ACTA ARITHMETICA
IX (1964)

On the addition of residue classes mod p

by

P. Erdös and H. Heilbronn (Bristol)

In this paper we investigate the following question. Let p be a prime, $a_1, \ldots, a_k$ distinct non-zero residue classes mod p, N a residue class mod p. Let

$$F(N) = F(N\,;\,p;\; a_1, \ldots, a_k)$$

denote the number of solutions of the congruence

$$e_1 a_1 + \ldots + e_k a_k \equiv N \pmod{p}$$

where the $e_1, \ldots, e_k$ are restricted to the values 0 and 1. What can be said about the function $F(N)$?

We prove two theorems.

THEOREM I. *$F(N) > 0$ if $k \geqslant 3(6p)^{1/2}$.*

THEOREM II. *$F(N) = 2^k p^{-1}\big(1+o(1)\big)$ if $k^3 p^{-2} \to \infty$ as $p \to \infty$.*

Theorem I is almost best possible. Put

$$a_1 = 1,\; a_2 = -1,\; a_3 = 2,\; a_4 = -2,\; \ldots,\; a_k = (-1)^{k-1}[\tfrac{1}{2}(k+1)].$$

Then it follows from an easy calculation that $F\big(\frac{1}{2}(p-1)\big) = 0$ if $k < 2(p^{1/2}-1)$. Theorem II is best possible. Define $a_1, \ldots, a_k$ as above and assume that $p^{2/3} < k = O(p^{2/3})$. Then it follows from our analysis that

$$\lim_{p\to\infty} p 2^{-k} F(0) > 1.$$

In the method of proof the two theorems differ considerably. The proof of Theorem I is elementary, depending entirely on the manipulation of residue classes mod p, whereas the proof of Theorem II is based on the application of finite Fourier series and simple considerations on diophantine approximations.

In an appendix we state various further conjectures which we are not able to prove.

Proof of Theorem I. We start with a definition. Let $b_1, \ldots, b_l$ be l distinct residue classes $\bmod p$. Then $B(x)$ denotes the number of solutions of the congruence

$$x \equiv b_i - b_j (\bmod p), \quad 1 \leqslant i \leqslant l,\ 1 \leqslant j \leqslant l.$$

We recall the inequality

$$B(x+y) \geqslant -l + B(x) + B(y), \tag{I.1}$$

which is easily proved as follows. Assume that

$$x \equiv b_i - b_j (\bmod p), \quad y \equiv b_g - b_h (\bmod p).$$

If $j = g$, this implies that

$$x+y \equiv b_i - b_h (\bmod p).$$

As there are only l possible values for b_j, (I.1) follows. It can also be written in the form

$$\bigl(l - B(x+y)\bigr) \leqslant \bigl(l - B(x)\bigr) + \bigl(l - B(y)\bigr). \tag{I.2}$$

LEMMA I.1. *Let* $1 < m \leqslant l < \frac{1}{2}p$; $a_1, \ldots, a_m$ *are distinct non-zero residue classes* $\bmod p$. *Then there exists an* i *in* $1 \leqslant i \leqslant k$ *such that*

$$B(a_i) < l - \tfrac{1}{6} m.$$

Proof. Put $r = 1 + [2l/m]$. By Davenport's theorem [1] about the addition of residue classes $\bmod p$, applied to the residue classes $0, a_1, \ldots, a_m$ we obtain $t \geqslant \operatorname{Min}(p-1, rm)$ distinct non-zero residue classes $c_1, \ldots, c_t$ which can be expressed as the sum of at most r residue classes a_j ($1 \leqslant j \leqslant m$), which need not have distinct indices j.

As

$$\sum_{s=1}^{t} B(c_s) \leqslant \sum_{z=1}^{p-1} B(z) = l(l-1),$$

it follows that there exists an s such that

$$B(c_s) \leqslant l(l-1)t^{-1} \leqslant l(l-1)\operatorname{Max}\bigl((p-1)^{-1}, (rm)^{-1}\bigr) < \tfrac{1}{2} l,$$

or

$$l - B(c_s) > \tfrac{1}{2} l.$$

Hence, by (I.2), there exists an a_i such that

$$l - B(a_i) > \tfrac{1}{2} l r^{-1} \geqslant \tfrac{1}{2} l m (m + 2l)^{-1} \geqslant \tfrac{1}{6} m,$$

which completes the proof of the lemma.

