ACTA ARITHMETICA
XXX (1976)

On additive bases

by

J. M. DESHOUILLERS (Talence),
P. ERDÖS and A. SÁRKÖZI (Budapest)

1. Let $A = \{a_1, a_2, \ldots\}$ (where $a_1 = 0 < a_2 < \ldots < a_n < \ldots$) be an infinite sequence of non-negative integers. The sequence of numbers, which can be written in the form $a_{i_1} + a_{i_2} + \ldots + a_{i_h}$, is denoted by hA (for $h = 1, 2, \ldots$). Furthermore, let $A^k = \{a_1^k, a_2^k, \ldots, a_n^k, \ldots\}$ (for $k = 1, 2, \ldots$).

If there exists a number k such that

$$kA = \{0, 1, 2, \ldots, n, \ldots\} \tag{1}$$

holds then A is called a *basis* (more exactly: an additive basis of finite order), and the least k, satisfying (1), is called the *order* of the basis A.

F. Dress raised the problem whether there existed sequences B, C such that B is a basis but B^2 is not a basis, while on the other hand, C is not a basis but C^2 is a basis?

The purpose of this paper is to construct such sequences B, C.

In the second section, we shall give two lemmas implying that a sequence is not a basis; it should be noticed that the basic idea of the two criteria is the same one: if a sequence A is such that for some irrational number α (resp. for an infinity of convenient rationals α) the sequence $\alpha A = \{\alpha a_1, \alpha a_2, \ldots\}$ is badly distributed mod 1, then A is not a basis. Note that one can find a larger list of similar criteria in Stöhr [3].

Both criteria may be used to construct sequences B and C with the required properties, but we shall use the "analytic" criterion (Lemma 2) in the third section, in order to construct the sequence B since it gives a fairly explicit result, and the "arithmetic" criterion (Lemma 1) in the fourth section since the construction of the sequence C is altogether elementary.

For a real number θ, we shall write: $e(\theta) = \exp(2i\pi\theta)$, $\{\theta\}$ for the fractional part of θ, and $\|\theta\| = \inf(\{\theta\}, 1-\{\theta\})$.

One more notation:

Let a, m be integers, $m > 0$. The integer r, uniquely determined by the conditions

$$a \equiv r \pmod{m},$$
$$\left[\frac{m}{2}\right] - m < r \leqslant \left[\frac{m}{2}\right]$$

(i.e. the absolute least residue of r modulo m), will be denoted by $r(a, m)$. Clearly, for any non-negative integer a and any positive integer m

(2) $$|r(a, m)| \leqslant a \quad \text{for} \quad a \geqslant 0$$

holds, furthermore, for any integers a, b, m $(m > 0)$,

(3) $$|r(a \pm b, m)| \leqslant |r(a, m)| + |r(b, m)|$$

and

(4) $$|r(a-b, m)| \geqslant |r(a, m)| - |r(b, m)|.$$

The last definition: let A be a sequence of non-negative integers, m be a positive integer, n, ε be non-negative real numbers. A is said to have property $P(n, \varepsilon, m)$ if $a \in A$, $a \geqslant n$ imply that $|r(a, m)| < \varepsilon m$.

2. In this section, we are going to prove two lemmas that we need in the construction of both sequences B and C.

LEMMA 1. *Let A be a given sequence of non-negative integers. Let us suppose that there exists an infinite sequence $p_1 < p_2 < \ldots < p_k < \ldots$ of natural numbers greater than one, and an infinite sequence $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \ldots$ of positive real numbers with*

(5) $$\lim_{k \to +\infty} \varepsilon_k = 0$$

such that, for some infinite sequence $n_1, n_2, \ldots, n_k, \ldots$ of non-negative real numbers, A has property $P(n_k, \varepsilon_k, p_k)$ for $k = 1, 2, \ldots$ Then A is not a basis.

