Soit η_0 une unité fondamentale positive de K.

$$\alpha_2^{(k)} = \eta_0^{u_2}\frac{\zeta_i}{\zeta_j}, \qquad \alpha_1^{(k)} = \eta_0^{u_1}\frac{\zeta_h}{\zeta_j}$$

où i, j, h sont des fonctions de k dans $[1, N]$ et u_1, u_2 des entiers dépendants de k.

Les relations (IV.11) permettent de borner les entiers u_2 et u_1. Alors $\alpha_1^{(k)}$ et $\alpha_2^{(k)}$ ne prennent qu'un nombre fini de valeurs.

Références

[1] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer Verlag, 1959.

[2] H. Minkowski, *Zur Theorie der Kettenbrüche*, Gesammelte Abhandlugen, Vol. I, Teubner, Leipzig 1911, p. 278–292.

[3] O. Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithm*, Math. Ann. 64 (1907), p. 1–76.

[4] W. M. Schmidt, *On simultaneous approximation of two algebraic numbers by rationals*, Acta Math. 119 (1967), p. 27–50.

[5] G. Szekeres, *Multidimensional continued fractions*, Ann. Univ. Sci. Budapest, Eötvos Sect. Math. 13 (1970), p. 113–140.

[6] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Transl. of Math. Monograph, vol. 10, 1964.

Reçu le 19.1.1979
et dans la forme modifiée le 7.6.1979 (1130)

ACTA ARITHMETICA
XL (1982)

On a conjecture of R. L. Graham

by

R. J. Simpson (Adelaide, S. A., Australia)

Graham [2] has conjectured that if $a_1, a_2, \ldots, a_n$ is any increasing sequence of positive integers, then

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

Various necessary conditions have been established for a sequence that falsifies the conjecture. Among these are the following:

(1) Not all the a_i are square free (Marica and Schönheim [3]).

(2) n is not a prime (Szemeredi [2]).

(3) $n-1$ is not a prime (Vélez [4]).

(4) If p is a prime, and $p|a_i$ for some i, then $p \leqslant (n-1)/2$ (Boyle [1]).

(5) If any a_i is a prime p then $p = (a_j + a_k)/2$ for some j, k (Weinstein [5]).

In this note we improve (5) by showing:

THEOREM. *If $a_1, a_2, \ldots, a_n$ is a sequence that falsifies the conjecture, then no a_i is a prime.*

Proof. The proof is by contradiction. We assume the opposite and separate the sequence in two sets: (i) those integers less than n and (ii) those which are greater than or equal to n.

By (4), p is a member of the first set. It is clear that p must divide each member of the second.

Let $k = \left[\dfrac{n-1}{p}\right]$, where square brackets denote integer part, let $B = \{b_i\}$ be the set of positive integers which are relatively prime to p and less than n, and let $C = \{c_i\}$ be the set of integers greater than k and less than n. Note that the number of elements of B and the number of elements of C are both equal to $n-k-1$. There are k positive integers less than n and divisible by p.

The integers in set (ii) above are of the form $c_j p$. We will show that for each b_i that is a member of the sequence, there corresponds a unique $c_j p$ that cannot be a member. It will follow that there are at most $n-1$ numbers a_i in the sequence, which is a contradiction.

Assume that b_i is a member of the sequence. Let m be the smallest integer such that

$$p(p^m b_i - 1) \geqslant n. \tag{6}$$

Then

$$\frac{p(p^m b_i - 1)}{(b_i, p(p^m b_i - 1))} = p(p^m b_i - 1) \geqslant n.$$

Thus $p(p^m b_i - 1)$ cannot be a member of the sequence. Furthermore, no two $c_j p$'s of this form can be equal, for if $p(p^m b_i - 1) = p(p^c b_j - 1)$, $b_i \neq b_j$

$$p^m b_i = p^c b_j. \tag{7}$$

So $p|b_i$ or $p|b_j$, which contradicts the definition of the b_i.

We next show that for all but at most one b_i, $p^m b_i - 1$ is less than n and thus an element of C.

If $p^m b_i - 1 \geqslant n$ and $p(p^{m-1} b_i - 1) < n$ then

$$n < p^m b_i < n + p \tag{8}$$

or

$$\frac{n}{p} < p^{m-1} b_i < \frac{n}{p} + 1. \tag{9}$$

There can be only one integer that satisfies this inequality. By the reasoning used after equation (7) it can be satisfied by only one b_i.

We have now paired all but at most one of the elements of B with elements of C. If an element of C is still unaccounted for it must equal $n-1$. For if $n-1$ had already been excluded we would have

$$(n-1)p = p(b_i p^m - 1) \quad \text{for some } i \text{ and } m.$$

So $n = b_i p^m$, and p divides n, but if this is so there can be no b_i satisfying (9).

We finally show that if b_h is the single remaining element of B, then

$$\frac{(n-1)p}{(b_h, (n-1)p)} \geqslant n.$$

Let $(b_h, n-1) = q$, $b_h = b_0 q$, and $n-1 = n_0 q$. Putting these values in (8) we get,

$$n_0 q + 1 < p^m b_0 q \leqslant n_0 q + p, \qquad n_0 + 1/q < p^m b_0 \leqslant n_0 + p/q.$$

But $p^m b_0$ is an integer, so $p/q \geqslant 1$. Equality is impossible since this would imply $p|b_h$. Therefore

$$\frac{(n-1)p}{(b_h, (n-1)p)} = \frac{(n-1)p}{q} > n-1.$$

Thus b_h and $p(n-1)$ cannot both be members of the sequence.

For every b_i that is a member of the sequence there corresponds a number $c_j p$ that is not a member. Thus the members of the sequence must come from the k multiples of p less than n, and a single member of each of the $n-1-k$ pairs of incompatible elements of B and C. This allows at most $n-1$ integers in the sequence, which is a contradiction. This completes the proof.

References

[1] R. D. Boyle, *On a problem of R. L. Graham*, Acta Arith. 34 (1978), pp. 163–177.

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

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

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

[5] Gerald Weinstein, *On a conjecture of Graham concerning greatest common divisors*, Proc. Amer. Math. Soc. 63 (1977), pp. 33–38.

Received on 22.3.1979 (1148)