[5] J. Bell and B. Slomson, *Models and Ultraproducts*, Amsterdam–London 1969.
[6] M. Deuring, *Über den Tschebotareffschen Dichtigkeitssatz*, Math. Ann. 110 (1935), pp. 414–415.
[7] L. Gillman and M. Jerison, *Rings of Continuous Functions*, Princeton 1960.
[8] L. J. Goldstein, *Analytic Number Theory*, Englewood Cliffs 1971.
[9] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper ("Zahlbericht") I, Ia*, Würzburg 1970.
[10] M. Jarden, *Elementary Statements over large algebraic fields*, Trans. Amer. Math. Soc. 164 (1972), pp. 67–91.
[11] — *On Čebotarev Sets*, Arch. Math. 25 (1974), pp. 495–497.
[12] — Lecture, held at a meeting on superprimes of algebraic number fields, Oberwolfach 1974.
[13] N. Klingen, *Zur Idealstruktur in Nichtstandardmodellen von Dedekindringen*, J. Reine Angew. Math. 274/275 (1975), pp. 38–60.
[14] S. Lang, *Algebraic Number Theory*, London 1970.
[15] C. R. MacCluer, *A reduction of the Čebotarev density theorem to the cyclic case*, Acta Arith. 15 (1968), pp. 45–47.
[16] F. K. Schmidt, *Die Theorie der Klassenkörper über einem Körper algebraischer Funktionen in einer Unbestimmten und mit endlichem Koeffizientenbereich*, Sitz.-Ber. phys. med. Soz. Erlangen 62 (1930), pp. 267–284.

Received on 24. 3. 1975 (691)

ACTA ARITHMETICA
XXXII (1977)

Some remarks on a number theoretic problem of Graham

by

WILLIAM YSLAS VÉLEZ (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, $a_i/(a_i, a_j)$ 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*

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

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 $Q = \{a_1 < a_2 < \ldots < a_n\}$, let $A =$ l.c.m. $\{a_1, a_2, \ldots, a_n\}$ and form

$$Q^{-1} = \{A/a_n < A/a_{n-1} < \ldots < A/a_1\}.$$

It is easy to show that Q and Q^{-1} have the same set of ratios.

Notation. Let $M_n =$ l.c.m. $\{1, 2, \ldots, n\}$ and $b_i^{(n)} = M_n/(n-i+1)$, so $M_n/n < M_n/(n-1) < \ldots < M_n/2 < M_n/1$ 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 $\{b_1^{(n)} < b_2^{(n)} < \ldots \ldots < b_n^{(n)}\}$. That is, either

$$a_i = ki \quad \text{for all } i,$$

or

$$a_i = kb_i^{(n)} \quad \text{for all } i.$$

Graham also made the following conjecture.

CONJECTURE II. *Assume*

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

Then the sequence is a standard sequence except for $n = 4$, where we have the additional sequence $\{2 < 3 < 4 < 6\}$.

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

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

$$\max_{i,j}\{a_i/(a_i, a_j),\, b/(a_i, b),\, a_i/(a_i, b)\} > n+1,$$

except possibly when $n = 4$.

For $n = 4$ we have the only exception to the assertion of the theorem, namely, $Q = \{2\cdot 1 < 2\cdot 2 < 2\cdot 3\}$, $b = 3$, i.e., $\{2 < 3 < 4 < 6\}$.

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

Assume $a_i = k'\cdot b_i^{(n)}$. Let $a = \text{l.c.m.}\,\{a_1, a_2, \ldots, a_n, b\}$ and form the new sequence

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

Hence we have the new sequence

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

We will prove the theorem for this sequence.

We assume that Q' is not a standard sequence.

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

Hence, we may assume that $k > 1$.

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

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

If $b' = n$, then $k(n-1)/\big(k(n-1), b'\big) = k(n-1) > n+1$ for $k > 2$ or $n > 3$. If $k = 2$, $n = 3$, then $2(3-1) = 3+1$ and this gives the sequence $\{2 < 4 < 6,\, b' = 3\}$.