Proof. Let us argue indirectly and suppose that there exists a positive integer l for which

(6) $$lA = \{0, 1, 2, \ldots, n, \ldots\}.$$

By (5), clearly, there exists a subsequence $p_{i_1} < p_{i_2} < \ldots < p_{i_{l+1}}$ of the sequence $p_1, p_2, \ldots, p_k, \ldots$ such that

(7) $$\varepsilon_{i_j} < \frac{1}{8l} \quad \text{for} \quad j = 1, 2, \ldots, l+1$$

and

(8) $$\frac{p_{i_{j+1}}}{8l} > \max\{n_{i_1}, n_{i_2}, \ldots, n_{i_j}\} \quad \text{for} \quad j = 1, 2, \ldots, l.$$

(To find such a subsequence $p_{i_1}, p_{i_2}, \ldots, p_{i_{l+1}}$, all we have to do is to choose i_{j+1} to be sufficiently large depending on $i_1, i_2, \ldots, i_j$, after beginning with an arbitrary i_1 such that $\varepsilon_{i_1} < 1/8l$.)

Let m be any integer satisfying

(9) $$|r(m, p_{i_j})| = \left[\frac{p_{i_j}}{2}\right] \quad \text{for} \quad j = 1, 2, \ldots, l+1.$$

(6) implies the existence of integers $a_{t_1}, a_{t_2}, \ldots, a_{t_l}$ such that

(10) $$m = a_{t_1} + a_{t_2} + \ldots + a_{t_l} \quad \text{and} \quad a_{t_j} \in A \quad \text{for} \quad j = 1, 2, \ldots, l.$$

We may suppose that

(11) $$a_{t_1} \geqslant a_{t_2} \geqslant \ldots \geqslant a_{t_l}.$$

We shall prove by induction that, for $j = 0, 1, 2, \ldots, l$,

(12) $$m - \sum_{\nu=1}^{j} a_{t_\nu} > \frac{p_{i_{l-j+1}}}{8}.$$

In this way, we obtain a contradiction. Namely, the difference on the left-hand side of (12) is positive also for $j = l$ by (12), while, on the other hand, the same difference must be equal to 0 by (10). Thus to complete the proof, we have to prove (12).

For $j = 0$, (12) asserts that

$$m > \frac{p_{i_{l+1}}}{8}.$$

Indeed, by (2) and (9),

$$m \geqslant |r(m, p_{i_{l+1}})| = \left[\frac{p_{i_{l+1}}}{2}\right] > \frac{p_{i_{l+1}}}{4} > \frac{p_{i_{l+1}}}{8}.$$

Let us suppose now that (12) holds for some j $(0 \leqslant j \leqslant l-1)$; we have to show that this implies that (12) holds also for $j+1$, i.e.

(13) $$m - \sum_{\nu=1}^{j+1} a_{t_\nu} > \frac{p_{i_{l-j}}}{8}.$$

(10) and (12) imply that

$$\sum_{\nu=j+1}^{l} a_{t_\nu} = m - \sum_{\nu=1}^{j} a_{t_\nu} > \frac{p_{i_{l-j+1}}}{8}.$$

Thus, by (11),

$$a_{t_{j+1}} = \max_{\nu=j+1,\dots,l} a_{t_\nu} \geqslant \frac{\sum_{\nu=j+1}^{l} a_{t_\nu}}{l-j} > \frac{p_{i_{l-j+1}}}{8(l-j)} \geqslant \frac{p_{i_{l-j+1}}}{8l}. \tag{14}$$

(8), (11) and (14) give that

$$a_{t_1} \geqslant a_{t_2} \geqslant \dots \geqslant a_{t_{j+1}} > \frac{p_{i_{l-j+1}}}{8l} > n_{i_{l-j}}. \tag{15}$$

