof.** Since g.c.d. \(\{a_1, a_2, \ldots, a_n\} = 1\) and \(p \mid a_i\), there exists an \(a_j\) such that \(p \mid a_j\). Hence \(a_i(a_i, a_j) \geq p\). But by hypothesis the maximum of the ratios \(a_i(a_i, a_j)\) is \(n\), hence we have \(p < n\).

**Lemma 2.** If g.c.d. \(\{a_1, a_2, \ldots, a_n\} = 1\) and \(\max_{i,j} \{a_i(a_i, a_j)\} < n\), then \(a_iM_n\) for all \(i\).

**Proof.** Let \(M_n = p_1^{k_1} \cdots p_t^{k_t}\) and assume \(p_t^{k_t+1} \mid a_i\). Then there exists \(a_j\) such that \((a_i, p_t) = 1\). Hence
\[ p_t^{k_t+1} \mid a_j(a_j, a_k) \]

But this says that the ratio is larger than \(n\). (Recall that since \(M_n = \text{l.c.m.}(1, 2, \ldots, n)\) then if \(p_t^{k_t} \leq n\), \(p_t^{k_t+1} > n\) we must have \(p_t \mid \text{l.c.m.}(1, 2, \ldots, n) \).

**Lemma 3.** If \(a_i = p_t^{k_t} = M_n/n\) and \(\max_{i,j} \{a_i(a_i, a_j)\} < n\) with g.c.d. \((a_1, \ldots, a_n) = 1\), then \(a_i = p_t^{k_t}\) for all \(i\).

**Proof.** We have \(a_i = M_n/n\), \(a_i = \text{l.c.m.}(1, 2, \ldots, n)\). Assume \((a_i, n) = d 
eq 1\). Then there exists a prime \(p_2\) such that \(p_2 \mid a_i\). Hence \(a_i = p_2^{k_2}\). But this says that \(a_i = p_2^{k_2}\), hence \(a_i = p_2^{k_2}\) for all \(i\).

**Corollary.** If g.c.d. \(\{a_1, a_2, \ldots, a_n\} = 1\) and \(\max_{i,j} \{a_i(a_i, a_j)\} < n\) then \(a_i = p_t^{k_t}\) for all \(i\).

**Proof.** Since \(\max_{i,j} \{a_i(a_i, a_j)\} < n\), we have that \(a_i = M_n/n\), where \(c_1 < c_2 < \ldots < c_t\). If \(c_t > b^{k_t}\), then \(M_n/c_t > M_n/(n-i-1)\), so \(n-(i-1) > c_t\). So we have \(n-i-1 > c_t > c_{i+1} > \ldots > c_t\). Hence
\[ \{c_1, c_{i+1}, \ldots, c_t\} = \{1, 2, \ldots, n-i\}. \]

But \(\{c_1, c_{i+1}, \ldots, c_t\} = n-(i-1) > n-i \in \{1, 2, \ldots, n-i\}\), and we have a contradiction.

**Theorem 4.** Conjecture II is true for \(n = p\), \(p\) a prime.

**Proof.** We may assume that g.c.d. \(\{a_1, a_2, \ldots, a_n\} = 1\). Since \(a_i(a_i, a_j) = p_j\), we have that \(a_i < p_j\). If \(a_i \neq p_j\), for all \(i, j\), consider \(a_i = a_i(a_i, p)\). Then \(\{a_1, \ldots, a_n\} = p\). Furthermore, since \(p^{t+1} > M_n\), we have that \((a_i, p) = 1\), so \(a_i(a_i, a_j) < p\), which contradicts Theorem 3. Hence, for some \(i, j\) we must have \(a_i = p_j\). But this implies that \(i = j = p = a_i\). Furthermore, since \(p^{t+1} > M_n\), for all \(i > 1\), then \(a_i = p_j = c_t\), with \(c_t = p > c_t > \ldots > c_1 = 1\).

Hence, \(a_i = b^{k_t}\) and \(a_i < = a_p\) is a standard sequence.

Hence, assume that \((a_t, p) = 1\), for some \(i > 1\). Then \(a_t = b^{k_t}a_t = k_t\), \(k_t < k_t < k_t < p\). Then \((a_t, a_t) = (p_t, k_t, k_t) = a_t\), so \(a_t(a_t, a_t) = p_tk_t < p\), which implies that \(k_t = 1\). So we have that \((a_t, p) = 1\), then \(a_t = k_t\).

If \(a_t = p_t = c_t\), then \(a_t(a_t, a_t) = (p_t, c_t) = a_t\).

Hence \(a_t(a_t, a_t) = k_t < p_t < p_t\), so \(k_t < p_t\), since \(k_t < p_t\).

