ACTA ARITHMETICA
LX.2 (1991)

Arithmetic progressions in sumsets

by

IMRE Z. RUZSA* (Budapest)

1. Introduction. Let $A, B \subset [1, N]$ be sets of integers, $|A| = |B| = cN$. Bourgain [2] proved that $A + B$ always contains an arithmetic progression of length $\exp(\log N)^{1/3-\varepsilon}$. Our aim is to show that this is not very far from the best possible.

THEOREM 1. *Let ε be a positive number. For every prime $p > p_0(\varepsilon)$ there is a symmetric set A of residues* mod p *such that $|A| > (1/2 - \varepsilon)p$ and $A + A$ contains no arithmetic progression of length*

$$\exp(\log p)^{2/3+\varepsilon}. \tag{1.1}$$

A set of residues can be used to get a set of integers in an obvious way. Observe that the $1/2$ in the theorem is optimal: if $|A| > p/2$, then $A + A$ contains every residue.

Acknowledgement. I profited much from discussions with E. Szemerédi; he directed my attention to this problem and to Bourgain's paper.

2. The construction. In this section we describe the set A of Theorem 1 and prove its properties, assuming Theorems 2 and 3 (to be stated below) which will be proved in Sections 3 and 4.

Our construction goes as follows. Take k residues $a_1, \ldots, a_k \in \mathbf{Z}_p$ and write

$$F(x) = \sum e(a_j x/p), \qquad f(x) = \operatorname{Re} F(x) = \sum \cos(2\pi a_j x/p); \tag{2.1}$$

here, as usual, $e(t) = \exp 2\pi i t$. Take a $Q > 0$ and set

$$A = \{x : f(x) > Q\}. \tag{2.2}$$

---

* This paper was presented at the CBMS regional conference in Manhattan, Kansas, May 1990. Participation was supported by Hungarian National Foundation for Scientific Research, Grant No. 1811 and NSF.

A is a symmetric set of residues. If $x, y \in A$, then we have

$$\begin{aligned} 2Q <\ & \mathrm{Re} \sum (e(a_j x/p) + e(a_j y/p)) \\ =\ & \mathrm{Re} \sum e(a_j y/p) \left(1 + e\left(\frac{a_j(x-y)}{p} \right) \right) \\ \le\ & \sum \left| 1 + e\left(\frac{a_j(x-y)}{p} \right) \right| . \end{aligned}$$

Consequently, $A - A$ (which is equal to $A + A$ by the symmetry) will be disjoint from the set

$$H = \left\{ h : \sum |1 + e(a_j h/p)| < 2Q \right\} . \tag{2.3}$$

Our task is to find $a_1, \ldots, a_k$ and Q so that $|A| > (1/2 - \varepsilon)p$ and H intersects every not too short arithmetic progression.

For a typical choice of $a_1, \ldots, a_k$, the functions $e(a_j x/p)$ will be almost independent, thus $f(x)$ has approximately a normal distribution with variance $k/2$; hence $|A| \sim p/2$ will hold if $Q = o(\sqrt{k})$. We formulate this exactly as follows.

2.1. Definition. We call the sequence $a_1, \ldots, a_k \in \mathbf{Z}_p$ *K-independent* for a number $K > 0$ if the equation

$$\sum a_j x_j \equiv 0 \pmod p \tag{2.4}$$

has no solution with $0 < \sum |x_j| \le K$.

Theorem 2. *Let $a_1, \ldots, a_k$ be a K-independent sequence of residues* $\bmod p$, *$c_1, \ldots, c_k$ real numbers*, $\sum c_j^2 = 2\sigma^2 > 0, \max |c_j| = \Delta, \sum |c_j| = S$. *Put*

$$f(x) = \sum c_j \cos(2\pi a_j x/p) .$$

We have uniformly in t

$$\frac{1}{p} \sum_{f(x) \le t\sigma} 1 - \Phi(t) \ll \left(\frac{\Delta}{\sigma} \right)^2 + \min\left(\frac{1}{\sqrt{K}}, \frac{S}{\sigma K} \right), \tag{2.5}$$

where Φ is the standard normal distribution. In particular, *if $c_j = 1$ for all j*, *then*

$$\frac{1}{p} \sum_{f(x) \le Q} 1 - \Phi\left(\sqrt{\frac{2}{k}} Q \right) \ll \frac{1}{k} + \min\left(\frac{1}{\sqrt{K}}, \frac{\sqrt{k}}{K} \right) . \tag{2.6}$$

Theorem 2 will be proved in Section 4.

