With (3.14) and (3.22) this yields the case $D < 0$ of our principal result.

THEOREM. *Let $f(x, y)$ be a binary cubic form, irreducible over the integers. Then there exist constants C_1, C_2, depending on f, such that, as $Z \to \infty$,*

$$\Sigma_1 = \sum_{|f(r,s)| \leqslant Z} d(|f(r, s)|) = C_1 Z^{2/3} \log Z + C_2 Z^{2/3} + O(Z^{9/14+\varepsilon}),$$

for any fixed $\varepsilon > 0$.

From (4.12), it appears that C_1 and C_2 are in fact given by

$$C_1 = \frac{\sqrt{3}}{|D|^{1/6}} \cdot \frac{\Gamma^2(\frac{1}{3})}{\Gamma(\frac{2}{3})} c_4, \qquad C_2 = \frac{\sqrt{3}}{|D|^{1/6}} \cdot \frac{\Gamma^2(\frac{1}{3})}{\Gamma(\frac{2}{3})} (2c_5 - c_4),$$

where c_4 and c_5 are as defined in (5.7), or as given by the alternative expressions (5.8). Since $c_4 \neq 0$, we have $C_1 \neq 0$, so the sum Σ_1 is in fact asymptotic to $C_1 Z \log Z$.

The proof for the case $D > 0$ is similar in principle, the principal differences relating to the definition of the appropriate function m. Furthermore the above expressions for C_1 and C_2 should be multiplied by a factor $\sqrt{3}$, as should the expression for c_3 in (4.12). We suppress all other details.

References

[1] R. Dedekind, Ges. Math. Werke, 1 Bd., pp. 202–232.
[2] P. Erdös, *On the sum $\sum d\{f(k)\}$*, J. London Math. Soc. 27 (1952), pp. 7–15.
[3] C. Hooley, *On the number of divisors of quadratic polynomials*, Acta Math. 110 (1963), pp. 97–114.
[4] — *On binary cubic forms*, J. Reine Angew. Math. 226 (1967), pp. 30–87.
[5] E. Landau, *Vorlesungen über Zahlentheorie*, 2, Hirzel 1927.
[6] — *Einfuhrung in die Theorie der Algebraische Zahlen*, Teubner 1928.
[7] T. Nagell, *Introduction to Number Theory*, New York 1951.
[8] H. Weyl, *Algebraic Theory of Numbers*, Princeton 1940.
[9] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) 21 (1922), pp. 235–255.

UNIVERSITY OF READING
Reading, Great Britain

Received on 3. 8. 1968

ACTA ARITHMETICA
XVII (1970)

Structure of maximal sum-free sets in C_p

by

H. P. YAP (Singapore)

1. Introduction and definitions. Let G be an additive group with non-empty subsets S and T. Let $S \pm T = \{s \pm t;\ s \in S, t \in T\}$ respectively, $\bar{S}$ be the set complement of S in G and $|S|$ be the cardinal of S. We abbreviate $\{f\}$, where $f \in G$, to f. If $S+S$ and S have no element in common, then we say that S is a sum-free set in G or that S is sum-free in G. If S is a sum-free set in G and if for every sum-free set T in G, $|S| \geqslant |T|$, then S is said to be a maximal sum-free set in G. We denote by $\lambda(G)$ the cardinal of a maximal sum-free set in G. We say that S is in arithmetic progression with the difference d if $S = \{s, s+d, \ldots, s+nd\}$ for some $s, d \in G$ and some integer $n \geqslant 0$.

Let C_p be the additive group of residues mod the prime p. In [5], we proved that $\lambda(C_p) = k+1$ if $p = 3k+2$ and $\lambda(C_p) = k$ if $p = 3k+1$. (We note that most of the results in [5] were generalized and improved by Diananda and Yap, see [1].) In [4], we proved that (i) if S is a maximal sum-free set in C_p, $p = 3k+2$, then $-S \equiv \{-s;\ s \in S\} = S$; (ii) there are altogether $(p-1)/2$ distinct maximal sum-free sets S_j, $j = 1, 2, \ldots \ldots, (p-1)/2$, in C_p, given by

$$S_j = \{js;\ s \in S_0\}, \quad j = 1, 2, \ldots, (p-1)/2,$$

where $S_0 = \{1+3i;\ i = 0, 1, \ldots, k\}$; and (iii) any two maximal sum-free sets in C_p are isomorphic.