By our assumption, A has property $P(n_{i_{l-j}}, \varepsilon_{i_{l-j}}, p_{i_{l-j}})$; thus (7) and (15) imply that

$$|r(a_{t_\nu}, p_{i_{l-j}})| \leqslant \varepsilon_{i_{l-j}} p_{i_{l-j}} < \frac{p_{i_{l-j}}}{8l}, \quad \nu = 1, \dots, j-1. \tag{16}$$

We obtain from (2), (3), (4), (9), (10) and (16) that

$$m - \sum_{\nu=1}^{j+1} a_{t_\nu} \geqslant \Big| r\Big(m - \sum_{\nu=1}^{j+1} a_{t_\nu}, p_{i_{l-j}}\Big)\Big|$$

$$\geqslant |r(m, p_{i_{l-j}})| - \sum_{\nu=1}^{j+1} |r(a_{t_\nu}, p_{i_{l-j}})| > \left[\frac{p_{i_{l-j}}}{2}\right] - (j+1)\frac{p_{i_{l-j}}}{8l}$$

$$> \frac{p_{i_{l-j}}}{4} - l\frac{p_{i_{l-j}}}{8l} = \frac{p_{i_{l-j}}}{8}.$$

Thus (13) and also Lemma 1 is proved.

LEMMA 2. *Let A be a sequence of non-negative integers, and let us suppose that there exists an irrational number α such that the set of the fractional parts of the elements αa (where a belongs to A) has only a finite number of limit points.*

Then A is not a basis.

Proof. Let $x_1, x_2, \dots, x_k$ be the set of limit points of the set of the fractional parts of the αa's, and let ε be a positive real number; we write:

$$A'_\varepsilon = \{a \in A \mid \forall j \in [1, k]: \|\alpha a - x_j\| > \varepsilon\}, \tag{17}$$

$$A_{\varepsilon,j} = \{a \in A \mid \|\alpha a - x_j\| \leqslant \varepsilon\} \quad \text{for} \quad j = 1, \dots, k, \tag{18}$$

$$A_\varepsilon = \bigcup_1^k A_j. \tag{19}$$

(i) By (17), (18) and (19) it is clear that A is the union of A'_ε and A_ε. By hypothesis, A'_ε is a finite set, and the sequence A_ε has upper asymptotic density

$$\bar{d}A_\varepsilon = \limsup_{N\to\infty} {}^{\#}\{a \leqslant N \mid a \in A_\varepsilon\}/N$$

which does not exceed $2\varepsilon k$, because the sequence $(\alpha n)_{n\in N}$ is equidistributed mod 1. This is true for all ε, so that

$$\bar{d}A = 0.$$

(ii) Suppose now that, for some positive integer h, $\bar{d}hA = 0$. Clearly, we have

$$(h+1)A = (A'_\varepsilon + hA) \cup (h+1)A_\varepsilon. \tag{20}$$

The sequence $A'_\varepsilon + hA$ is a finite union of sequences which are obtained by translating hA, and so we have

$$\bar{d}(A'_\varepsilon + hA) = 0. \tag{21}$$

Let E_h be the set of the fractional parts of all the sums $x_{i_1} + \dots + x_{i_{h+1}}$; E_h is a finite set with at most $k^{(h+1)}$ elements. The sequence $(h+1)A_\varepsilon$ is included in the set of the integers m for which there exists a x in E_k such that:

$$\|\alpha m - x\| \leqslant (h+1)\varepsilon.$$

From the equidistribution mod 1 of the sequence $(\alpha m)_{m\in N}$, we get

$$\bar{d}\big((h+1)A_\varepsilon\big) \leqslant 2k^{(h+1)}(h+1)\varepsilon. \tag{22}$$

From (20), (21) and (22) we deduce:

$$\bar{d}\big((h+1)A\big) \leqslant 2k^{(h+1)}(h+1)\varepsilon. \tag{23}$$

Since (23) is true for all ε, $\bar{d}\big((h+1)A\big)$ equals 0.

(iii) By induction, we see that for every positive in teger h, the se quence hA has a zero upper asymptotic density, and so A cannot be a basis.

