PACIFIC JOURNAL OF MATHEMATICS
Vol. 26, No. 2, 1968

THE ADDITION OF RESIDUE CLASSES MODULO n

CHARLES RYAVEC

In the present paper, the following is proved:

THEOREM. Let $a_1, \cdots, a_m$ be m distinct, nonzero residues modulo n, where n is any natural number and where

$$m \geqq 3\sqrt{6n} \exp\left\{c\frac{\sqrt{\log n}}{\log\log n}\right\},$$

where $c > 0$ is some large constant. Then the congruence

$$\varepsilon_1 a_1 + \cdots + \varepsilon_m a_m \equiv 0 \,(\mathrm{mod}\, n)$$

is solvable with $\varepsilon_i = 0$ or 1 and not all $\varepsilon_i = 0$.

The method of proof is completely elementary, in that it is based upon well-known results concerning the addition of residues modulo a natural number n and upon results from elementary number theory.

In a recent paper by Erdös and Heilbronn (see [1]) the following question is investigated. Let p be a prime and $a_1, \cdots, a_m$ distinct, nonzero residue classes modulo p, and N any residue class modulo p. Let $F(N) = F(N; p; a_1, \cdots, a_m)$ denote the number of solutions of the congruence

$$(1) \qquad \varepsilon_1 a_1 + \cdots + \varepsilon_m a_m \equiv N \,(\mathrm{mod}\, p),$$

where the ε_i are restricted to the values 0 or 1. What can be said about the function $F(N)$? The authors prove the following result:

THEOREM 1. *$F(N) > 0$ if $m \geqq 3\sqrt{6p}$.*

They conjecture that the bound $3\sqrt{6p}$ in Theorem 1 is not best possible: $3\sqrt{6p}$ can probably be replaced by $2\sqrt{p}$. On the other hand, they show that the constant 2 cannot be replaced by any smaller constant, as shown by the example

$$a_1 = 1, \quad a_2 = -1, \cdots, \quad a_m = (-1)^{m-1}\left[\frac{m+1}{2}\right].$$

Note that if $m < 2\cdot(\sqrt{p} - 2)$, $F(1/2(p-1) = 0$.

The question which now arises is what can be said about $F(N)$ if the prime p is replaced by a composite integer n? Theorem 1 is clearly false for composite n. In fact, even the bound $m \geqq -1 + n/2$ will not guarantee that $F(N) > 0$ for all N when n is composite. The difficulty is that all of the a_i may have a prime factor in common with n, in which case $N = 1$ could not be represented in the form

(1). However, this predicament does not arise when we try to represent 0 in the form (1). Therefore, it is natural to ask what condition on m will guarantee $F(0) > 0$ for all n. Erdös and Heilbronn conjectured that $F(0) > 0$ provided $m > 2\sqrt{n}$;[1] and at a conference at Ohio State University Erdös raised the question whether $F(0) > 0$ could be proved if one assumed the stronger hypothesis $m > K \cdot n^{(1/2)+\varepsilon}$, where ε is any positive number, and K is some absolute constant.

Since the expression $\exp\{c \cdot (\sqrt{\log n})/(\log\log n)\}$ is $O(n^{\varepsilon})$ for any $\varepsilon > 0$, the theorem of this paper answers Erdös' question.

2. Necessary lemmas.

In order to prove the theorem a number of lemmas will be needed. They are rather straightforward modifications of those given in [1] for the case when n is a prime.

LEMMA 1. *Let $b_1, \cdots, b_l$ be l distinct residues* modulo n; *and let $B(x)$ denote the number of solutions of*

$$x \equiv b_i - b_j \pmod{n}$$

with $1 \leqq i, j \leqq l$. Then $B(x + y) \geqq -l + B(x) + B(y)$; i.e.,

$$l - B(x + y) \leqq (l - B(x)) + (l - B(y)) .$$

Proof. See [1], page 150.

LEMMA 2. *Let $1 \leqq k \leqq l \leqq n/2$, $n \geqq 2$, and let $d_1, \cdots, d_k$ be k distinct nonzero residues* modulo n *such that $(d_i, n) = 1$. Let $b_1, \cdots, b_l$ be l distinct residues* modulo n. *Then there is an i, $1 \leqq i \leqq k$, such that*

$$B(d_i) < l - k/6 ,$$

where $B(d_i)$ is the number of solutions of

$$d_i \equiv b_s - b_t \pmod{n} .$$

Proof. Let G denote the cyclic group of residues modulo n, and let $A = \{0, d_1, \cdots, d_k\}$. Put $r = 1 + [(2l/k)]$. By I. Chowla's theorem on the addition of residues modulo n (see [2], Corollary 1. 2. 4 (p. 3)), one obtains

$$\begin{aligned} |2A| &\geqq |A| + |A| - 1 = 2k + 1 \\ &\vdots \\ |rA| &\geqq rk + 1 , \end{aligned}$$