Proof of Theorem I. We begin with a definition. If

$$1 \leqslant u \leqslant \tfrac{1}{2} k$$

we consider all possible subsets S_u of u elements of the classes

$$a_1, a_2, \ldots, a_{2u-1}, a_{2u}.$$

For each subset S_u we consider the number $L(S_u)$ of distinct residue classes which can be written in the form

$$e_1 a_1 + \ldots + e_{2u} a_{2u},$$

where

$$e_i = \begin{cases} 0 \text{ or } 1 & \text{if} \quad a_i \text{ lies in } S_u, \\ 0 & \text{if} \quad a_i \text{ does not lie in } S_u. \end{cases}$$

Next we put

$$L(u) = \max L(S_u),$$

where S_u ranges over all subsets of u elements. It is easily verified that $L(1) = 2$, $L(2) = 4$, and that $L(u) \geqslant u+2$ for $u \geqslant 2$. It is also clear that $L(u+1) \geqslant L(u)$.

Our next step is to prove the inequality

$$\text{(I.3)} \qquad L(u+1) \geqslant L(u) + \tfrac{1}{6}(u+2) \quad \text{for} \quad 2 \leqslant u \leqslant \tfrac{1}{2}k - 1$$

provided that $L(u) < \frac{1}{2}p$.

We assume that S_u is the set for which $L(S_u) = L(u)$. Then we have $L(u)$ residue classes $b_1, \ldots, b_{L(u)}$ which are representable as linear combinations of the a_j in S_u with coefficients 0 or 1. We also have at our disposal $m = u+2$ residue classes a_i not in S_u with $1 \leqslant i \leqslant 2u+2$. Lemma I.1 is applicable as

$$m = u+2 \leqslant L(u) < \tfrac{1}{2}p.$$

So we obtain an i in $1 \leqslant i \leqslant 2u+2$ such that a_i not in S_u,

$$B(a_i) < \tfrac{1}{6} m.$$

We now define S_{u+1} as the union of S_u and a_i. Then, by Lemma I.1,

$$L(u+1) \geqslant L(S_{u+1}) = L(u) + \big(l - B(a_i)\big) > L(u) + \tfrac{1}{6} m$$

which proves (I.3).

By addition, it follows immediately from (I.3) that either $L(u) \geqslant \frac{1}{2}p$ or that

$$L(u) \geqslant 4 + \sum_{n=2}^{u-1} \tfrac{1}{6}(n+2) > \tfrac{1}{12}(u+1)(u+2)$$

for all $u \leqslant \frac{1}{2}k$. Hence, putting $t = [(6p)^{1/2}]$, we have in any case

$$L(t) \geqslant \tfrac{1}{2}p.$$

Further we may assume that S_t contains $a_1, \ldots, a_t$.

We now apply the same argument to the $2t$ residue classes $a_{t+1}, \ldots, a_{3t}$. Again a linear combination of at most t of them will represent at least half the residue classes $\bmod p$.

Thus we have 2 (not necessarily disjoint) sets each containing at least half the residue classes $\bmod p$. From this it follows at once that every N is representable as a sum of an element of the first set and of an element of the second set. This completes the proof of Theorem I.

Proof of Theorem II. We start by introducing some notations. Small latin letters denote rational integers, and therefore by implication residue classes $\bmod p$. Small greek letters denote real numbers.

$$\Lambda = \log p, \quad p^{2/3} < k < p,$$

but until we reach Lemma II.5 it will be assumed that $k < p^{2/3}\Lambda$. The letter m with or without suffices will denote an integer in the interval $\frac{1}{4}k \leqslant m \leqslant k$. S_k is a given sequence of k non-zero distinct residue classes $\bmod p$, denoted by $a_1, \ldots, a_k$. For some permissible values of m we shall introduce subsequences S_m which we denote, without fear of misunderstanding, by $a_1, \ldots, a_m$.