(Note that we shall use only a special case of this lemma, where $k = 1$ and $x_1 = 0$, i.e. $\lim_{\substack{a\in A\\ a\to\infty}} \{\alpha a\} = 0$.)

3. In this section, we shall construct a sequence B having the desired properties. From now on, we write $\varrho = (1+\sqrt{5})/2$. We need two more lemmas:

LEMMA 3. *Let P be a positive integer, h a rational integer with absolute value less than $0.75P^{1/2}$, u and v two arbitrary integers and α a real number; we have:*

$$\Big|\sum_{n=1}^{P} e(\varrho h n^2 + \alpha n)\Big| \leqslant 7P^{1/2}(1+|h|^{1/2}) \tag{24}$$

and

$$\Big|\sum_{n_1=u+1}^{u+P} \sum_{n_2=v+1}^{v+P} e(2\varrho h n_1 n_2)\Big| \leqslant 7P^{3/2}(1+|h|^{1/2}). \tag{25}$$

Proof. (24) is obtained by combining the so-called fundamental inequality of van der Corput (cf. [1]), and Lemma 8a of Vinogradov (cf. [4], p. 24).

(25) is a trivial corollary of Lemma 10b of Vinogradov (cf. [4], p. 29).

LEMMA 4 (J. F. Koksma, cf. [2]). *Let a and b be two positive integers ($a < b$), and θ a positive real number not exceeding 1, M an integer greater than 200, f_1, f_2, f_3 three functions from $[a, b[\times[a, b[$ into $\mathbf{R}$; we write:*

$$S = S(a, b, \theta) = \#\{(n_1, n_2) |\ a \leqslant n_i < b,\ \{f_j(n_1, n_2)\} \leqslant \theta\ (j = 1, 2, 3)\},$$

$$p_h = \begin{cases} 30\,|h^{-1}| & \text{if} \quad h \neq 0, \\ 2 & \text{if} \quad h = 0, \end{cases}$$

$$T = \sum_{h_1, h_2, h_3}' \Big| \sum_{n_1=a}^{b-1} \sum_{n_2=a}^{b-1} e\Big(\sum_{j=1}^{3} h_j f_j(n_1, n_2)\Big)\Big|\, p_{h_1} p_{h_2} p_{h_3},$$

where the first summation is taken over the triples (h_1, h_2, h_3) such that:

$$0 \leqslant |h_j| \leqslant M \quad (j = 1, 2, 3) \quad \text{and} \quad h_1^2 + h_2^2 + h_3^2 \neq 0.$$

We have

(26) $$|S - \theta^3 (b-a)^2| \leqslant T + (b-a)^2 \frac{1200}{M}.$$

We are now in a position to prove

THEOREM 1. *Let*

$$B = \{n \in \mathbf{N} |\ \{\varrho n^2\} \leqslant 193 n^{-1/12}\}, \quad \text{where} \quad \varrho = (1+\sqrt{5})/2;$$

the sequence B is a basis of order at most 3, whereas B^2 is not a basis.

Proof. It is clear from Lemma 2 and from the definition of B that B^2 is not a basis.

Remark first that all the integers which are less than 3.193^{12} are in $3B$; thus it suffices to prove that any integer N greater than 2.160^{12} is in $3B$. Let

(27) $$\theta = 193 N^{-1/12}$$

and

(28) $$P = [N/2].$$

It suffices to show that there exist two integers n_1 and n_2 satisfying the conditions:

$$1 \leqslant n_1 \leqslant P, \quad 1 \leqslant n_2 \leqslant P,$$
$$\{\varrho n_1^2\} \leqslant \theta, \quad \{\varrho n_2^2\} \leqslant \theta, \quad \{\varrho (N - n_1 - n_2)^2\} \leqslant \theta,$$

since then n_1, n_2 and $N - n_1 - n_2$ are elements of B.