Hence \(k_t < p_t < p_t\), so \(a_t < \ldots < a_t\) takes the form

\[
(\ast) \quad a_t < k_1 < a_t < \ldots < k_t < a_t < \ldots < p_t < p_t < p_t < p_t < p_t < p_t < p_t.
\]

If \(k_t > p_t/2\), then \(p_t > k_t > p_t/2\), so \(c_t < 2, \) then \(a_t = 1\) and \((\ast)\) becomes

\[
(\ast \ast) \quad a_t < 2a_t < 3a_t < \ldots < (p_t) < p_t < p_t < p_t < p_t < p_t.
\]

so \(a_t = 1\), since g.c.d. \(\{a_1, \ldots, a_n\} = 1\), and \((\ast \ast)\) is a standard sequence.

Assume that \(k_t < p_t/2\), that is \(\{a_t(a_t, p) = 1\} < p_t/2\). Since there is at least one \(a_t, i > 1\), such that \(a_t(p) = 1\), we have that \(p_t < k_t < a_t\), so \(c_t < p_t\), that is, the \(c_t\) must assume fewer than \(p_t/2\) values. Hence \(\{a_t(a_t, p) < p_t/2\).

But \(\{a_t, a_2, \ldots, a_p\} = \{a_t: (a_t, p) = 1\} \cup \{a_t: p(a_t)\}

and this implies that \(\{a_t, a_2, \ldots, a_p\} = p = \{a_t(a_t, p) = 1\} \cup \{a_t: p(a_t)\} < p/2 + p/2 = p\), so \(p < p\). Hence \(k_t < p_t/2\).

**Corollary.** Conjecture I is true for \(n = p+1, p\) a prime.

**Proof.** Since both conjectures are true for \(n = p, p\) a prime, Theorem 1 readily gives us the desired result.
Unités de norme $-1$ de $\mathbb{Q}(\sqrt{-p})$ et corps de classes de degré 8 de $\mathbb{Q}(\sqrt{-p})$ où $p$ est un nombre premier congru à 1 modulo 8

par

PIERRE KAPLAN (Nancy)

Introduction. Soit $p$ un nombre premier congru à 1 modulo 8. Il s'écrit:

$$p = 2e^2 - d^2 = e^2 - 32d^2. \quad (1)$$

Soit $e = e_p = S + T\sqrt{p}$ une unité de norme $-1$ du corps quadratique $\mathbb{Q}(\sqrt{p})$; les nombres $S$ et $T$ sont des entiers rationnels tels que $S^2 - T^2p = -1$, et, comme $p = 1(\text{mod} 8)$, $T$ est impair et $S$ est divisible par 4.

Soient $k_4$ le corps quadratique $\mathbb{Q}(\sqrt{-p})$, $h(-p)$ le nombre de ses classes d'idéaux. Le 2-sous-groupe des classes d'idéaux de $k_4$ est cyclique d'ordre multiple de 4,$(1)$ et on sait (cf. [2], page 402 et ci-dessous § 2) que le corps $k_8 = k_4(i, \sqrt{-e})$ est l'extension cyclique de degré 4 non ramifiée de $k_4$.

Dans un travail récent ([3]), H. Cohn et G. Cooke ont trouvé que, si $h(-p) = 0(\text{mod} 8)$, l'extension cyclique de degré 8 non ramifiée de $k_4$ le corps $k_8 = k_4(\sqrt{p}, i, \sqrt{-p}a)\sqrt{i}\sqrt{-p}(1-i)\sqrt{a}$ où $\sqrt{-p} = i\sqrt{p}$ et où les signes de $a$ et de $T$ doivent être choisis de manière que $d = -T(\text{mod} 4)$. Simultanément ils prouvent que $S$ est divisible par 8 si et seulement si, $h(-p)$ est divisible par 8, c'est-à-dire que $h(-p) = S(\text{mod} 8)$.

Dans cette note, nous donnons une démonstration considérablement plus simple de ces résultats. Nous prouvons directement la congruence $S = h(-p)(\text{mod} 8)$ à partir d'une condition pour que $h(-p)$ soit divisible par 8. Nous montrons que le corps $k_8$ est une extension cyclique de degré 8 de $k_4$ et que cette extension est non ramifiée lorsque le nombre $S$ est divisible par 8.

Notre démonstration utilise (au § 1) la théorie des formes quadratiques binaires c'est-à-dire la théorie des corps quadratiques et (au § 2)

$(1)$ Si $p = 5(\text{mod} 8)$, $h(-p) = 2(\text{mod} 4)$ et si $p = 3(\text{mod} 4)$, $h(-p)$ est impair.