The set H is defined in terms of the function $g(h) = \sum |1 + e(a_j h/p)|$ which is more difficult to handle because of the $|\ |$ sign. We may try a square-mean inequality:

$$g(h) \le \sqrt{k \sum |1 + e(a_j h/p)|^2} = \sqrt{2k(k + f(h))}\,. \tag{2.7}$$

So, to guarantee a small value of $g(h)$ it is sufficient to have $f(h) \approx -k$. To ensure this we need a stronger assumption than K-independence.

2.2. Definition. We call the sequence $a_1, \ldots, a_k \in \mathbf{Z}_p$ *K, L-separated* for $K, L > 0$ if the equation

$$y + \sum a_j x_j \equiv 0 \pmod p \tag{2.8}$$

has no solution with $0 < \sum |x_j| \le K, |y| \le L$.

Theorem 3. *Let $a_1, \ldots, a_k$ be a K, L-separated sequence of residues* $\bmod p$, $c_1, \ldots, c_k$ *real numbers*, $\sum |c_j| = S$. *Put*

$$f(x) = \sum c_j \cos(2\pi a_j x/p)\,.$$

Suppose $k \ge 4$, $0 < \delta < 1/2$. *If*

$$K \ge \frac{4k}{\delta} \log \frac{2}{\delta} \tag{2.9}$$

and

$$T \ge \frac{4p}{L}(2/\delta)^{2k}\,, \tag{2.10}$$

then among any T consecutive values of x there is always one for which $f(x) > S(1 - \delta)$ as well as one with $f(x) < -S(1 - \delta)$.

This theorem will be proved in Section 3.

2.3. Corollary. *Let $a_1, \ldots, a_k$ be a K, L-separated sequence of residues* $\bmod p, g(h) = \sum |1 + e(a_j h/p)|$, $K > 4k$. *If* (2.9) *and* (2.10) *are satisfied, then among any T consecutive values of x there is always one for which $g(h) < k\sqrt{2\delta}$.*

Proof. This follows immediately from the previous theorem and inequality (2.7). ∎

This result is not directly applicable to our problem, since we need to find small values of $g(h)$ in every arithmetic progression, not just in those with difference 1. A sequence such that $a_1 d, \ldots, a_k d$ is K, L-separated for every $d \ne 0$ would suffice, but such a sequence does not exist. Fortunately, a somewhat weaker assumption also works.

2.4. Definition. We call the sequence $a_1, \ldots, a_k \in \mathbf{Z}_p$ *K, L, m-quasi-separated* if m of them can be omitted so that the remaining $k - m$ are K, L-separated.

2.5. Statement. *Let* $a_1, \ldots, a_k$ *be a* K, L, m*-quasiseparated sequence of residues* $\bmod p, g(h) = \sum |1 + e(a_j h/p)|$, $K > 4k$. *If* (2.9) *and* (2.10) *are satisfied, then among any* T *consecutive values of* x *there is always one for which* $g(h) < 2m + k\sqrt{2\delta}$.

Proof. Put $g = g_1 + g_2$, where g_1 contains the m omitted terms, and g_2 the remaining $k' = k - m$. We apply Corollary 2.3 to g_2. If (2.9) and (2.10) hold, they remain true with $k' < k$ in place of k, because the right-hand sides are increasing functions of k. Thus between T consecutive values we find one for which $g_2(h) < k'\sqrt{2\delta}$, which implies

$$g(h) \le 2m + g_2(h) < 2m + k\sqrt{2\delta}\,. \ \blacksquare$$

Next we show that with a suitable choice of the parameters almost all k-tuples are independent and quasiseparated.