For $r \not\equiv 0 \pmod p$ we put

$$\sigma(r) = \sigma(r, S_m) = \sum_{n=1}^{m} \sin^2(\pi r a_n/p),$$

$$\gamma(r) = \gamma(r, S_m) = \sigma(r, S_m)(m^3 p^{-2})^{-1}.$$

We note that $\gamma(r) \geqslant \gamma_0 > 0$, where γ_0 is an absolute constant. For given S_m we call r *critical* if $\gamma(r, S_m) < \Lambda$.

The symbol O implies absolute constants only. The symbol o refers to $p \to \infty$ uniformly in all other variables, unless stated otherwise.

If for S_k no value of r is critical, we take no further steps until we reach Lemma II.5. Otherwise we define

$$\mu = \operatorname{Min} \gamma(r, S_m)(\Lambda^6 + k - m),$$

where we admit all residue classes $r \not\equiv 0 \pmod p$, all m in $\frac{1}{2}k \leqslant m \leqslant k$ and all subsequences S_m of S_k containing m terms. For the remainder of the paper let s, m, S_m be the residue class s, the number m and the subsequence S_m for which the minimum is attained.

As some r is critical for S_k, it follows that

$$\mu \leqslant \operatorname*{Min}_{r \not\equiv 0} \gamma(r, S_k)\Lambda^6 < \Lambda^7.$$

As

$$\mu \geqslant \gamma_0(\Lambda^6 + k - m),$$

we have

$$\gamma_0(k - m + \Lambda^6) < \Lambda^7, \quad m > k - \gamma_0^{-1}\Lambda^7.$$

Further, for each subsequence $S_{m'}$ of S_m where $m' \geqslant \frac{1}{2}k$ we have

$$\gamma(r, S_{m'}) \geqslant \gamma(s, S_m).$$

LEMMA II.1. *Let* $r \not\equiv s \pmod{p}$ *be a critical value of* S_m. *Then there exist integers* u *and* v *such that* $vr \equiv us \pmod{p}$, $(u, v) = 1$, $1 \leqslant v \leqslant \Lambda$, $1 \leqslant u \leqslant \Lambda^2$.

Further, assuming that the residue classes sa_n $(1 \leqslant n \leqslant m)$ *are represented by numbers in the interval* $[-\frac{1}{2}p, \frac{1}{2}p]$, *these numbers are divisible by* v *with at most* $2\Lambda^5 m^3 p^{-2}$ *exceptions.*

Proof. Without loss of generality we may assume that $s = 1$ and that $|a_n| < \frac{1}{2}p$ for $1 \leqslant n \leqslant m$.

From Dirichlet's principle it follows by a classical argument that we can solve the congruence $vr \equiv u \pmod{p}$ subject to

$$1 \leqslant v \leqslant \Lambda, \quad 1 \leqslant |u| \leqslant p\Lambda^{-1}, \quad (u, v) = 1.$$

We write

$$vr = u + qp.$$

Because $s = 1$ is critical, the inequality

$$\sin^2(\pi a_n/p) \geqslant 4\Lambda m^2 p^{-2}$$

has at most $\frac{1}{4}m$ solutions. Similarly, because r is critical, the inequality

$$\sin^2(\pi r a_n/p) \geqslant 4\Lambda m^2 p^{-2}$$

has at most $\frac{1}{4}m$ solutions. Hence, for at least $m^* \geqslant \frac{1}{2}m$ values of a_n (say $a_1, \ldots, a_{m^*}$) we have

$$\sin^2(\pi a_n/p) < 4\Lambda m^2 p^{-2}, \qquad \sin^2(\pi r a_n/p) < 4\Lambda m^2 p^{-2};$$

$$|a_n| < \Lambda^{1/2} m, \qquad |ra_n - pg_n| < \Lambda^{1/2} m.$$

The last inequality, multiplied with v, gives

$$|ua_n - p(vg_n - qa_n)| < \Lambda^{1/2} mv \leqslant \Lambda^{3/2} m.$$

Putting

$$h_n = vg_n - qa_n,$$

this becomes

$$|ua_n - ph_n| < \Lambda^{3/2} m. \tag{II.1}$$

The sequence a_n contains m^* terms confined to the interval $[-\Lambda^{1/2} m, \Lambda^{1/2} m]$; hence it contains two terms a', a'' such that

$$1 \leqslant a'' - a' \leqslant 2\Lambda^{1/2} m (m^* - 1)^{-1} \leqslant 4\Lambda^{1/2} + o(1).$$

