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 \( Z \to \infty \),

\[
\Sigma_1 = \sum_{|t|, |s| \leq Z} d(|f(t, s)|) = C_1 Z^{23} \log Z + C_2 Z^{23} + O(Z^{23 - \varepsilon}),
\]

for any fixed \( \varepsilon > 0 \).

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

\[
C_1 = \frac{\sqrt{3}}{|D^{1/2} - I^{1/2}(1)|} c_4, \quad C_2 = \frac{\sqrt{3}}{|D^{1/2} - I^{1/2}(1)|} (2a_1 - c_4),
\]

where \( c_4 \) and \( c_{\delta} \) 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 \( \Sigma_1 \) 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 \( c_4 \) in (4.12). We suppress all other details.

**References**


**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 \( S+T = \{ s+t : s \in S, t \in T \} \) respectively, \( \tilde{S} \) 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 \( S+T \) 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 \( T \) \( G \), \( |S| \geq |T| \), then \( S \) is said to be a maximal sum-free set in \( G \). We denote by \( \lambda(S) \) 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 \( n \geq 0 \).

Let \( C_p \) be the additive group of residues modulo 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 [3] were generalized and improved by Diamanda 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 \( -S = \{ -s : s \in S \} = S \); (ii) there are altogether \((p-1)/2 \) distinct maximal sum-free sets \( S_j \), \( j = 1, 2, \ldots, (p-1)/2 \), 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 \( 1 \leq r \leq m - 3 \). If \( A = \{ b+id ; i = 0, 1, \ldots, r \} \), then \( d' = \pm d \pmod{m} \) \((\{3\})\).

**Lemma 2.** Let \( A = \{a+id ; i = 0, 1, 2, \ldots, r \} \) be a set of residues modulo \( m \) with \( (d, m) = 1 \) and \( 3 \leq r \leq m + 1 \). 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 \( d = \pm d \pmod{m} \).

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

\[ a + \bar{d} = b + jd \pmod{m}, \quad h \in \{2, 3, \ldots, r\} \]

from which it follows that

\[ (h+j-2)d = 0 \pmod{m}, \quad 1 < h, j \leq r \]

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

\[ A + B = G \quad \text{or} \quad |A + B| > |A| + |B| - 1. \]

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 \( |C| \geq |A| + |B| \) or one of the following holds: (i) \( C = G \); (ii) \( |C| = p - 1 \) and \( C = j - A \), where \( j = C \); (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 \( G = \mathbb{Z}_p \). If \( -S \neq S \), then

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

where \( (a, d) \) is a nonzero solution of

\[ 2a + (k-1)d = 0 \pmod{p}. \]

Conversely, if \( (a, d) \) 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

\[ S = \{-(a + kd), -(a+(k-1)d), a + d, \ldots, a + kd\} \]

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 \( G = \mathbb{Z}_p \). If \( -S \neq S \), then either

\[ S \cup (S + S) = G \]

or

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

where \( (a, d) \) is a nonzero solution of

\[ 2a + (k+1)d = 0 \pmod{p}. \]

Conversely, if \( (a, d) \) is a nonzero solution of (D), then \( S \), given by (C), is a maximal sum-free set in \( G \) and \( -S \neq S \). 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

\[ 2k + 1 = p - |S| \geq |S^* + S| \geq |S^*| + |S| - 1 = |S^*| + k - 1 \]

from which it follows that \( k < |S^*| \leq k + 2 \).

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

\[ S = \{a + id; \ i = 1, 2, \ldots, k\}. \]

Case 1. If \(-a + id \notin S\), then there exists \( j \in \{2, 3, \ldots, k\} \) such that

\[ a + d + (a + jd) = 0 \pmod{p}, \]

and

\[ 2a + (1+j)d = 0 \pmod{p}. \]

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

\[ 2\{a + [(1+j)/2]d\} = 0 \pmod{p}, \]

which is impossible. Hence \( j \) is even.