2.6. Lemma. *The number of* k*-tuples that are not* K*-independent is at most* $(2K+1)^k p^{k-1}$.

Proof. The number of possible equations (2.4) is at most $(2K+1)^k$, since each coefficient lies between $-K$ and K, and an equation has at most p^{k-1} solutions. $\blacksquare$

2.7. Lemma. *The number of* k*-tuples that are not* K, L*-separated is at most*

$$(2K+1)^k (2L+1) p^{k-1}\,.$$

Proof. The difference in comparison with the previous lemma is that we have to exclude equation (2.8), where there are $2L+1$ possibilities for y, thus the total number of equations is bounded by $(2K+1)^k(2L+1)$. $\blacksquare$

2.8. Lemma. *The number of* k*-tuples that are not* K, L, m*-quasiseparated is at most*

$$(2K+1)^{k(m+1)} (2L+1)^{m+1} p^{k-(m+1)}\,.$$

Proof. Let $F(k, m, K, L)$ denote the number of k-tuples to be estimated. We know

$$F(k, 0, K, L) \le (2K+1)^k (2L+1) p^{k-1}$$

from the previous lemma. Now we show

$$F(k, m, K, L) \le (2K+1)^k (2L+1) F(k-1, m-1, K, L)\,. \tag{2.11}$$

These inequalities yield the lemma by an easy induction.

To prove (2.11), take a k-tuple that is not K, L, m-quasiseparated. It must satisfy an equation of type (2.8). The number of possible equations is $\le (2K+1)^k(2L+1)$; we show that the number of such solutions of a fixed equation that are not quasiseparated is at most $F(k-1, m-1, K, L)$. Indeed, let j be a subscript such that $x_j \ne 0$. Then a_j is uniquely determined by $a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k$, which form a $(k-1)$-tuple that is not K, L, $m-1$-quasiseparated. ∎

Proof of Theorem 1. Given p and ε, we shall select a positive integer k, then a k-tuple of residues $a_1, \ldots, a_k$ and define A by (2.2). We use k as a parameter which we shall optimize at the end; we assume $k \to \infty$ and $k = o(\log p)$.

We take four other parameters K, L, m, K' and try to find a K'-independent k-tuple $a_1, \ldots, a_k$ such that $da_1, \ldots, da_k$ is K, L, m-quasiseparated for every $d \not\equiv 0 \pmod p$. According to Lemmas 2.6 and 2.8, such a k-tuple exists if

$$(2K'+1)^k p^{k-1} + (p-1)(2K+1)^{km}(2L+1)^m p^{k-m} < p^k .$$

This is satisfied if

$$(2K'+1)^k < p/2 \tag{2.12}$$

and

$$(2K+1)^k(2L+1) < p^{1-1/m}/2 . \tag{2.13}$$

(2.12) is satisfied with $K' = [p^{1/k}/3]$; we shall only need that $K' \to \infty$, which follows from the assumption $k = o(\log p)$.

We define A and H by (2.2) and (2.3), with $Q = \varepsilon\sqrt{k}$. We use Theorem 2 to estimate the cardinality of A (2.6) yields

$$\frac{1}{p}|A| > 1 - \Phi(\sqrt{2}\varepsilon) - O(1/k + 1/\sqrt{K'}) > 1/2 - \varepsilon$$

for large p, since both k and K' tend to infinity.

H is defined by the inequality $g(h) < 2Q$. We apply Statement 2.5. Since the conclusion we need is $g(h) < 2Q$, we put

$$m = [Q/2] = \left[\frac{\varepsilon}{2}\sqrt{k}\right] \tag{2.14}$$

and $\delta = \varepsilon^2/(2k)$. To satisfy (2.9), we define

$$K = [(k \log k)^2] .$$

With these parameters, Statement 2.5 is applicable not only to g but to any of the functions $g_d(h) = g(hd)$, and we conclude that there is an element of H among any T consecutive terms of an arithmetic progression, where T is given by (2.10). Our task is to minimize the quantity

$$\frac{p}{L}\left(\frac{4k}{\varepsilon^2}\right)^{2k} . \tag{2.15}$$

To satisfy (2.13) we put

$$L = [p^{1-1/m} K^{-k} 3^{-k-1}]$$

and then (2.15) becomes

$$\le 3^{k+1}p^{2/(\varepsilon\sqrt{k})}\left(\frac{4k^2\log k}{\varepsilon^2}\right)^{2k}.$$

The choice $k=[(\log p/\log\log p)^{2/3}]$ yields

$$T<\exp c_\varepsilon(\log p\log\log p)^{2/3}. \ \blacksquare$$

3. Large values of f. This section is devoted to the proof of Theorem 3. Let $a_1,\dots,a_k\in\mathbf{Z}_p$, $c_1,\dots,c_k$ real numbers, $F(x)=\sum c_je(a_jx/p)$, $f(x)=\operatorname{Re}F(x)=\sum c_j\cos(2\pi a_jx/p)$, $\sum|c_j|=S$.