As by (II.1) for some h

$$|u(a''-a')-ph| < 2\Lambda^{3/2}m = o(p),$$

it follows that $h = 0$ since

$$|u(a''-a')| \leqslant |u|\big(4\Lambda^{1/2}+o(1)\big) \leqslant 4p\Lambda^{-1/2}+o(p) = o(p).$$

And $h = 0$ implies

$$|u| \leqslant |u|(a''-a') < 2\Lambda^{3/2}m.$$

If $|u| \leqslant \Lambda^2$, the first part of our lemma is proved. Hence we may assume

$$\Lambda^2 < |u| < 2\Lambda^{3/2}m. \tag{II.2}$$

We now consider all integers of the form ux where $|x| < \Lambda^{1/2}m$. They contain the sequence ua_n, $1 \leqslant n \leqslant m^*$.

We proceed to count how many of these x satisfy

$$|ux-ph_x| < \Lambda^{3/2}m \tag{II.3}$$

for some suitable integer h_x. If h_x is fixed, the number of x in the interval (II.3) is obviously

$$\leqslant 1+2|u|^{-1}\Lambda^{3/2}m.$$

On the other hand, it follows from $|x| < \Lambda^{1/2}m$ and (II.3) that

$$|h_x| \leqslant |u|\Lambda^{1/2}mp^{-1}+\Lambda^{3/2}mp^{-1}.$$

Hence the number of x in $|x| < \Lambda^{1/2}m$ satisfying (II.3) does not exceed

$$\begin{aligned}(1+2|u|^{-1}\Lambda^{3/2}m)&(1+2|u|\Lambda^{1/2}mp^{-1}+2\Lambda^{3/2}mp^{-1})\\ &\leqslant (1+2|u|^{-1}\Lambda^{3/2}m)(2+2|u|\Lambda^{1/2}mp^{-1})\\ &= 2+4\Lambda^2m^2p^{-1}+2|u|\Lambda^{1/2}mp^{-1}+4|u|^{-1}\Lambda^{3/2}m\\ &\leqslant 2+4\Lambda^2m^2p^{-1}+4\Lambda^2m^2p^{-1}+4\Lambda^{-1/2}m\\ &= o(m) < m^*.\end{aligned}$$

As the set of ux with $|x| < \Lambda^{1/2}m$ contains the set ua_n with $1 \leqslant n \leqslant m^*$, (II.1) is not true for all $n \leqslant m^*$. Thus (II.2) is disproved, and the first part of our lemma is established.

Next we note that $h_n = 0$ implies $v \mid a_n$. We now return to our original sequence S_m and remove from it all terms for which either

$$\sin^2(\pi a_n/p) \geqslant \Lambda^{-4} \quad \text{or} \quad \sin^2(\pi r a_n/p) \geqslant \Lambda^{-4}.$$

Then we have for the remaining terms

$$|a_n| \leqslant \pi^{-1}\Lambda^{-2}p\big(1+o(1)\big) \quad \text{and} \quad |ra_n - pg_n| \leqslant \pi^{-1}\Lambda^{-2}p\big(1+o(1)\big)$$

or, after multiplication with v, using our previous notation,

$$|ua_n - ph_n| \leqslant \pi^{-1}\Lambda^{-1}p\big(1+o(1)\big).$$

Hence

$$p\,|h_n| \leqslant |ua_n| + o(p) \leqslant \big(\pi^{-1}+o(1)\big)p < p,$$

$$h_n = 0, \qquad v \mid a_n.$$

The number of terms we have omitted is

$$\leqslant \Lambda^4\big(\sigma(1)+\sigma(r)\big) \leqslant 2\Lambda^5 m^3 p^{-2}.$$

This finishes the proof of the lemma.

LEMMA II.2. $v = 1$ *under the conditions of Lemma* II.1.