We shall use Lemma 4 with the following notations:

$$a := 1, \quad b := P+1, \quad M := [P^{1/4}],$$
$$f_1(n_1, n_2) := \varrho n_1^2, \quad f_2(n_1, n_2) := \varrho n_2^2, \quad f_3(n_1, n_2) := \varrho (N - n_1 - n_2)^2$$

We have to evaluate the sums

(29) $$U(h_1, h_2, h_3) = \Big| \sum_{n_1=1}^{P} \sum_{n_2=1}^{P} e\big(\varrho (h_1 n_1^2 + h_2 n_2^2 + h_3 (N - n_1 - n_2)^2)\big)\Big|.$$

Let us consider three cases:

(i) $h_1 + h_3 \neq 0$; by (24), we have:

(30) $$U(h_1, h_2, h_3) \leqslant \sum_{n_2=1}^{P} \Big| \sum_{n_1=1}^{P} e\big(\varrho (h_1 + h_3) n_1^2 + \beta n_1\big)\Big| \leqslant 7P^{3/2}\big(1 + (2M)^{1/2}\big).$$

(ii) $h_2 + h_3 \neq 0$; we obtain the same majorization in the same way.

(iii) $h_3 = -h_2 = -h_1$; by (25), we have

(31) $$U(h_1, h_2, h_3) = \Big| \sum_{n_1=1}^{P} \sum_{n_2=1}^{P} e\big(2\varrho h_3 (n_1 - N)(n_2 - N)\big)\Big| \leqslant 7P^{3/2}\big(1 + (2M)^{1/2}\big).$$

In order to apply Lemma 4, we require also the inequality

(32) $$\sum_{h_1, h_2, h_3}' p_{h_1} \cdot p_{h_2} \cdot p_{h_3} = 8 \Big(\sum_{h=1}^{M} \frac{30}{h}\Big)^3 + 24 \Big(\sum_{h=1}^{M} \frac{30}{h}\Big)^2 + 24 \Big(\sum_{h=1}^{M} \frac{30}{h}\Big)$$
$$< 8 \Big(1 + \sum_{h=1}^{M} \frac{30}{h}\Big)^3 \leqslant 250\,000 (\operatorname{Log} M)^3.$$

With the notations of Lemma 3, (26) becomes, in view of (29), (30), (31) and (32),

(33) $$|S - \theta^3 P^2| \leqslant 7P^{3/2}(1 + \sqrt{2} P^{1/8})\, 250\,000 \cdot 4^{-3} (\operatorname{Log} P)^3 + 1201 P^{7/4}.$$

Since P is greater than 160^{12}, $\operatorname{Log} P$ is less than $4.82 P^{1/24}$, and (33) becomes

(34) $$|S - \theta^3 P^2| \leqslant 6.16 \cdot 10^6 P^{2-1/4} \leqslant 7.34 \cdot 10^6 N^{-1/4} P^2.$$

By (27) and (28), we have

(35) $$\theta^3 P^2 > 7.34 \cdot 10^6 N^{-1/4} P^2.$$

Comparing (34) and (35), we see that S is positive, and the proof of Theorem 1 is now complete.

4. In this section, we will construct a sequence C such that C is not a basis but C^2 is a basis (of order at most 6). We need one more lemma.

LEMMA 5. *Let p be any odd prime number, a any integer. Then there exist integers x, y, z such that*

(36) $$x^2+y^2+z^2 \equiv a \pmod{p^2}$$

and

(37) $$|r(x,p)| < \sqrt{3p}, \quad |r(y,p)| < \sqrt{3p}, \quad |r(z,p)| < \sqrt{3p}.$$

Proof. If $p = 3$, the lemma is trivial, so we suppose $p > 3$. Since p^2 is congruent to 1 mod 8, we may write

(38) $$a \equiv rp+s \pmod{p^2},$$

where r, s are integers, such that

(39) $$0 \leqslant r < p$$

and

(40) $$1 \leqslant s \leqslant 3p, \quad \text{and } s \text{ not congruent to } 0 \text{ or } 7 \bmod 8.$$