[1] Relative to this conjecture, we mention an unpublished result of Mann and Olson (see [3]). They have shown that if G is a group of type (p, p) and $a_1, \cdots, a_m$ are distinct elements of G, then $F(g) > 0$ for every $g \in G$ if $m \geqq 2p = 2\sqrt{|G|}$.

provided $jA \neq G$ for $1 \leqq j \leqq r$. Hence, we obtain $t \geqq \min(n-1, rk)$ distinct, nonzero residues $c_1, \cdots, c_t$ modulo n which can be expressed as sums of not more than r of the d_j; and the summands need not be distinct

Since $\sum_{1 \leqq s \leqq t} B(c_s) \leqq B(1) + \cdots + B(n-1) = l(l-1)$, there is an s such that

$$\begin{aligned} B(c_s) &\leqq \frac{l(l-1)}{t} \\ &\leqq l(l-1) \max\left\{\frac{1}{n-1}, \frac{1}{rk}\right\} \\ &\leqq \frac{l(l-1)}{2l-1} = \frac{l}{2} \frac{l-1}{l-\frac{1}{2}} < \frac{l}{2} ; \end{aligned}$$

i.e., $l - B(c_s) > l/2$.

By using induction on the conclusion of Lemma 1, we obtain

$$l - B(x_1 + \cdots + x_t) \leqq \sum_{i=1}^{t} (l - B(x_i)) . \tag{2}$$

By construction, $c_s \equiv \sum_{i=1}^{r} \varepsilon_i d_{j_i} \pmod{n}$ is solvable with not all $\varepsilon_i = 0$. Rewrite the above expression as $c_s \equiv \sum_{i=1}^{r_1} d_{j_i} \pmod{n}$, where we have suppressed those terms in the sum for which $\varepsilon_i = 0$. Applying (2) we obtain

$$\frac{l}{2} < l - B(c_s) \leqq \sum_{i=1}^{r} (l - B(d_{j_i})) .$$

Therefore, one obtains a d_i such that

$$l - B(d_i) > \frac{l}{2r_1} \geqq \frac{l}{2r} \geqq \frac{lk}{2(k+2l)} \geqq \frac{k}{6} ,$$

since $1 \leqq r_1 \leqq r$.

Now let $1 \leqq d_1 < d_2 < \cdots < d_\nu \leqq n-1$ be ν distinct, nonzero residues modulo n such that $(d_i, n) = 1$. For $1 \leqq u \leqq \nu/2$, consider all possible subsets, S_u, of u elements from the set $\{d_1, \cdots, d_{2u}\}$. For each subset S_u, let $L(S_u)$ denote the number of distinct residue classes modulo n which can be obtained in the form $\varepsilon_1 d_1 + \cdots + \varepsilon_{2u} d_{2u}$, where not all $\varepsilon_i = 0$ and where $\varepsilon_i = 0$ or 1 and $\varepsilon_i = 0$ if d_i is not in S_u. Note that determining $L(S_u)$, we do not include the residue class 0 unless it can be expressed as the sum of $\leqq u$ distinct elements of S_u.

Finally, put $L(u) = \operatorname{Max}(L(S_u))$, where the maximum is taken over all subsets, S_u, of u elements from the set $\{d_1, \cdots, d_{2u}\}$.

LEMMA 3. *Let* $d_1, \cdots, d_\nu$ *satisfy the properties in the above definition. If*

$$\varepsilon_1 d_1 + \cdots + \varepsilon_\nu d_\nu \equiv 0 \pmod{n}$$

implies that all $\varepsilon_i = 0$, *then*

$$L(u+1) \geqq L(u) \quad \textit{when} \quad u \geqq 1 \tag{3}$$

$$L(u) \geqq u + 2 \qquad \textit{when} \quad u \geqq 3\,, \qquad \textit{for } n \geqq 4\,. \tag{4}$$

Proof. (3) is obvious. In order to prove (4), it may be assumed without loss of generality that the maximum, $L(u)$, is obtained from $d_1, \cdots, d_u$, which are distinct modulo n by assumption. Also, $d_1 + \cdots + d_u$ is distinct from them by the assumption that

$$\varepsilon_1 d_1 + \cdots + \varepsilon_\nu d_\nu \equiv 0(n)$$

is impossible unless all $\varepsilon_i = 0$. Now let $T = \{d_1 + d_i \mid 2 \leqq i \leqq u\}$. Each element of T is distinct from $d_1 + \cdots + d_u$, when $u \geqq 3$, and from d_1. It will be shown that at least one element of T is distinct from all of $d_1, \cdots, d_u$. This element, in addition to the $u + 1$ elements $d_1, \cdots, d_u, d_1 + \cdots + d_u$ will give $u + 2$ distinct residues modulo n, which proves (4), provided $u \geqq 3$.