Proof. We have by Lemma II.1 a subsequence S_{m^*} of S_m represented by $a_1, \ldots, a_{m^*}$ say, such that

$$m^* \geqslant m - 2\Lambda^5 m^3 p^{-2},$$

$$-\tfrac{1}{2}p < sa_n < \tfrac{1}{2}p, \quad v \mid sa_n \quad \text{for} \quad 1 \leqslant n \leqslant m^*.$$

For this subsequence we have

$$\begin{aligned}\sigma(v^{-1}s) &= \sum_{n=1}^{m^*}\sin^2\big(\pi sa_n/(vp)\big) \leqslant v^{-2}\sum_{n=1}^{m^*}(\pi sa_n/p)^2 \\ &\leqslant v^{-2}(\tfrac{1}{2}\pi)^2\sum_{n=1}^{m^*}\sin^2(\pi sa_n/p) \leqslant (\tfrac{1}{2}v^{-1}\pi)^2\sum_{n=1}^{m}\sin^2(\pi sa_n/p) \\ &= (\tfrac{1}{2}v^{-1}\pi)^2\mu m^3 p^{-2} < \mu m^{*3}p^{-2}\end{aligned}$$

which for $v \geqslant 2$ contradicts the minimum definition of μ as

$$m^* \geqslant m(1-2\Lambda^5 m^2 p^{-2}) = m + o(m) \geqslant \tfrac{1}{2}k.$$

LEMMA II.3. *There exists an* m_0 *in the interval*

$$m - \Lambda^{21} m^3 p^{-2} \leqslant m_0 \leqslant m$$

and a subsequence S_{m_0} *of* S_m, *say* $a_1, \ldots, a_{m_0}$, *such that*

$$\sum_{n=1}^{m_0}\sin^4(\pi sa_n/p) \leqslant \Lambda^{-19} m^3 p^{-2}.$$

Proof. From the series

$$\sigma(s, S_m) = \sum_{n=1}^{m}\sin^2(\pi sa_n/p) \leqslant \Lambda m^3 p^{-2}$$

we remove all terms for which

$$|\sin(\pi s a_n/p)| \geqslant \Lambda^{-10}.$$

The number of terms removed is

$$m - m_0 \leqslant (\Lambda^{10})^2 \sigma(s, S_m) \leqslant \Lambda^{21} m^3 p^{-2}$$

and

$$\sum_{n=1}^{m_0} \sin^4(\pi s a_n/p) \leqslant \Lambda^{-20} \sum_{n=1}^{m_0} \sin^2(\pi s a_n/p)$$

$$\leqslant \Lambda^{-20} \sigma(s, S_m) \leqslant \Lambda^{-19} m^3 p^{-2}.$$

LEMMA II.4.

$$\sigma(s, S_m) = \mu m^3 p^{-2}; \tag{II.4}$$

$$\sigma(us, S_m) \geqslant u^2 \mu m_0^3 p^{-2} + O(\Lambda^{-11} m^3 p^{-2}) \quad \textit{for} \quad 1 \leqslant |u| \leqslant \Lambda^2, \tag{II.5}$$

where m_0 *is defined by Lemma* II.3;

$$\sigma(r, S_m) \geqslant \Lambda m^3 p^{-2} \quad \textit{for the other } r \not\equiv 0 \pmod p. \tag{II.6}$$

Proof. (II.4) follows from the minimum definition. (II.6) is a consequence of Lemma II.1 and Lemma II.2.

To prove (II.5) we note that for all $\alpha, t \neq 0$,

$$\sin^2(t\alpha) - t^2 \sin^2(\alpha) = O(t^4 \sin^4 \alpha). \tag{II.7}$$

(II.7) is true because for $0 \leqslant \alpha \leqslant |t|^{-1}$

$$\sin^2(t\alpha) = t^2\alpha^2 + O(t^4\alpha^4), \quad t^2 \sin^2 \alpha = t^2\alpha^2 + O(t^2\alpha^4),$$

whereas for $|t|^{-1} < \alpha \leqslant \frac{1}{2}\pi$

$$\sin^2(t\alpha) \leqslant 1 = O(t^2 \sin^2 \alpha) = O(t^4 \sin^4 \alpha).$$

From (II.7) and Lemma II.3 we obtain for $t \neq 0$

$$\sigma(ts, S_{m_0}) - t^2 \sigma(s, S_{m_0}) = O(t^4 \Lambda^{-19} m^3 p^{-2}).$$