By Legendre's theorem, there exist non-negative integers b, c, d such that

(41) $$b^2+c^2+d^2 = s.$$

(40) and (41) imply that

(42) $$0 \leqslant b \leqslant \sqrt{s} \leqslant \sqrt{3p}, \quad 0 \leqslant c \leqslant \sqrt{s} \leqslant \sqrt{3p}, \quad 0 \leqslant d \leqslant \sqrt{s} \leqslant \sqrt{3p}.$$

By (40), at least one of the numbers b, c, d is positive; we may suppose that $b > 0$. Then

$$1 \leqslant b \leqslant \sqrt{3p}$$

which implies that $(b, p) = 1$. Thus also $(2b, p) = 1$ (p is odd); therefore there exists an integer v such that

(43) $$2vb \equiv r \pmod{p}$$

holds.

Let

$$x = vp+b, \quad y = c, \quad z = d.$$

Then we obtain from (38), (41) and (43) that

$$x^2+y^2+z^2 = (vp+b)^2+c^2+d^2 = v^2p^2+2vbp+b^2+c^2+d^2$$
$$= v^2p^2+2vbp+s \equiv rp+s \equiv a \pmod{p^2},$$

whence (36) holds.

Furthermore, by (2) and (42),

$$|r(x,p)| = |r(vp+b,p)| = |r(b,p)| \leqslant b < \sqrt{3p}.$$

The other three inequalities in (37) follow immediately from (2) and (42). (Clearly we need not put equality signs in (37)).

THEOREM 2. *There exists a sequence C such that C is* **not** *a basis but C^2 is a basis (of order at most 6).*

Proof. Let p_k $(k = 1, 2, \ldots)$ denote the kth odd prime number: $p_1 = 3$, $p_2 = 5$, $p_3 = 7, \ldots$ Let

(44) $$n_k = 12(p_1p_2\ldots p_k)^4 \quad \text{for} \quad k = 1, 2, \ldots$$

Let us define the sequence C in the following way: let

$$C\cap[0, n_1] = \{0, 1, 2, \ldots, n_1\}.$$

If $n > n_1$, then for some positive integer k, $n_k < n \leqslant n_{k+1}$. Then $n \in C$ holds if and only if

(45) $$|r(n, p_i)| < \sqrt{3p_i} \quad \text{for} \quad i = 1, 2, \ldots, k.$$

By our construction, the sequence C has property $P\left(n_k, \sqrt{\frac{3}{p_k}}, p_k\right)$ for $k = 1, 2, \ldots$; thus C is not a basis by Lemma 1.

Thus we have to prove only that C^2 is a basis. We will show that C^2 is a basis of order at most 6, i.e., for any given non-negative integer m, there exist integers $C_1, C_2, \ldots, C_6$ such that

(46) $$m = \sum_{j=1}^{6} C_j^2$$

and

(47) $$C_j \in C \quad \text{for} \quad j = 1, 2, \ldots, 6.$$

For $m \leqslant n_1$, the existence of such numbers $C_1, C_2, \ldots, C_6$ is trivial. Assume next $m > n_1$. Then

(48) $$n_k < m \leqslant n_{k+1}$$

for some integer k.

Let us apply Lemma 5 with $a = m$, $p = p_i$ where $i = 1, 2, \ldots, k$. We obtain that, for $i = 1, 2, \ldots, k$, there exist integers x_i, y_i, z_i such that

$$x_i^2+y_i^2+z_i^2 \equiv m \pmod{p_i^2}$$

and

$$|r(x_i, p_i)| < \sqrt{3p_i}, \quad |r(y_i, p_i)| < \sqrt{3p_i}, \quad |r(z_i, p_i)| < \sqrt{3p_i}.$$

Let us denote the least non-negative solution of the congruence system

$$x \equiv x_i \pmod{p_i^2} \quad (i = 1, 2, \ldots, k);$$

$$y \equiv y_i \pmod{p_i^2} \quad (i = 1, 2, \ldots, k);$$

resp.

$$z \equiv z_i \pmod{p_i^2} \quad (i = 1, 2, \ldots, k);$$

by C_1', C_2', resp. C_3'.