So assume that no element of T is distinct from $d_1, \cdots, d_u$, and let $d_1 + d_i = d_j$, where j is a function of i. It is clear that

$$\{d_j \mid 2 \leqq j \leqq u\} = \{d_2, \cdots, d_u\}\,,$$

since no two d_j are congruent modulo n and none are congruent to d_1. Consequently,

$$\sum_{i=2}^{u} (d_1 + d_i) \equiv \sum_{j=2}^{u} d_j \pmod{n}\,.$$

Therefore, $(u-1)d_1 \equiv 0 \pmod{n}$, which is impossible since $(d_1, n) = 1$, and

$$2 \leqq u - 1 < \nu - 1 \leqq n - 2\,.$$

LEMMA 4. *Let* $d_1, \cdots, d_u, \cdots, d_\nu$ *satisfy the same conditions as in Lemma* 3. *For* $3 \leqq u \leqq -1 + \nu/2$, *either* $L(u) > n/2$ *or*

$$L(u+1) > L(u) + \frac{u+2}{6}\,.$$

Proof. If $L(u) > n/2$ we are finished. So assume that $L(u) \leqq n/2$. Now let S_u be a set for which $L(u) = L(S_u)$. So we have $L(u)$ distinct residue classes $b_1, \cdots, b_{L(u)}$ modulo n which are representable as sums of distinct elements from S_u. We have $\nu - u \geqq 1 + \nu/2 \geqq u + 2$ other elements d_i which are not in S_u. Select $u + 2$ of these and, if necessary, relabel them as $d_1, \cdots, d_{u+2}$. Since $1 \leqq u + 2 \leqq L(u) \leqq n/2$, we can apply Lemma 2 to the sets $\{b_1, \cdots, b_{L(u)}\}$ and $\{d_1, \cdots, d_{u+2}\}$, where $k = u + 2$, $l = L(u)$. Hence, we obtain an i, $1 \leqq i \leqq u + 2$ for which $B(d_i) < L(u) - (u + 2)/6$, where $B(d_i)$ is the number of representations of d_i in the form

$$d_i \equiv b_j - b_h \pmod n .$$

Putting $S_{u+1} = S_u \cup \{d_i\}$, we have

$$L(u + 1) \geqq L(S_{u+1}) = L(u) + (L(u) - B(d_i)) > L(u) + \frac{u + 2}{6} .$$

LEMMA 5. *As before, let* $1 \leqq d_1 < \cdots < d_\nu \leqq n - 1$ *be* ν *distinct, nonzero residues modulo* n *such that* $(d_i, n) = 1$. *Then if* $\nu \geqq 3\sqrt{6n}$, *the congruence*

$$\varepsilon_1 d_1 + \cdots + \varepsilon_\nu d_\nu \equiv 0 \pmod n$$

is solvable with not all $\varepsilon_i = 0$.

Proof. Assume that $\varepsilon_1 d_1 + \cdots + \varepsilon_\nu d_\nu \equiv 0 \pmod n$

with $\varepsilon_i = 0$ or 1, implies

that all $\varepsilon_i = 0$. We will then obtain a contradiction. By Lemma 4, either $L(u) > n/2$ or

$$L(u) > \sum_{\lambda=3}^{u-1} \left(\frac{\lambda + 2}{6}\right) + L(3) \geqq \frac{u^2 + 3u + 42}{12} ,$$

which is larger than $n/2$ provided $u \geqq \sqrt{6n}$. Therefore, with $u \geqq \sqrt{6n}$, we have $L(u) > n/2$ in either case. But we have $\nu \geqq 3\sqrt{6n}$ distinct residues. Applying the preceding analysis to the more than $2\sqrt{6n}$ remaining residues, we obtain $L(u) > n/2$ for this set also.