We shall compare f to a sum of independent random variables. Let $X_1,\dots,X_k$ be independent random variables uniformly distributed on the circle $|z|=1$, $\xi_j=\operatorname{Re}X_j$, $Z=\sum c_jX_j$, $\zeta=\operatorname{Re}Z=\sum c_j\xi_j$.

We shall calculate moments of f and ζ. Write

$$R_{uv}=\mathbf{E}(Z^u\overline{Z}^v),\qquad r_l=\mathbf{E}\zeta^l=2^{-l}\sum_{v=0}^{l}\binom{l}{v}R_{v,l-v}. \tag{3.1}$$

We are interested in the distribution of f on T consecutive numbers, say $y+1,\dots,y+T$. Write

$$\begin{aligned} M_{uv}&=\frac1T\sum_{z=y+1}^{y+T}F(x)^u\overline{F(x)^v},\\ m_l&=\frac1T\sum_{z=y+1}^{y+T}f(x)^l=2^{-l}\sum_{v=0}^{l}\binom{l}{v}M_{v,l-v}. \end{aligned}\tag{3.2}$$

3.1. Lemma. *If the sequence $a_1,\dots,a_k$ is K,L-separated, then for $u+v\le K$ we have*

$$|M_{uv}-R_{uv}|\le\frac{p}{TL}S^{u+v}. \tag{3.3}$$

Proof. Write

$$\phi(b)=\frac1T\sum_{y=x+1}^{y+T}e(bx/p).$$

It is well known that

$$\phi(b)\begin{cases}=1 & \text{if } b\equiv0 \pmod p,\\ =0 & \text{if } b\not\equiv0, T=p,\\ \le 1/T\|b/p\| & \text{anyway,}\end{cases}\tag{3.4}$$

where $\|\dots\|$ means the distance from the nearest integer. We have

$$M_{uv}=\sum c_{i_1}\dots c_{i_u}\overline{c}_{j_1}\dots\overline{c}_{j_v}\phi(a_{i_1}+\dots+a_{i_u}-a_{j_1}-\dots-a_{j_v})$$

and

$$R_{uv} = {\sum}' c_{i_1} \ldots c_{i_u} \overline{c}_{j_1} \ldots \overline{c}_{j_v}, \tag{3.5}$$

where the $'$ means that the summation is over those sequences of subscripts for which $(j_1, \ldots, j_v)$ is a permutation of $(i_1, \ldots, i_u)$ (thus it is empty unless $u = v$). The assumption of K, L-separation means that the number $b = a_{i_1} + \ldots + a_{i_u} - a_{j_1} - \ldots - a_{j_v}$ satisfies $\|b/p\| \geq L/p$ unless $(j_1, \ldots, j_v)$ is a permutation of $(i_1, \ldots, i_u)$. Consequently we have

$$|M_{uv} - R_{uv}| \leq \frac{p}{TL} \sum |c_{i_1} \ldots c_{i_u} \overline{c}_{j_1} \ldots \overline{c}_{j_v}| = \frac{p}{TL} S^{u+v}. \ \blacksquare$$

3.2. Lemma. *If the sequence $a_1, \ldots, a_k$ is K, L-separated, then for $l \leq K$ we have*

$$|m_l - r_l| \leq \frac{p}{TL} S^l. \tag{3.6}$$

Proof. This follows from the previous lemma, (3.1) and (3.2). $\blacksquare$

Proof of Theorem 3. Assume indirectly that $f(x) \leq S(1-\delta)$ for $x = y+1, \ldots, y+T$. (The case of big negative values follows by considering the function $-f(x)$ similarly.) Then for every number

$$U \geq \delta S/2 \tag{3.7}$$

we have

$$|f(x) + U| \leq U + S(1-\delta)$$

for the same values of x. Consequently,

$$\frac{1}{T} \sum (f(x) + U)^l \leq (U + S(1-\delta))^l \tag{3.8}$$

for any even integer l. The sum on the left side of (3.8) is equal to

$$\sum_{j=0}^{l} m_j U^{l-j} \binom{l}{j} = \sum_{j=0}^{l} r_j U^{l-j} \binom{l}{j} + \text{error} = \mathbf{E}((\zeta + U)^l) + \text{error}. \tag{3.9}$$

By the previous lemma,

$$|\text{error}| \leq \frac{p}{TL} \sum_{j=0}^{l} S^j U^{l-j} \binom{l}{j} = \frac{p}{TL} (S+U)^l \quad \text{if } l \leq K. \tag{3.10}$$