We may now choose $\lambda_1, \lambda_2, \lambda_3$ belonging to $\{0, 1\}$, such that:

$$\sum_{j=1}^{3} (C_j' + \lambda_j p_1 p_2 \ldots p_k)^2 \equiv m-1 \pmod 4.$$

Let $C_j = C_j' + \lambda_j p_1 \ldots p_k$ $(j = 1, 2, 3)$. Then clearly,

(49) $$0 \leqslant C_j < 2(p_1 p_2 \ldots p_k)^2 \quad \text{for} \quad j = 1, 2, 3.$$

By the definition of the x_i's, y_i's, z_i's and C_j's $(i = 1, 2, \ldots, k$, $j = 1, 2, 3)$,

(50) $$C_1^2 + C_2^2 + C_3^2 \equiv m \pmod{(p_1 p_2 \ldots p_k)^2}$$

and

(51) $$|r(C_j, p_i)| < \sqrt{3p_i} \quad \text{for} \quad j = 1, 2, 3, \; i = 1, 2, \ldots, k.$$

(44) and (49) give that

(52) $$0 \leqslant C_j < n_k \quad \text{for} \quad j = 1, 2, 3.$$

By the construction of the sequence C, (51) and (52) imply that

$$C_j \in C \quad \text{for} \quad j = 1, 2, 3.$$

To complete the proof that C^2 is a basis of order at most 6, we have to show that the number

(53) $$t = m - (C_1^2 + C_2^2 + C_3^2)$$

can be written in form

(54) $$t = C_4^2 + C_5^2 + C_6^2$$

where

(55) $$C_j \in C \quad (j = 4, 5, 6).$$

We obtain from (44), (48) and (52) that

$$t = m - (C_1^2 + C_2^2 + C_3^2) \leqslant m \leqslant n_{k+1}$$

and

$$t = m - (C_1^2 + C_2^2 + C_3^2) > n_k - 12(p_1 p_2 \ldots p_k)^4 \geqslant 0,$$

thus

(56) $$0 \leqslant t \leqslant n_{k+1}.$$

Furthermore, it follows from (50) and the definition of t that $t \equiv 0 \pmod{(p_1 \ldots p_k)^2}$. Let

(57) $$t = q(p_1 p_2 \ldots p_k)^2.$$

By Legendre's theorem, there exist non-negative integers q_1, q_2, q_3 such that

(58) $$q = q_1^2 + q_2^2 + q_3^2$$

since $t \equiv 1 \pmod 4$, and so $q \equiv 1 \pmod 4$.

Let

$$C_j = q_{j-3} p_1 p_2 \ldots p_k \quad (j = 4, 5, 6).$$

Then (57) and (58) give that

(59) $$\sum_{j=4}^{6} C_j^2 = \sum_{j=4}^{6} (q_{j-3} p_1 p_2 \ldots p_k)^2 = (p_1 p_2 \ldots p_k)^2 (q_1^2 + q_2^2 + q_3^2) = q(p_1 p_2 \ldots p_k)^2 = t;$$

thus (54) holds.

Furthermore, by (56) and (59),

(60) $$0 \leqslant C_j \leqslant \sqrt{t} \leqslant t \leqslant n_{k+1} \quad (j = 4, 5, 6)$$

and clearly,

(61) $$|r(C_j, p_i)| = |r(q_{j-3} p_1 p_2 \ldots p_k, p_i)| = 0 \quad (j = 4, 5, 6; \; i = 1, 2, \ldots, k).$$

By the construction of the sequence C, (60) and (61) imply (55), and thus we have proved that C^2 is a basis of order at most 6.

