ACTA ARITHMETICA
LXV.2 (1993)

Sums of distinct residues mod p

by

Öystein J. Rödseth (Bergen)

1. Introduction. Given distinct residue classes $a_1, a_2, \ldots, a_k$ modulo a prime p, let s denote the number of distinct residue classes of the form $a_i + a_j$, $i \neq j$. An old conjecture of Erdős and Heilbronn states that (cf. Erdős [7, p. 410] and Guy [11, p. 73])

$$s \geq \min(p, 2k-3)\,. \tag{1}$$

Erdős and Graham [8, p. 95] refer this problem to the paper [9] of Erdős and Heilbronn, but the conjecture (1) is not explicitly stated in [9]. Erdős and Heilbronn are, however, considering closely related problems and it does seem reasonable that the problem (1) was raised during their work on the paper [9].

If $a_i = a + id$, $i = 0, 1, \ldots, k-1$, for some residue classes a and d, then (1) holds with equality. Hence, if (1) is true, it is certainly best possible. Some sufficient conditions for (1) to hold can be found in [1], [2], [15]. In particular, Rickert [15] shows that (1) holds if $k \leq 12$ or if $p \leq 2k+3$. He also shows that (1) holds if $p > 6 \cdot 4^{k-4}$.

In addition, it is a rather immediate consequence of the Cauchy–Davenport Theorem that (see Section 2)

$$s \geq \min(p, \tfrac{3}{2}k-2)\,. \tag{2}$$

In this note we show the two theorems below. Both are easy consequences of results in the literature. The first theorem follows from Pollard's (simple and elegant) extension [13] of the Cauchy–Davenport Theorem, the second from a (deep) result of Freiman [10].

Theorem 1. $s \geq \min(p, 2k-(4k+1)^{1/2})$.

Theorem 2. *There exists an absolute constant c such that if $p > ck$, then $s \geq 2k-3$.*

2. Proof of Theorem 1. Let A, B be non-empty sets of residue classes mod p. We use $|A|$ to denote the number of elements in A, and $A+B$ is the set of sums $a+b$, $a \in A$, $b \in B$. Further, we write xA for the set of elements xa, $a \in A$, x an integer or a residue class. In particular, $-A = (-1)A$ and $A - B = A + (-B)$. For a residue class y we also write y for the singleton set $\{y\}$.

Let $\nu(x) = \nu_{A,B}(x)$ denote the number of distinct representations of the residue class x as $x = a + b$, $a \in A$, $b \in B$. Then

$$\nu(x) = |A \cap (x - B)| \,. \tag{3}$$

Further, for a positive integer r, let $N_r = N_r(A, B)$ denote the number of distinct residue classes x satisfying $\nu(x) \geq r$. Then $N_1 = |A + B|$, and

$$p \geq N_1 \geq N_2 \geq \ldots \tag{4}$$

If $N_r \neq p$, then there is a residue class x for which $\nu(x) \leq r - 1$. Hence by (3),

$$p \geq |A \cup (x - B)| = |A| + |x - B| - \nu(x) \geq |A| + |B| - r + 1\,;$$

that is,

$$p \geq |A| + |B| - r + 1 \quad \text{ if } N_r \neq p\,. \tag{5}$$

The theorem of Pollard [13] states that

$$N_1 + N_2 + \ldots + N_r \geq r \min(p, |A| + |B| - r) \tag{6}$$

for $r = 1, 2, \ldots, \min(|A|, |B|)$. For $r = 1$, this is the Cauchy–Davenport Theorem [3], [5], [6].

Now, let $a_1, \ldots, a_k$ be distinct residue classes $\bmod\, p$, and let $A = B = \{a_1, \ldots, a_k\}$. Suppose that $k > 1$, and consider the $k \times k$ matrix $M = (m_{ij})$, where $m_{ij} = a_i + a_j$. Putting $t = N_1$, we have that t is the number of distinct entries in M, and N_2 is the number of distinct residue classes which appear at least twice in M. Since M is symmetric, N_2 thus equals the number of distinct residue classes outside the main diagonal; hence $N_2 = s$.

By (5) we thus have

$$p \geq 2k - 1 \quad \text{ if } s \neq p\,. \tag{7}$$

Moreover, since $s \geq |(a_i + A) \cup (a_j + A)| - 2$ for all i and j, we have

$$s \geq 2k - 2 - |(a_i + A) \cap (a_j + A)| = 2k - 2 - \nu_{A,-A}(a_i - a_j)\,,$$

so that

$$s \geq 2k - 2 - m\,, \tag{8}$$

where

$$m = \min_{0 \neq x \in A - A} \nu_{A,-A}(x)\,.$$

Suppose that $s \neq p$. By (7) and the Cauchy–Davenport Theorem, we then have $|A-A| \geq 2k-1$. Since

$$k(k-1) = \sum_{0 \neq x \in A-A} \nu_{A,-A}(x) \geq (|A-A|-1)m\,,$$

we thus have $m \leq k/2$ and (2) follows by (8).