We estimate the main term as follows:

$$\mathbf{E}((\zeta + U)^l) \geq (U + S(1-\eta))^l \mathbf{P}(\zeta \geq S(1-\eta))$$

with any $0 < \eta < 1$. Now $\zeta \geq S(1-\eta)$ certainly holds if $\xi_j \operatorname{sg} c_j \geq 1 - \eta$ for all $j = 1, \ldots, k$. The probability of one such event is

$$\frac{1}{\pi} \arccos(1-\eta) \geq \frac{\sqrt{2}}{\pi} \sqrt{\eta} \geq \eta$$

if $\eta < 1/5$. This yields $\mathbf{P}(\zeta \ge S(1-\eta)) \ge \eta^k$, hence

$$\mathbf{E}((\zeta + U)^l) \ge \eta^k (U + S(1-\eta))^l \,. \tag{3.11}$$

Combining (3.7)–(3.10) we get the inequality

$$(U + S(1-\delta))^l \ge \eta^k (U + S(1-\eta))^l - \frac{p}{TL}(S+U)^l \,.$$

After introducing the parameter $\varrho = S/(U+S)$ and rearranging, this takes on the simpler form

$$p/(TL) \ge \eta^k (1-\eta\varrho)^l - (1-\delta\varrho)^l \,. \tag{3.12}$$

Condition (3.7) can be rewritten as

$$\varrho \le 2/(2+\delta) \,. \tag{3.13}$$

We put $\eta = \delta/2$ into (3.12); the assumption $\delta < 1/3$ guarantees $\eta < 1/5$. We use the inequality $(1-t)^2 \ge 1 - 2t$ to obtain

$$p/(TL) \ge \eta^k z - z^2 \tag{3.14}$$

with $z = (1-\eta\varrho)^l$. The quadratic function in (3.14) assumes its maximum at $z = \eta^k/2$ and this choice yields

$$p/(TL) \ge \eta^{2k}/2 = (\delta/2)^{2k}/2 \,,$$

which contradicts (2.10). The choice of z determines ϱ, and it is compatible with (3.13) if and only if

$$\eta^k/2 = \delta^k 2^{-k-1} \ge \left(1 - \frac{\delta\varrho}{2}\right)^l = \left(\frac{2}{2+\delta}\right)^l ,$$

or, equivalently,

$$l \ge \frac{k\log(2/\delta) + \log 2}{\log(1+\delta/2)} \,. \tag{3.15}$$

We have to find an even integer l greater than the bound above but less than K; this is possible if K is greater than the right side of (3.15) $+2$, which follows from (2.9). ■

3.3. Remark. Some of our calculations were far from optimal. Performing them with more precision would not, however, yield an essential improvement in the results. I do not know whether a more sophisticated method than this moment inequality could lead to sharper results and an improvement of the exponent in Theorem 1. I feel that most of the loss comes from the square-mean inequality used in (2.7).

4. The normal distribution of f. We prove Theorem 2. We retain the notations introduced at the beginning of the previous section. We shall compare the distribution of f to that of ζ, and ζ to the normal distribution. Since we are now interested in distribution on all residues, we put $T = p$.

We also assume that our function is normalized so that $\sum c_j^2 = 2$, that is, $\sigma = 1$. We recall the notation $\Delta = \max |c_j|$.

We use Esseen's famous inequality [3] in its simplest form:

4.1. Lemma. *Let $G_1(x)$ and $G_2(x)$ be distribution functions with the corresponding characteristic functions $\gamma_1(t)$ and $\gamma_2(t)$. Assume that $G_1'(x)$ exists and $G_1'(x) \le V$ for all x. Then*

$$\sup_x |G_1(x) - G_2(x)| \ll \frac{V}{T} + \int_0^T \frac{|\gamma_1(t) - \gamma_2(t)|}{t}\, dt \tag{4.1}$$

where the implied constant is absolute.

First we consider ζ. Let $\psi(t) = \mathbf{E}e^{it\zeta}$ be its characteristic function, $P(x) = \mathbf{P}(\zeta \le x)$ its distribution.