5. It can be proved by a similar construction that, for any given positive integer k, there exist sequences D, E such that D is a basis but D^k is not a basis, while E is not a basis but E^k is a basis (only the computation becomes slightly longer). The same idea even could be applied to construct a sequence F such that F is a basis but $\sum_{k=2}^{+\infty} F^k$ is not a basis (but the construction would be even more complicated).

Furthermore, we remark that the sequence B constructed by us was a basis of order at most 3, while C^2 was a basis of order at most 6 (but neither B^2 nor C is a basis). We guess that there exist also sequences G, H such that G is a basis of order 2 but G^2 is not a basis, while H is not a basis but H^2 is a basis of order 4.

Finally let L be a set of positive integers; is it true that there exists a sequence A such that A^n is a basis if and only if n belongs to L? The answer is yes if there is only a finite number of integers which do not lie in L.

Added in proof. The first named author and E. Fouvry proved in a paper which will appear in the J. London Math. Soc. that for any set L of positive integers there does exist a sequence A such that A^n is a basis if and only if n belongs to L; it is clear from their proof that there exists also a sequence H which is not a basis such that H^2 is a basis of order at most 5.

References

[1] J. G. van der Corput, *Neue zahlentheorische Abschätzungen*, Math. Zeitsch. 29 (1929), pp. 397–426.

[2] J. F. Koksma, *Some theorems on Diophantine inequalities*, Math. Centrum Amsterdam Script. 5 (1950).

[3] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe*, J. Reine Angew. Math. 194 (1955), pp. 111–140.

[4] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, London 1954.

Received on 29. 5. 1974
and in revised form on 2. 12. 1974 (593)

ACTA ARITHMETICA
XXX (1976)

A sharper bound for the least pair of consecutive k-th power non-residues of non-principal characters (mod p) of order $k > 3$

by

RICHARD H. HUDSON (Columbia, S. C.)

1. History of the problem. Let χ be a non-principal character (mod p) of fixed order k and let $n_2(k,p)$ denote the smallest positive integer satisfying

$$(1.1)\qquad \chi\big(n_2(k,p)\big) \neq 0 \text{ or } 1, \qquad \chi\big(n_2(k,p)+1\big) \neq 0 \text{ or } 1.$$

The first significant success in providing an upper bound for $n_2(k,p)$ was that of P. D. T. A. Elliott ([3], p. 52) who showed that for real valued characters (mod p), i.e. Legendre symbols ($p > 2$), that

$$(1.2)\qquad n_2(k,p) = O(p^{1/4+\varepsilon})$$

for each $\varepsilon > 0$ and $p \geqslant 5$.

Although (1.2) is a relatively easy consequence of D. A. Burgess's [1] deep and thoroughly remarkable character sum estimates, Elliott improved (1.2) when, in addressing the Number Theory Conference in Boulder, Colorado in 1972 [4], he showed that

$$(1.3)\qquad n_2(k,p) = O\Big(p^{\frac{1}{4}\left(1-\frac{e^{-10}}{2}\right)+\varepsilon}\Big)$$

for each $\varepsilon > 0$ and $p \geqslant 5$.

2. A new bound for $n_2(k,p)$. An "alternative bound" for $n_2(k,p)$ was provided in [7] where I proved that

$$(2.1)\qquad n_2(k,p) \leqslant \big(q_1(k,p)-1\big)\big(q_2(k,p)\big)$$

where $q_1(k,p)$ and $q_2(k,p)$ are, for each fixed k, respectively the smallest and the second smallest positive primes with $\chi\big(q_1(k,p)\big) \neq 0$ or 1, $\chi\big(q_2(k,p)\big) \neq 0$ or 1.

I asserted in [7] which was written in the Fall of 1973, and I announced when I spoke in Oberwolfach, Germany in January, 1974, that (2.1) leads to an improvement of (1.3) for all non-principal characters