In this note, we shall study the structural properties of maximal sum-free sets in C_p, $p = 3k+1$.

2. Main theorems. We shall make use of the following lemmas and theorems.

LEMMA 1. *Let $A = \{a+id;\ i = 0, 1, \ldots, r\}$ be a set of residues modulo m with $(d, m) = 1$ and $1 \leqslant r \leqslant m-3$. If $A = \{b+id';\ i = 0, 1, \ldots, r\}$, then $d' \equiv \pm d \pmod{m}$ ([3]).*

LEMMA 2. *Let $A = \{a+id;\ i = 1, 2, \ldots, r\}$ be a set of residues modulo m with $(d, m) = 1$ and $2 \leqslant r \leqslant (m+1)/2$. Then A can be written in only* *two ways in arithmetic progression form, namely, either*

$$A = \{a+id;\ i = 1, 2, \ldots, r\}$$

or

$$A = \{(a+(r+1)d)+i(-d);\ i = 1, 2, \ldots, r\}.$$

Proof. By Lemma 1, if $A = \{b+id';\ i = 1, 2, \ldots, r\}$, then $d' \equiv \pm d \pmod m$.

Now, suppose $A = \{b+id;\ i = 1, 2, \ldots, r\}$. If $b \neq a$, let $b+d = a+jd$, $1 < j \leqslant r$. Then

$$a+d \equiv b+hd \pmod m, \qquad h \in \{2, 3, \ldots, r\}$$

from which it follows that

$$(h+j-2)d \equiv 0 \pmod m, \qquad 1 < h, j \leqslant r$$

which is impossible.

Similarly, from $A = \{(a+(r+1)d)+i(-d);\ i = 1, 2, \ldots, r\}$, we can prove that if $A = \{b+i(-d);\ i = 1, 2, \ldots, r\}$, then $b = a+(r+1)d$.

The proof of Lemma 2 is complete.

THEOREM 1 (Cauchy–Davenport). *If A and B are non-empty subsets of a group G of prime order p, then*

$$A+B = G \quad \text{or} \quad |A+B| \geqslant |A|+|B|-1.$$

THEOREM 2 (Vosper). *Let G be the additive group of residues modulo a prime p. Let A, B be non-empty subsets of G and $C = A+B$. Then either $|C| \geqslant |A|+|B|$ or one of the following holds:* (i) $C = G$; (ii) $|C| = p-1$ *and* $\bar{B} = f-A$, *where* $f = \bar{C}$; (iii) *A and B are in arithmetic progression with the same difference*; (iv) $|A| = 1$ *or* $|B| = 1$.

In this note, the following two theorems will be proved.

THEOREM 3. *Let $p = 3k+1$ be a prime and S be a maximal sum-free set in $G = C_p$. If $-S \neq S$, then*

(A) $$S = \{a+id;\ i = 1, 2, \ldots, k\}$$

where $(x, y) = (a, d)$ is a nonzero solution of

(B) $$2x+(k-1)y \equiv 0 \pmod p.$$

Conversely, if $(x, y) = (a, d)$ is a nonzero solution of (B), *then S, given by* (A), *is a maximal sum-free set in G such that $-S \neq S$. The number of maximal sum-free sets S of G such that $-S \neq S$ is $p-1$.*