4.2. Lemma. *There are absolute constants $\beta > 0$, $B > 1$ and $T_0 > 1$ such that*

$$|\psi(t)| \le \begin{cases} \exp(-\beta t^2) & \text{for } |t| \le T_0/\Delta, \\ (B\Delta|t|)^{-1/\Delta^2} & \text{for } |t| > T_0/\Delta. \end{cases} \tag{4.2}$$

Proof. By the definition of ζ we have

$$\psi(t) = \prod J(c_j t)\,, \tag{4.3}$$

where

$$J(t) = \mathbf{E}e^{it\xi_j} = \frac{1}{2\pi}\int_0^{2\pi} e^{it\cos\alpha}\, d\alpha$$

is a Bessel function. We only need the following properties of $J(t)$:

$$J(t) = 1 - t^2/4 + O(t^4) \tag{4.4}$$

for small t, $J(t) \ll |t|^{-1/2}$ for large t, and $|J(t)| < 1$ for all $t \ne 0$. Hence the function

$$\beta_T = \min_{|t|\le T} \frac{-\log|\psi(t)|}{t^2} \tag{4.5}$$

satisfies

$$\beta_T \ge \begin{cases} \dfrac{\log BT}{2T^2} & \text{for } T > T_0, \\ \beta & \text{for } T \le T_0 \end{cases} \tag{4.6}$$

with suitable constants $\beta > 0$, $B > 1$ and $T_0 > 1$. Observe that $|J(t)| \le \exp(-\beta_T t^2)$ for $|t| \le T$ by the definition of β_T. Since $|c_j t| \le \Delta|t|$ for all j, an application of this inequality for the numbers $c_j t$ with $T = \Delta|t|$ and a substitution to (4.3) yields

$$|\psi(t)| \le \exp\Big(-\beta_T \sum (c_j t)^2\Big) = \exp(-2\beta_T t^2)\,.$$

(4.2) follows from this inequality and (4.6). ∎

4.3. Statement. *We have*

$$\max|P(x)-\Phi(x)| \ll \Delta^2 . \tag{4.7}$$

Proof. By Lemma 4.1, the left side is

$$\ll \int_0^\infty \frac{|\psi(t)-e^{-t^2/2}|}{t}\,dt . \tag{4.8}$$

Let $T_1>0$ be a number such that (4.4) holds for $|t|<T_1$. Applying (4.4) to each factor we obtain

$$\psi(t)=e^{-t^2/2}+O\Big(t^4\sum c_j^4\Big)=e^{-t^2/2}+O(\Delta^2t^4),$$

for $|t|\le T_1/\Delta$, since

$$\sum c_j^4 \le (\max c_j)^2\sum c_j^2 \le 2\Delta^2 .$$

For $|t|\le T_1/\Delta$ this implies

$$\psi(t)-e^{-t^2/2} \ll \Delta^2t^2e^{-t^2/2},$$

which implies that the contribution of $|t|\le T_1/\Delta$ to (4.8) is $O(\Delta^2)$. For $|t|>T_1/\Delta$ we apply Lemma 4.2 to ψ and obtain the same bound after a routine calculation. ∎

4.4. Remark. The bound $O(\Delta^2)$ is sharp. We could immediately deduce the weaker bound $O(\Delta)$ from the Berry–Esseen inequality [1, 3]. The improvement is due mainly to the fact that not only the first but also the third moments of ξ_j vanish.

Now we turn to comparing ζ and f.

4.5. Lemma. *If the sequence $a_1,\dots,a_k$ is K-independent, then $m_l=r_l$ for $l\le K$.*

The proof is analogous to that of Lemma 3.2, we just apply the second case of (3.4) instead of the third. ∎

Recall that $S=\sum|c_j|$.

4.6. Lemma. *Let $l=2u$ be an even positive integer. Then*

$$r_l\le\min(S^l,u!) .$$

Proof. We always have $|\zeta|\le S$, thus $r_l\le S^l$ is obvious. To prove $r_l\le u!$ recall that by (3.1) and (3.5)

$$r_l=2^{-l}\sum c_{i_1}\dots c_{i_u}\overline{c}_{j_1}\dots\overline{c}_{j_u},$$

where the summation is over those sequences of subscripts for which $(j_1,\ldots,j_u)$ is a permutation of $(i_1,\ldots,i_u)$. Since a fixed sequence $(i_1,\ldots,i_u)$ has at most $u!$ permutations, we obtain

$$r_l \le 2^{-l}u!\sum |c_{i_1}\ldots c_{i_u}|^2 = 2^{-l}u!\Big(\sum |c_j|^2\Big)^u = u!\,. \ \blacksquare$$