Alternatively, since the diagonal in the matrix M contains k elements we have

$$k + s \geq t\,, \tag{9}$$

and (2) follows by (9), (6) with $r = 2$, and (7).

We now prove Theorem 1. Suppose that $s \neq p$. By (6) and (7) we have $N_1 + N_2 + \ldots + N_r \geq r(2k-r)$ for the integer $r = \lceil ((4k+1)^{1/2} - 1)/2 \rceil$. Using (4) and (9), we get $k + rs \geq r(2k-r)$, and an easy calculation gives Theorem 1.

We remark that some of the results in this section also hold for the additive group of residue classes mod p replaced by more general structures. A result corresponding to (5) holds in an arbitrary quasi-group (cf. McWorter [12]). Also, if p is replaced by an arbitrary positive integer n, then (2) holds if $\gcd(a_i - a_j, n) = 1$ for some fixed i and all $j \neq i$. For in this case we can use the Cauchy–Davenport–Chowla Theorem [4] instead of the Cauchy–Davenport Theorem in the argument above. Finally, Pollard's result (6) also hold if $\gcd(a_i - a_j, n) = 1$ for all i and j, $j \neq i$ (cf. [14]). Therefore Theorem 1 also holds $\bmod n$ as long as this condition is satisfied.

3. Proof of Theorem 2. For residue classes $x \neq 0$ and y, the set $xA+y$ is an *affine image* of A. The *affine diameter* of A is the smallest positive integer $d = d(A)$ such that the interval $[0, d-1]$ contains representatives of all elements of some affine image of A.

Now, the corollary of Freiman [10, p. 93] can be stated as follows: *There exists an absolute constant c such that if $t < 3k-3$ and $p > ck$, then* $d(A) \leq t - k + 1$.

By (9) we have $s \geq 2k-3$ if $t \geq 3k-3$. To prove Theorem 2 we may therefore assume that $t < 3k-3$. By Freiman's result there then exists an absolute constant $c \geq 4$ such that if $p > ck$, then $d(A) \leq 2k-3$. Since $s = s(A)$ is an affine invariant, i.e. $s(A') = s(A)$ for all affine images A' of A, we can assume that each a_i has an integer representative r_i such that $0 = r_1 < r_2 < \ldots < r_k \leq 2k-4$. Then all the $2k-3$ integers $r_1 + r_2 < r_1 + r_3 < \ldots < r_1 + r_k < r_2 + r_k < \ldots < r_{k-1} + r_k$ are distinct mod p, and the proof of Theorem 2 is complete.

Acknowledgments. This work was supported by the Norwegian Research Council for Science and the Humanities and by Alcatel Telecom Norway A/S. We also thank the Johannes Gutenberg-Universität in Mainz, Germany for its hospitality.

References

[1] W. Brakemeier, *Ein Beitrag zur additiven Zahlentheorie*, Dissertation, Tech. Univ. Braunschweig, 1973.
[2] —, *Eine Anzahlformel von Zahlen modulo n*, Monatsh. Math. 85 (1978), 277–282.
[3] A. L. Cauchy, *Recherches sur les nombres*, J. École Polytech. 9 (1813), 99–116.
[4] I. Chowla, *A theorem on the addition of residue classes*, Proc. Indian Acad. Sci. 2 (1935), 242–243.
[5] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. 10 (1935), 30–32.
[6] —, *A historical note*, ibid. 22 (1947), 100–101.
[7] P. Erdős, *Some problems in number theory*, in: Computers in Number Theory, A. O. L. Atkin and B. J. Birch (eds.), Academic Press, 1971, 405–414.
[8] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Enseign. Math., Genève, 1980.
[9] P. Erdős and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), 149–159.
[10] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Transl. Math. Monographs 37, Amer. Math. Soc., Providence, R.I., 1973.
[11] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1981.
[12] W. A. McWorter, *On a theorem of Mann*, Amer. Math. Monthly 71 (1964), 285–286.
[13] J. M. Pollard, *A generalisation of the theorem of Cauchy and Davenport*, J. London Math. Soc. 8 (1974), 460–462.
[14] —, *Addition properties of residue classes*, ibid. 11 (1975), 147–152.
[15] U.-W. Rickert, *Über eine Vermutung in der additiven Zahlentheorie*, Dissertation, Tech. Univ. Braunschweig, 1976.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BERGEN
ALLÉGT. 55
N-5007 BERGEN, NORWAY
E-mail: RODSETH@MI.UIB.NO

Received on 22.2.1993 (2386)