Moreover, if S, given by (A) *is a maximal sum-free set in G, then*

$$S^* = -S \cup S = \{-(a+kd), -(a+(k-1)d), a+d, \ldots, a+kd\}.$$

is such that

$$S^* \cap (S-S) = \emptyset \quad \text{and} \quad S^* \cup (S-S) = G.$$

THEOREM 4. *Let $p = 3k+1$ be a prime and S be a maximal sum-free set in $G = C_p$. If $-S = S$, then either*

$$S \cup (S+S) = G$$

or

(C) $$S = \{a+id;\ i = 1, 2, \ldots, k\},$$

where $(x, y) = (a, d)$ is a nonzero solution of

(D) $$2x+(k+1)y \equiv 0 \pmod p.$$

Conversely, if $(x, y) = (a, d)$ is a nonzero solution of (D), *then S, given by* (C), *is a maximal sum-free set in G and $-S = S$. There are $(p-1)/2$ distinct maximal sum-free sets S in G such that* (i) *S is in arithmetic progression and* (ii) $-S = S$.

3. Proof of Theorem 3. If S is a maximal sum-free set in G such that $-S \neq S$, let $S^* = -S \cup S$. Then we have $(S^*+S) \cap S = \emptyset$ and thus by the Cauchy–Davenport theorem and the fact that $|S| = k$, we have

(1) $$2k+1 = p-|S| \geqslant |S^*+S| \geqslant |S^*|+|S|-1 = |S^*|+k-1$$

from which it follows that $k < |S^*| \leqslant k+2$.

Since k is even, and $|S^*|$ is always even, hence $|S^*| = k+2$.

Now, from (1), we have $|S^*+S| = |S^*|+|S|-1$ and thus by Vosper's theorem, we know that S and S^* are in arithmetic progression with the same difference d ($\neq 0$). Thus

(A) $$S = \{a+id;\ i = 1, 2, \ldots, k\}.$$

Case 1. If $-(a+d) \in S$, then there exists $j \in \{2, 3, \ldots, k\}$ such that $(a+d)+(a+jd) \equiv 0 \pmod p$, i.e.

(2) $$2a+(1+j)d \equiv 0 \pmod p.$$

If j is odd, then $a+((1+j)/2)d \in S$ and

$$2(a+((1+j)/2)d) \equiv 0 \pmod p,$$

which is impossible. Hence j is even.

Thus for each $s \in S' = \{a+d, a+2d, \ldots, a+jd\}$, it is clear that $-s \in S'$. If $j < k-2$, then there exists i such that $1 \leqslant i \leqslant k-j$ for which $-(a+(j+i)d) \in S$ and thus there exists r such that $1 \leqslant r \leqslant k-j$ for which

$$(a+(j+i)d)+(a+(j+r)d) \equiv 0 \pmod p$$

and from (2) it follows that $(j+i+r-1)d \equiv 0 \pmod p$ where $j+i+r-1 \leqslant 2k-1$, which is impossible. Hence $j = k-2$ and therefore

(3) $$-\big(a+(k-1)d\big),\ -(a+kd) \notin S.$$

From the above discussion, it follows that $(x, y) = (a, d)$ is a nonzero solution of

(B) $$2x+(k-1)y \equiv 0 \pmod p.$$

We now prove that the converse is also true.

Suppose (a, d) is a nonzero solution of (B), i.e.

(4) $$2a+(k-1)d \equiv 0 \pmod p.$$

We shall prove that S, given by (A), is a maximal sum-free set in G. In fact, if $(S+S) \cap S \neq \emptyset$, then for some $i \in I = \{1, 2, \ldots, k\}$, $j \in J = \{2, 3, \ldots, 2k\}$,

(5) $$a+id \equiv 2a+jd \pmod p.$$

From (4) and (5), we have

(6) $$2(j-i)-k+1 \equiv 0 \pmod p, \qquad i \in I,\ j \in J.$$

Now,

$$\max\big\{\big(2(j-i)-k+1\big);\ i \in I,\ j \in J\big\} = 3k-1 < p,$$

$$\min\big\{\big(2(j-i)-k+1\big);\ i \in I,\ j \in J\big\} = -3k+5 > -p$$

and $2(j-i)-k+1 \neq 0$, $i \in I$, $j \in J$ because k is even.