4.7. Lemma. *If $\Delta < 1/2$, then $P'(x)$ is bounded by an absolute constant.*

Proof. This follows from the familiar inequality

$$P'(x) \le \int\limits_{-\infty}^{\infty} |\psi(t)|\,dt$$

and Lemma 4.2. $\blacksquare$

4.8. Statement. *If $\Delta < 1/2$, then*

$$\frac{1}{p}\sum_{f(x)\le t\sigma} 1 - P(t) \ll \min\Big(\frac{1}{\sqrt{K}},\frac{S}{K}\Big). \tag{4.9}$$

Proof. Denote this difference by R. By the previous lemma and Lemma 4.1 we have

$$R \ll \frac{1}{T} + \int\limits_0^T \frac{|\psi(t)-\chi(t)|}{t}\,dt\,, \tag{4.10}$$

where

$$\chi(t) = \frac{1}{p}\sum_{x=1}^{p} e^{itf(x)}\,.$$

For every real t and positive integer l we have

$$e^{it} = \sum_{j=1}^{l-1}\frac{(it)^j}{j!} + \vartheta\frac{t^l}{l!}$$

with $|\vartheta|\le 1$. Applying this formula both to $e^{it\zeta}$ and $e^{itf(x)}$ we obtain

$$\psi(t) = \sum_{j=1}^{l-1}\frac{r_j}{j!}(it)^j + \vartheta r_l\frac{|t|^l}{l!}\,,\qquad \chi(t) = \sum_{j=1}^{l-1}\frac{m_j}{j!}(it)^j + \vartheta m_l\frac{|t|^l}{l!}\,.$$

In view of Lemma 4.5 we have for even $l\le K$

$$|\psi(t)-\chi(t)| \le 2r_l\frac{t^l}{l!}\,.$$

Substituting this into (4.10) we find

$$R \ll \frac{1}{T} + \frac{r_l}{l!}\frac{T^l}{l}\,.$$

The optimal choice is $T = (l!/r_l)^{1/(l+1)}$ and it yields

$$R \ll \left(\frac{r_l}{l!}\right)^{1/(l+1)} \ll \frac{r_l^{1/l}}{l} \min\left(\frac{S}{l}, \frac{1}{\sqrt{l}}\right)$$

by Lemma 4.6. The statement follows by taking the maximal admissible value $l = 2[K/2]$. ∎

Proof of Theorem 2. For $\Delta < 1/2$ the conclusion follows from Statements 4.3 and 4.8, and for $\Delta \geq 1/2$ it holds obviously. ∎

5. Concluding remarks. In a typical problem of combinatorial number theory, the extremal sets are either very regular, or random sets. Our case is different. If we take a random subset of $\mathbf{Z}_p$, then with probability 1 we have $A + A = \mathbf{Z}_p$. If A is an arithmetic progression of k elements, then $A+A$ is also an arithmetic progression itself. "Multidimensional" arithmetic progressions are somewhat better. Say, put

$$A = \{n : n = x_1 d_1 + \ldots + x_k d_k,\ 0 \leq x_i \leq m - 1\},$$

a set of m^k elements if all of them are different. Here $A + A$ contains arithmetic progressions of $2m - 1$ elements but no longer if, say, $d_{j+1}/d_j > 2m$. This gives n^δ for the length if $|A| = cN$, $A \subset [1, N]$, where $\delta = \delta(c) \to 0$ as $c \to 0$, still far from (1.1).

Another application of a niveau set of a trigonometric polynomial to an additive problem was given in [4].

References

[1] A. C. Berry, *The accuracy of the Gaussian approximation to the sum of independent variables*, Trans. Amer. Math. Soc. 49 (1941), 122–136.

[2] J. Bourgain, *On arithmetic progressions in sums of sets of integers*, in: A Tribute to Paul Erdős (A. Baker, B. Bollobás, A. Hajnal, eds.), Cambridge Univ. Press, Cambridge 1990, 105–109.

[3] C. G. Esseen, *Fourier analysis of distribution functions. A mathematical study of the Laplace–Gaussian law*, Acta Math. 77 (1945), 1–125.

[4] I. Z. Ruzsa, *Essential components*, Proc. London Math. Soc. 54 (1987), 38–56.

MATHEMATICAL INSTITUTE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST, PF. 127, H-1364 HUNGARY

Received on 30.1.1991 (2116)