This gives (II.5) as

$$\sigma(us, S_{m_0}) \leqslant \sigma(us, S_m), \quad \sigma(s, S_{m_0}) \geqslant \mu m_0^3 p^{-2}.$$

LEMMA II.5. *If* $\beta_r = \prod_{n=1}^{k} \cos(\pi r a_n/p)$, *then*

$$\sum_{r=1}^{p-1} |\beta_r| = o(1)$$

as $p \to \infty$, $kp^{-2/3} \to \infty$.

Proof. We note first that if $k < \Lambda p^{2/3}$, then m and m_0 are defined and

$$\lim_{p\to\infty} mk^{-1} = 1, \quad \lim_{p\to\infty} m_0 m^{-1} = 1.$$

For $r \not\equiv 0 \pmod p$ we have

$$|\beta_r| \leqslant \prod_{n=1}^{m} |\cos(\pi r a_n/p)| \leqslant \Big\{m^{-1}\sum_{n=1}^{m}\cos^2(\pi r a_n/p)\Big\}^{m/2}$$
$$= \{1-m^{-1}\sigma(r, S_m)\}^{m/2} \leqslant e^{-(1/2)\sigma(r,S_m)}.$$

Hence if r is not critical for S_m, (II.6) is applicable and

$$|\beta_r| \leqslant e^{-(1/2)\Lambda m^3 p^{-2}} \leqslant p^{-2},$$

as eventually $m^3p^{-2} \geqslant 4$.

If (II.4) is applicable, it gives

$$|\beta_s| = |\beta_{-s}| \leqslant e^{-(1/2)\mu m^3/p^2} \leqslant e^{-(1/2)\gamma_0 m^3/p^2} = o(1),$$

whereas (II.5) if applicable gives for $2 \leqslant |u| \leqslant \Lambda^2$

$$|\beta_{us}| \leqslant e^{-(1/2)u^2\mu m_0^3 p^{-2} + O(\Lambda^{-11}m^3p^{-2}} \leqslant e^{-(1/2)|u|\gamma_0 m^3 p^{-2}},$$

$$\sum_{2\leqslant|u|\leqslant\Lambda^2} |\beta_{us}| \leqslant 2\sum_{u=2}^{\infty} e^{-(1/2)u\gamma_0 m^3p^{-2}} = 2e^{-\gamma_0 m^3 p^{-2}}(1-e^{-(1/2)\gamma_0 m^3 p^{-2}})^{-1} = o(1).$$

This completes the proof of Lemma II.5 if $k < \Lambda p^{2/3}$ and if at least one r is critical for S_k.

Otherwise, we still have for $r \not\equiv 0 \pmod p$

$$|\beta_r| \leqslant e^{-(1/2)\sigma(r,S_k)}.$$

If $k < \Lambda p^{2/3}$ and no critical r exists, we have

$$|\beta_r| < e^{-(1/2)\sigma(r,S_k)} \leqslant e^{-(1/2)\Lambda k^3 p^{-2}} < p^{-2}$$

eventually. Finally, if $k \geqslant \Lambda p^{2/3}$,

$$\sigma(r, S_k) \geqslant 2 \sum_{1\leqslant n\leqslant(k+1)/2} \sin^2(\pi n/p) \geqslant 8 \sum_{1\leqslant n\leqslant(k+1)/2} n^2 p^{-2}$$
$$= \tfrac{1}{3}k^3p^{-2}\big(1+o(1)\big) > \tfrac{1}{4}\Lambda^3$$

and

$$|\beta_r| < e^{-\Lambda^3/8} < e^{-2\Lambda} = p^{-2}$$

eventually. This completes the proof of the lemma.