Hence (5) cannot be true. This shows that S, given by (A), is sum-free in G and thus is a maximal sum-free set in G.

Case 2. If $-(a+d) \notin S$, then $-(a+2d) \notin S$. Otherwise if $-(a+2d) \in S$, then there exists $j \in \{3, 4, \ldots, k\}$ such that $(a+2d)+(a+jd) \equiv 0 \pmod p$, from which it follows, by arguments similar to the previous ones, that $j = k-1$ and thus $a+kd = -(a+d) \in S$ which contradicts the hypothesis. In this case, by similar arguments, we can show that if

$$S = \{a+id;\ i = 1, 2, \ldots, k\}$$

is sum-free in G then $(x, y) = (a, d)$ is a nonzero solution of

(7) $$2x+(k+3) \equiv 0 \pmod p$$

and conversely, if $(x, y) = (a, d)$ is a nonzero solution of (7), then S, given by $S = \{a+id;\ i = 1, 2, \ldots, k\}$ is a maximal sum-free set in G such that $-S \neq S$.

Let

$$\Sigma_1 = \big\{S;\ S = \{a+id;\ i = 1, 2, \ldots, k\}\big\}$$

where $(x, y) = (a, d)$ is a nonzero solution of (B), and

$$\Sigma_2 = \big\{S;\ S = \{a+id;\ i = 1, 2, \ldots, k\}\big\}$$

where $(x, y) = (a, d)$ is a nonzero solution of (7).

We now prove that $\Sigma_2 = \Sigma_1$.

Suppose $S_1 = \{a_1+id_1;\ i = 1, 2, \ldots, k\} \in \Sigma_1$, then

(8) $$2a_1+(k-1)d_1 \equiv 0 \pmod p.$$

Put

(9) $$d_2 = -d_1, \qquad a_2 = 2d_1-a_1.$$

Then

(10) $$\begin{aligned}2a_2+(k+3)d_2 &= 2(2d_1-a_1)+(k+3)(-d_1)\\ &= -2a_1-(k-1)d_1 \equiv 0 \pmod p.\end{aligned}$$

From (9), we have

(11) $$d_1 = -d_2, \qquad a_1 = -(a_2+2d_2).$$

Thus, for each $0 \leqslant i \leqslant k-1$,

$$\begin{aligned}a_1+(k-i)d_1 &= -(a_2+2d_2)+(k-i)(-d_2)\\ &= -a_2-(k+2-i)d_2\\ &\equiv a_2+(i+1)d_2 \pmod p \qquad \text{(by (10))}\end{aligned}$$

and

$$\begin{aligned}S_1 &= \{a_1+(k-i)d_1;\ i = 0, 1, \ldots, k-1\}\\ &= \{a_2+(i+1)d_2;\ i = 0, 1, \ldots, k-1\}\\ &= \{a_2+id_2;\ i = 1, 2, \ldots, k\} \in \Sigma_2.\end{aligned}$$

Hence $\Sigma_1 \subseteq \Sigma_2$.

Similarly, we can prove that $\Sigma_2 \subseteq \Sigma_1$ and thus $\Sigma_2 = \Sigma_1$.

Let

$$S = \{a+id;\ i = 1, 2, \ldots, k\}, \qquad S_0 = \{a_0+id_0;\ i = 1, 2, \ldots, k\} \in \Sigma_1.$$

We shall now prove that if $(a_0, d_0) \neq (a, d)$, then $S_0 \neq S$. If $S_0 = S$, then by Lemma 1, $d_0 \equiv \pm d \pmod p$. If $d_0 = -d$, then because both $(x, y) = (a_0, d_0)$ and $(x, y) = (a, d)$ are solutions of (B), $a_0 = -a$. Thus by Lemma 2, $-a = a_0 = a+(k+1)d$ from which it follows that $2a+$

$+(k+1)d \equiv 0 \pmod{p}$ which contradicts the fact that $2a+(k-1)d \equiv 0 \pmod{p}$. Hence $d_0 = d$ and thus $a_0 = a$. This shows that if $(a_0, d_0) \neq (a, d)$, then $S_0 \neq S$. Hence $|\Sigma_1| = p-1$.