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 Q' and

$$k(b'+1)/\big(k(b'+1), b'\big) = k(b'+1).$$

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

If not, then $kb'+1 < kb'+k \leqslant n+1$. Define l by

$$k(k^{l+1}b'+1) > n+1,$$
$$k(k^l b'+1) \leqslant n+1.$$

Then $l \geqslant 0$ and we have that $k^{l+1}b'+1 < k^{l+1}b'+k \leqslant n+1$, so $k^{l+1}b'+1 \leqslant n$; $k(k^{l+1}b'+1)$ appears somewhere in the sequence Q', and

$$k(k^{l+1}b'+1)/\big(k(k^{l+1}b'+1), b'\big) = k(k^{l+1}b'+1) > n+1. \blacksquare$$

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

$$\max_{1\leqslant i,j\leqslant n} \{a_i/(a_i, a_j)\} \geqslant n.$$

If $\max\limits_{1\leqslant i,j\leqslant n} \{a_i/(a_i, a_j)\} > n$, then

$$\max_{1\leqslant i,j\leqslant n+1} \{a_i/(a_., a_j)\} \geqslant n+1.$$

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

$$\max_{1\leqslant i,j\leqslant n+1} \{a_i/(a_i, a_j)\} \geqslant n+1. \blacksquare$$

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 $a_i \equiv a_j \not\equiv 0 \pmod p$, $i > j$, then $a_i = a_j + p\cdot r$. Let $d = (a_i, a_j)$, then $d \mid (a_i - a_j)$, so $d \mid pr$, but $(d, p) = 1$, so $d \mid r$. So we have that

$$a_i/(a_i, a_j) = (a_j + pr)/d = a_j/d + (pr)/d > p.$$

So we have that if two of the a_i are congruent modulo p to a unit, then $\max\limits_{i,j}\{a_i/(a_i, a_j)\} > p$.

Assume that $a_i \not\equiv a_j \pmod p$, if $a_i \not\equiv 0 \pmod p$, $a_j \not\equiv 0 \pmod p$. 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 $(a_j, p) = 1$, hence $p \mid a_i/(a_i, a_j)$, so $a_i/(a_i, a_j) \geqslant p$. $\blacksquare$

From now on we will only consider sequences for which

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

LEMMA 1. *If* g.c.d. $(a_1, a_2, \ldots, a_n) = 1$, $\max\limits_{i,j}\{a_i/(a_i, a_j)\} \leqslant n$ *and* p *is a prime with* $p \mid a_i$, *for some* i, *then* $p \leqslant n$.

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 $p \nmid a_j$. Hence $a_i/(a_i, a_j) \geqslant p$. But by hypothesis the maximum of the ratios $a_i/(a_i, a_j)$ is $\leqslant n$, hence we have $p \leqslant n$. ■

LEMMA 2. *If* g.c.d. $(a_1, a_2, \ldots, a_n) = 1$ *and* $\max\limits_{i,j}\{a_i/(a_i, a_j)\} \leqslant n$, *then* $a_i \mid M_n$, *for all* i.

Proof. Let $M_n = p_1^{l_1} \ldots p_s^{l_s}$ and assume $p_i^{l_i+1} \mid a_k$. Then there exists a_j such that $(a_j, p_i) = 1$. Hence

$$p_i^{l_i+1} \mid a_k/(a_j, a_k).$$

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 $p_i^{l_i} \leqslant n$, $p_i^{l_i+1} > n$, we must have $p_i^{l_i} \mid M_n$ and $p_i^{l_i+1} \nmid M_n$). We now see that if the maximum of the ratios is $\leqslant n$, then each element of the sequence divides M_n. ■

LEMMA 3. *If* $a_1 = b_1^{(n)} = M_n/n$ *and* $\max\limits_{i,j}\{a_i/(a_i, a_j)\} \leqslant n$ *with* g.c.d. $(a_1, \ldots, a_n) = 1$, *then* $a_i = b_i^{(n)}$ *for all* i.