Therefore, we have two, not necessarily disjoint, sets each with more than $n/2$ residues modulo n. Call these two sets A, B. By a well-known argument, either $A + B = G$ or

$$|G| \geqq |A| + |B| > n/2 + n/2 = n .$$

Therefore, $A + B = G$; and we conclude that 0 is representable as the sum of distinct elements from $\{d_1, \cdots, d_\nu\}$. This contradicts our original assumption that 0 is not so represented. Therefore,

$$\varepsilon_1 d_1 + \cdots + \varepsilon_\nu d_\nu \equiv 0 \pmod n$$

is solvable nontrivially.

3. **Proof of theorem.** For each divisor d of n, let $\Phi(d) = \{a_i \mid d = (a_i, n)\}$. Put $\Phi(d) = \{c_1, \cdots, c_h\}$, where h and the c_j depend on d, although this dependence is suppressed without loss of clarity.

For each $c_j \in \Phi(d)$, we have $c_j = dc'_j$, where $(n/d, c'_j) = 1$. Furthermore, since the c_j are distinct modulo n, the c'_j are distinct modulo n/d, and they satisfy

$$1 \leqq c'_1 < \cdots < c'_h \leqq \left[\frac{n-1}{d}\right] = \frac{n}{d} - 1 .$$

Therefore, by Lemma 5, if $h \geqq 3\sqrt{6n/d}$, the congruence

$$\varepsilon_1 c'_1 + \cdots + \varepsilon_h c'_h \equiv 0 \pmod{n/d}$$

is solvable nontrivially, in which case the congruence $\varepsilon_1 c_1 + \cdots + \varepsilon_h c_h \equiv 0 \pmod{n}$ is solvable nontrivially.

So if $m = \sum_{d/n} |\Phi(d)| \geqq \sum_{d/n} 3\sqrt{6n/d}$, then for some d, $\Phi(d)$ will contain more than $3\sqrt{6n/d}$ distinct elements modulo n such that $\{(a_i/d), (n/d)\} = 1$. Thus, the congruence $\varepsilon_1 a_1 + \cdots + \varepsilon_m a_m \equiv 0 \pmod{n}$ will be solvable nontrivially.

We now obtain an upper bound for $\sum_{d/n} 3\sqrt{6n/d}$ in terms of n. Suppose $p^{e_p} \| n$. Then we have

$$\begin{aligned}\sum_{d/n} 3\sqrt{6n/d} &= 3\sqrt{6n} \sum_{d/n} d^{-(1/2)} \\ &= 3\sqrt{6n} \prod_{p/n} (1 + p^{-(1/2)} + \cdots + (p^{e_p})^{-(1/2)}) \\ &< 3\sqrt{6n} \prod_{p/n} (1 - p^{-(1/2)})^{-1} .\end{aligned}$$

Put $f(n) = \prod_{p/n} (1 - p^{-(1/2)})^{-1}$ and choose the prime $q = q(n)$ such that $\eta = \prod_{p \leqq q} p \leqq n < q' \prod_{p \leqq q} p$, where q' is the smallest prime greater than q. Clearly $f(\eta) \geqq f(n)$. Now

$$\begin{aligned}\log (f(\eta)) &= -\sum_{p \leqq q} \log (1 - p^{-(1/2)}) = \sum_{p \leqq q} p^{-(1/2)} + O(1) \\ &= O\Big(\sum_{p \leqq q} p^{-(1/2)}\Big) = O\Big(\frac{\sqrt{q}}{\log q}\Big) .\end{aligned}$$

But $\log \eta = \sum_{p \leqq q} \log p = \delta(q) \leqq \log n$. It is well known that there exist positive constants α and β such that

$$\alpha q \leqq \delta(q) \leqq \beta q$$

for all primes q. Hence, we conclude that $\log n \geqq \alpha \cdot q$. Also, $\eta' = \eta \cdot q' > n$, which implies that $\log \eta' > \log n$. But $\log \eta' = \delta(q') \leqq \beta q' = \beta q(q'/q) \leqq \gamma q$, for some constant $\gamma > 0$. Therefore, $\log q \geqq \gamma_1 \cdot \log \log n$;

and so

$$f(n) \leqq f(\eta) \leqq \exp\left\{c\frac{\sqrt{\log n}}{\log\log n}\right\},$$

where $c > 0$ is some positive constant.

BIBLIOGRAPY

1. P. Erdös, and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arithmetika **7** (1964), 149-159.
2. H. B. Mann, *The Addition Theorems of Number Theory and Group Theory*, New York, Interscience Publishers, 1965.
3. H. B. Mann, and J. E. Olson, *Sums of Sets in the Elementary Abelian Group of Type* (p, p), Math Research Center, United States Army, Madison, Wisconsin.

Received November 27, 1967.

UNIVERSITY OF EASTERN MICHIGAN