Proof of Theorem II. Put $A = \sum_{n=1}^{k} a_n$. Then

$$F(N) = p^{-1}\sum_{r=0}^{p-1} e^{-2\pi i r N/p}\prod_{n=1}^{k}(1+e^{2\pi i r a_n/p})$$

$$= p^{-1}2^k \sum_{r=0}^{p-1} e^{\pi i r(A-2N)/p}\beta_r,$$

$$|F(N)-p^{-1}2^k| \leqslant p^{-1}2^k \sum_{r=1}^{p-1}|\beta_r| = o(p^{-1}2^k)$$

by Lemma II.5. This proves the theorem.

Finally, if k is even, $p^{2/3} \leqslant k \leqslant O(p^{2/3})$

$$a_1 = 1,\ a_2 = -1,\ a_3 = 2,\ a_4 = -2,\ \ldots,\ a_{k-1} = \tfrac{1}{2}k,\ a_k = -\tfrac{1}{2}k,$$

then $A = 0$, $\beta_r \geqslant 0$. Hence

$$F(0) = p^{-1}2^k\Big(1+\sum_{r=1}^{p-1}\beta_r\Big) \geqslant p^{-1}2^k(1+\beta_1).$$

An easy calculation shows that

$$\beta_1 = \prod_{n=1}^{k/2}\cos^2(\pi n/p) \sim e^{-(24)^{-1}\pi^2k^3p^{-2}},$$

which does not tend to zero. This shows that Theorem II is best possible.

Unproved Conjectures.

CONJECTURE 1. *It is possible to replace the constant* $3\cdot 6^{1/2}$ *in Theorem* I *by the constant* 2.

This is fairly plausible. Let S_k^* be the sequence

$$a_1 = 1,\ a_2 = -1,\ a_3 = 2,\ a_4 = -2,\ \ldots,\ a_k = (-1)^{k-1}[\tfrac{1}{2}(k+1)]$$

and let $G(S_k)$ be the number of residue classes N for which

$$F(N; p; S_k) = F(N; p; a_1, \ldots, a_k) > 0.$$

Then we can state

CONJECTURE 2. $G(S_k) \geqslant G(S_k^*)$ *for all* $k \geqslant 1$.

This would of course imply Conjecture 1.

For composite moduli Theorem I and II cease to be true. It is however reasonable to formulate

CONJECTURE 3. $F(0) > 0$ *for* $k > 2p^{1/2}$, *where* p *is not necessarily a prime.*

This conjecture may also be true for finite abelian groups of composite order p, and possibly even, *mutatis mutandis*, for non-abelian groups.

Finally we mention a more complicated, but probably easier problem.

CONJECTURE 4. *Let $n, s, l_1, \ldots, l_s$ be positive integers, such that $l_1 + \ldots + l_s = n$. Let $a_\lambda^{(\sigma)}$ $(1 \leqslant \sigma \leqslant s,\ 1 \leqslant \lambda \leqslant l_\sigma)$ be n residue classes* mod n *such that $a_\lambda^{(\sigma)} \not\equiv a_\mu^{(\sigma)} (\operatorname{mod} n)$ for $1 \leqslant \mu < \lambda \leqslant \sigma$. Then there exists a nonvoid subset T of the integers $1 \leqslant \sigma \leqslant s$, such that for σ in T we can choose a $\lambda(\sigma)$ in $1 \leqslant \lambda \leqslant l_s$ with the effect that*

$$\sum_{\sigma \text{ in } T} a_{\lambda(\sigma)}^{(\sigma)} \equiv 0 (\operatorname{mod} n).$$

As the paper goes to press Dr Flor informs us that Conjecture 4 follows from a recent result by P. Scherk [2]. We also want to draw the attention of the reader to a theorem by P. Erdös, A. Ginzburg and A. Ziv [3] which states that each set of $2n-1$ integers contains a sub-set of n integers, the sum of which is divisible by n.

References

[1] H. Davenport, *On the addition of residue classes*, Journ. London Math. Soc. 10 (1935), pp. 30-32.

[2] P. Scherk, *Distinct elements in a set of sums*, Amer. Math. Monthly 62 (1955), pp. 46-47.

[3] P. Erdös, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel, 10F (1961), pp. 41-43.

Reçu par la Rédaction le 22. 8. 1963