Proof. We have $a_1 = M_n/n$, $a_k = j_k a_1/i_k$, $(i_k, j_k) = 1$, $i_k < j_k \leqslant n$. Assume $(j_k, n) = d \neq j_k$. Then there exists a prime $p = p_1$ such that $p_1 \mid j_k$, $p_1 \nmid n$. Thus, since $p_1^{l_1} \mid a_1$ and $(i_k, j_k) = 1$ we have $p_1^{l_1+1} \mid a_k$ which contradicts Lemma 2. Hence, $j_k \mid n$ so that

$$a_k = n a_1/d_k, \quad 1 \leqslant d_k \leqslant n.$$

But the a_k are increasing and there are exactly n of them. Hence, this says $d_1 = n$, $d_2 = n-1, \ldots, d_n = 1$, i.e.,

$$a_k = n a_1/(n-k+1) = M_n/(n-k+1). \ ■$$

COROLLARY. *If* g.c.d. $(a_1, \ldots, a_n) = 1$ *and* $\max\limits_{i,j}\{a_i/(a_i, a_j)\} \leqslant n$, *then* $a_i \leqslant b_i^{(n)}$, *for all* i.

Proof. Since $\max\limits_{i,j}\{a_i/(a_i, a_j)\} \leqslant n$, we have that $a_i = M_n/c_i$, where $c_1 > c_2 > \ldots > c_n$. If $a_i > b_i^{(n)}$, then $M_n/c_i > M_n/(n-(i-1))$, so $n-(i-1) > c_i$. So we have $n-(i-1) > c_i > c_{i+1} > \ldots > c_n$. Hence

$$\{c_i, c_{i+1}, \ldots, c_n\} \subset \{1, 2, \ldots, n-i\}.$$

But $|\{c_i, c_{i+1}, \ldots, c_n\}| = n-(i-1) > n-i = |\{1, 2, \ldots, n-i\}|$, 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. $(a_1, a_2, \ldots, a_p) = 1$. Since $a_i/(a_i, a_j) \leqslant p$, we have that $a_i \leqslant p a_j$. If $a_i \neq p a_j$, for all i, j, consider $a_i' = a_i/(a_i, p)$. Then $|\{a_1', \ldots, a_p'\}| = p$. Furthermore, since $p^2 \nmid M_p$, where M_p is l.c.m. $\{1, 2, \ldots, p\}$, we have that $(a_i', p) = 1$, so $\max\limits_{i,j}\{a_i'/(a_i', a_j')\} < p$, which contradicts Theorem 3. Hence, for some i, j we must have $a_i = p a_j$. But this implies that $i = 1$, $j = p$ and $a_p = p a_1$. Furthermore, since $p^2 \nmid M_p$, $p \nmid a_1$.

If $p \mid a_i$, for all $i > 1$, then $a_i = p a_1/c_i$, with $c_1 = p > c_2 > \ldots > c_p = 1$. Hence, $a_i = b_i^{(n)}$ and $a_1 < \ldots < a_p$ is a standard sequence.

Hence, assume that $(a_i, p) = 1$, for some $i > 1$. Then $a_i = k_1 a_1/k_2$, $(k_1, k_2) = 1$, $k_2 \mid a_1$, $k_2 < k_1 < p$. Then $(a_p, a_i) = (p a_1, k_1 a_1/k_2) = a_1/k_2$, so $a_p/(a_i, a_p) = p k_2 \leqslant p$, which implies that $k_2 = 1$. So we have that if $(a_i, p) = 1$, then $a_i = k_i a_1$.

If $a_j = p a_1/c$, $(c, p) = 1$, then $(a_j, a_i) = (p \cdot a_1/c, k_i c \cdot a_1/c) = a_1/c$. Hence $a_i/(a_i, a_j) = k_i a_1/(a_1/c) = k_i c \leqslant p$, so $k_i < p/c$, since $(k_i c, p) = 1$. Hence $k_i a_1 < p a_1/c$, so $a_i < a_j$. That is, the sequence $a_1 < \ldots < a_p$ takes the form

$$(*) \qquad a_1 < k_1 a_1 < \ldots < k_l a_1 < p a_1/c_1 < \ldots < p a_1/c_r < p a_1/1.$$

If $k_l > p/2$, then $p/c_1 > k_l > p/2$, so $c_1 < 2$, that is $c_1 = 1$ and $(*)$ becomes

$$(**) \qquad a_1 < 2a_1 < 3a_1 < \ldots < (p-1) a_1 < p a_1,$$

so $a_1 = 1$, since g.c.d. $(a_1, \ldots, a_p) = 1$, and $(**)$ is a standard sequence.