Thus for each \( a + S' = \{a + d, a + 2d, \ldots, a + jd\} \), it is clear that \(-a + S' \neq S \). If \( j < k - 2 \), then there exists \( i \) such that \( 1 \leq i < k - j \) for which

\[ -a + (j - i)d \notin S \] and thus there exists \( r \) such that \( 1 \leq r \leq k - j \) for which

\[ a + (j - r)d + (a + (j + r)d) = 0 \pmod{p} \]
and from (2) it follows that \((j+i+r-1)d \equiv 0 \pmod{p}\) where \(j+i+r-1 \leq 2k-1\), which is impossible. Hence \(j = k-2\) and therefore

\[(3)\quad -(a+(k-1)d), -(a+kd) \in S.\]

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

\[(B)\quad 2x+(k-1)y \equiv 0 \pmod{p}.\]

We now prove that the converse is also true.

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

\[(4)\quad 2a+(k-1)d \equiv 0 \pmod{p}.\]

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)\quad a+id \equiv 2a+jd \pmod{p}.

From (4) and (5), we have

\[(6)\quad 2(j-i)-k+1 \equiv 0 \pmod{p}, \quad i \in I, j \in J.

Now,

\[
\begin{align*}
\max \{&\langle 2(j-i)-k+1; \ i \in I, j \in J\rangle \} = 3k-1 < p, \\
\min \{ &\langle 2(j-i)-k+1; \ i \in I, j \in J\rangle \} = -3k+5 > -p
\end{align*}
\]

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 \(-\langle a+2d \rangle \in S\), then there exists \(j \in \{3, 4, \ldots, k\}\) such that \(\langle a+2d \rangle + \langle a+jd \rangle \equiv 0 \pmod{p}\), from which it follows, by arguments similar to the previous ones, that \(j = k-1\) and thus \(a+kd \equiv -(a+d) \in S\) 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)\quad 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

\[
S_1 = \{S; \ S = \{a+id; \ i = 1, 2, \ldots, k\}\}
\]

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

\[
S_2 = \{S; \ S = \{a+id; \ i = 1, 2, \ldots, k\}\}
\]

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

We now prove that \(S_2 = S_1\).

Suppose \(S_2 = \{a_1+id_1; \ i = 1, 2, \ldots, k\} \in S_1\), then

\[(8)\quad 2a_1+(k-1)d_1 \equiv 0 \pmod{p}.

Put

\[(9)\quad d_2 = -d_1, \quad a_2 = 2d_1-a_1.

Then

\[(10)\quad 2a_2+(k+3)d_2 = 2(2d_2-a_1)+(k+3)(-d_1) = -2a_1-(k-1)d_1 \equiv 0 \pmod{p}.

From (9), we have

\[(11)\quad d_2 = -d_2, \quad a_1 = -(a_2+2d_2).

Thus, for each \(0 \leq i \leq k-1\),

\[
a_1+(k-i)d_1 = -(a_2+2d_2)+(k-i)(-d_2) = a_2+(i+1)d_1 \pmod{p} \quad \text{(by (10))}
\]

and

\[
S_1 = \{a_1+(k-i)d_1; \ i = 0, 1, \ldots, k-1\} = \{a_2+(i+1)d_1; \ i = 0, 1, \ldots, k-1\} = \{a_2+id_2; \ i = 1, 2, \ldots, k\} \in S_2.
\]

Hence \(S_1 \subseteq S_2\).

Similarly, we can prove that \(S_2 \subseteq S_1\) and thus \(S_1 = S_2\).

Let

\[
S = \{a+id; \ i = 1, 2, \ldots, k\}, \quad S_0 = \{a_2+id_2; \ i = 1, 2, \ldots, k\} \in S_1.
\]

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, \(d_0 = \pm d \pmod{p}\). If \(d_0 = -d\), then because both \((x, y) = (a_0, d_0)\) and \((x, y) = (a, d)\) are solutions of \(3\), \(a_0 = -a\). Thus by Lemma 2, \(-a = a_0 = a+(k+1)d\) from which it follows that \(2a+...
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


UNIVERSITY OF SINGAPORE
Singapore, 19

Received on 16.1.1969

---

4. Proof of Theorem 4. Let $S$ be a maximal sum-free set in $G$. If $S = S$, then $|S| = 3$ is odd. Thus, from $2k+1 > |S| > 2k-1$, 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 $(C) S = \{a+id : i = 1, 2, \ldots, k\}$.

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

(D) $2a+(k+1)d = 0$ (mod $p$)

and conversely, if $(a, y) = (a, d)$ 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 $C_9$, $S \cup (S+S) = C_9$. 