Next, from (3), we have

$$S^* = S \cup \{-(a+(k-1)d),\ -(a+kd)\}. \tag{12}$$

From $|S^*+S| = |S^*|+|S|-1$, we know by applying Vosper's theorem, that S^* and S are in arithmetic progression with the same difference d'. Again, by Lemma 1, $d' \equiv \pm d \pmod{p}$.

We now write S^* in the arithmetic progression form with difference d. We have either

$$(a+kd)+d \equiv -(a+rd) \pmod{p} \qquad (r = k-1 \text{ or } k)$$

or

$$(a+d)-d \equiv -(a+rd) \pmod{p} \qquad (r = k-1 \text{ or } k).$$

But, because of $2a+(k-1)d \equiv 0 \pmod{p}$, the first case is not true and the second case is true only when $r = k-1$. Hence we write S^* in the arithmetic progression form as follows:

$$S^* = -S \cup S = \{-(a+kd),\ -(a+(k-1)d),\ a+d, \ldots, a+kd\}. \tag{13}$$

Finally, from $(S+S^*) \cap S = \emptyset$, it follows that $S^* \cap (S-S) = \emptyset$ and since $|S-S| = 2|S|-1 = 2k-1$, therefore $|S^*|+|S-S| = (k+2)+ +2k-1 = 3k+1 = p$. Thus $S^* \cup (S-S) = G$.

The proof of Theorem 3 is complete.

Remarks. The results that $S^* \cap (S-S) = \emptyset$ and $S^* \cup (S-S) = G$ are useful in constructing certain classes of point-symmetric graphs satisfying some critical conditions (see [6]).

4. Proof of Theorem 4. Let S be a maximal sum-free set in G. If $-S = S$, then $|S+S|$ is odd. Thus, from $2k+1 \geqslant |S+S| \geqslant 2k-1$, it follows that either $|S+S| = 2k+1$ and thus $S \cup (S+S) = G$ or $|S+S| = 2k-1 = 2|S|-1$ and thus by Vosper's theorem

$$S = \{a+id;\ i = 1, 2, \ldots, k\}. \tag{C}$$

In the later case, we can prove that $(x, y) = (a, d)$ is a nonzero solution of

$$2x+(k+1)y \equiv 0 \pmod{p} \tag{D}$$

and conversely, if $(x, y) = (a, d)$ is a nonzero solution of (D), then S, given by (C), is a maximal sum-free set in G.

The proof that there are $(p-1)/2$ distinct maximal sum-free sets S in G such that (i) S is in arithmetic progression and (ii) $-S = S$ is omitted.

The following example shows that the first case in Theorem 4 exists.

Example. $S = \{\pm 1, \pm 3, \pm 7\}$ is a maximal sum-free set in C_{19}, $S \cup (S+S) = C_{19}$.

The structure of maximal sum-free sets S in C_p, $p = 3k+1$, such that (i) S is not in arithmetic progression and (ii) $-S = S$ is still unknown to the author.

References

[1] P. H. Diananda and H. P. Yap, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad. 45 (1969), pp. 1–5.

[2] H. B. Mann, *Addition theorems*, Interscience 1965.

[3] — and J. E. Olson, *Sums of sets in the elementary abelian group of type (p, p)*, J. of Combinatorial Theory 2 (1967), pp. 275–284.

[4] H. P. Yap, *The number of maximal sum-free sets in C_p*, Nanta Math. 2 (1) (1968), pp. 68–71.

[5] — *Maximal sum-free sets of group elements*, J. London Math. Soc. 44 (1969), pp. 131–136.

[6] — *An application of additive group theory to graph theory* (unpublished).

UNIVERSITY OF SINGAPORE
Singapore, 10

Received on 16. 1. 1969