Assume that $k_l < p/2$, that is, $|\{a_i\colon (a_i, p) = 1\}| < p/2$. Since there is at least one a_i, $i > 1$, such that $(a_i, p) = 1$, we have that $p/c_1 > k_l \geqslant 2$, so $c_1 < p/2$, that is, the c_i must assume fewer than $p/2$ values. Hence $|\{a_i\colon p \mid a_i\}| < p/2$. But

$$\{a_1, a_2, \ldots, a_p\} = \{a_i\colon (a_i, p) = 1\} \cup \{a_i\colon p \mid a_i\}$$

and this implies that

$$|\{a_1, \ldots, a_p\}| = p = |\{a_i\colon (a_i, p) = 1\}| + |\{a_i\colon p \mid a_i\}| < p/2 + p/2 = p,$$

so $p < p$. Hence $k_l \not< p/2$. ■

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. ■

Remark. If g.c.d. $(a_1, \ldots, a_n) = 1$, then for each n, Conjecture I holds for all but a finite number of sequences $\{a_1 < a_2 < \ldots < a_n\}$, since by Lemma 2, all counterexamples must have $a_i | \text{l.c.m.}\{1, 2, \ldots, n\}$.

References

[1] R. L. Graham, Personal communication.
[2] J. Marica and J. Schönheim, *Differences of sets and a problem of Graham*, Canad. Math. Bull. 12 (5) (1969), pp. 635–637.
[3] E. Szemerédi, Oral Communication.
[4] Riko 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.

Received on 10. 6. 1975 (725)

ACTA ARITHMETICA
XXXII (1977)

Unités de norme −1 de $Q(\sqrt{p})$ et corps de classes de degré 8 de $Q(\sqrt{-p})$ 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:

$$p = 2e^2 - d^2 = e'^2 - 32d'^2. \tag{1}$$

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

Soient k_2 le corps quadratique $Q(\sqrt{-p})$, $h(-p)$ le nombre de ses classes d'idéaux. Le 2-sous-groupe des classes d'idéaux de k_2 est cyclique d'ordre multiple de 4([1]) et on sait (cf. [2], page 402 et ci-dessous § 2) que le corps $k_8 = k_2(i, \sqrt{\varepsilon})$ est l'extension cyclique de degré 4 non ramifiée de k_2.

Dans un travail récent ([3]), H. Cohn et G. Cooke ont trouvé que, si $h(-p) \equiv 0 \pmod 8$, l'extension cyclique de degré 8 non ramifiée de k_2 est le corps $k_{16} = k_8\left(\sqrt{(d+\sqrt{-p})(1-i)\sqrt{\varepsilon}}\right)$ où $\sqrt{-p} = i\sqrt{p}$ et où les signes de d et de T doivent être choisis de manière que $d \equiv -T \pmod 4$. Simultanément ils prouvent que S est divisible par 8 si et seulement si, $h(-p)$ est divisible par 8, c'est-à-dire que $h(-p) \equiv S \pmod 8$.

Dans cette note, nous donnons une démonstration considérablement plus simple de ces résultats. Nous prouvons directement la congruence $S \equiv h(-p) \pmod 8$ à partir d'une condition pour que $h(-p)$ soit divisible par 8. Puis nous montrons que le corps k_{16} est une extension cyclique de degré 8 de k_2 et que cette extension est non ramifiée quand 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 $p \equiv 5 \pmod 8$, $h(-p) \equiv 2 \pmod 4$ et si $p \equiv 3 \pmod 4$, $h(-p)$ est impair.