EDITH LIPKIN

Subset sums of sets of residues


<http://www.numdam.org/item?id=AST_1999__258__187_0>
SUBSET SUMS OF SETS OF RESIDUES

by

Edith Lipkin

Dedicated to Grisha Freiman, with respect and affection

Abstract. — The number \( m \) is called the critical number of a finite abelian group \( G \), if it is the minimal natural number with the property:
for every subset \( A \) of \( G \) with \( |A| \geq m \), \( 0 \notin A \), the set of subset sums \( A^* \) of \( A \) is equal to \( G \). In this paper, we prove the conjecture of G. Diderrich about the value of the critical number of the group \( G \), in the case \( G = \mathbb{Z}_q \), for sufficiently large \( q \).

Let \( G \) be a finite Abelian group, \( A \subset G \) such that \( 0 \notin A \). Let \( A = \{a_1, a_2, \ldots, a_{|A|}\} \), where \( |A| = \text{card} A \).

Let

\[ A^* := \{x \mid x = a_1 \varepsilon_1 + a_2 \varepsilon_2 + \cdots + a_{|A|} \varepsilon_{|A|}, \ \varepsilon_j \in \{0, 1\}, \ 1 \leq j \leq |A|, \ \sum_{j=1}^{|A|} \varepsilon_j > 0\} \]

and

\[ X := \{m \in \mathbb{N} \mid \forall A \subset G, |A| \geq m \Rightarrow A^* = G\}. \]

Since \( |G| - 1 \in X \), then \( X \neq \emptyset \) if \( |G| > 2 \). The number

\[ c(G) = \min_{m \in X} m \]

was introduced by George T. Diderrich in [1] and called the critical number of the group \( G \).

In this note we study the magnitude of \( c(G) \) in the case \( G = \mathbb{Z}_q \), where \( \mathbb{Z}_q \) is a group of residue classes modulo \( q \). We set \( c(q) := c(\mathbb{Z}_q) \). A survey of the problem was given by G.T. Diderrich and H.B. Mann in [2].

In the case when \( q \) is a prime number John Olson [3] proved that

\[ c(q) \leq \sqrt{4q - 3} + 1. \]

1991 Mathematics Subject Classification. — 11 P99, 05 D99.

Key words and phrases. — Subset sum, residue.

© Astérisque 258, SMF 1999
Recently J.A. Dias da Silva and Y.O. Hamidoune [4] have found the exact value of \( c(q) \) for which an estimate

\[
2q^{1/2} - 2 < c(q) < 2q^{1/2}
\]

is valid.

If \( q = p_1p_2, p_1 \geq p_2, p_1, p_2 - \text{prime numbers} \), then

\[
p_1 + p_2 - 2 \leq c(G) \leq p_1 + p_2 - 1
\]

as was proved by Diderrich [1].

It was proved in [2] that for \( q = 2\ell, \ell > 1 \)

\[
c(G) = \ell \text{ if } \ell \geq 5 \text{ or } q = 8
\]

\[
c(G) = \ell + 1 \text{ in all other cases.}
\]

Thus, to give thorough solution for \( G = \mathbb{Z}_q \) we have to find \( c(q) \) when \( q \) is a product of no less than three prime odd numbers.

G. Diderrich in [1] has formulated the following conjecture:

Let \( G \) be an Abelian group of odd order \( |G| = ph \) where \( p \) is the least prime divisor of \( |G| \) and \( h \) is a composite number. Then

\[
c(G) = p + h - 2.
\]

We prove here this conjecture for the case \( G = \mathbb{Z}_q \) for sufficiently large \( q \).

**Theorem 1.** — There exists a positive integer \( q_0 \) that if \( q > q_0 \) and \( q = ph, p > 2, \) where \( p \) is the least prime divisor of \( q \) and \( h \) is a composite number, we have

\[
c(q) = p + h - 2.
\]

To prove Theorem 1 we need the following results.

**Lemma 1.** — Let \( A = \{a_1, a_2, \ldots, a_{|A|}\} \subset N, N = \{1, 2, \ldots, \ell\}, S(A) = \sum_{i=1}^{|A|} a_i, \)

\[
A(g) = \{x \in A | x \equiv 0(\text{mod } g)\}, \quad B(A) = \frac{1}{2} \left( \sum_{i=1}^{|A|} a_i^2 \right)^{1/2}.
\]

Suppose that for some \( \varepsilon > 0 \) and \( \ell > \ell_1(\varepsilon) \) we have \( |A| \geq \ell^{2/3+\varepsilon} \) and

\[
(1) \quad |A(g)| \leq |A| - \ell^{3+\frac{\varepsilon}{2}},
\]

for every \( g \geq 2 \). Then for every \( M \) for which

\[
|M - \frac{1}{2}S(A)| \leq B(A)
\]

we have \( M \subset A^* \).

**Lemma 2.** — Let \( \varepsilon \) be a constant, \( 0 < \varepsilon \leq 1/3 \). There exists \( \ell_0 = \ell_0(\varepsilon) \) such that for every \( \ell \geq \ell_0 \) and every set of integers \( A \subset [1, \ell] \), for which

\[
(2) \quad |A| \geq \ell^{3+\varepsilon},
\]
the set $A^*$ contains an arithmetic progression of $\ell$ elements and difference $d$ satisfying the condition

\begin{equation}
 d < \frac{2\ell}{|A|}.
\end{equation}

We cited as Lemma 1 the Proposition 1.3 on page 298 of [5].

**Proof of Lemma 2.** — Let us first assume that $A$ fulfills the condition (1) in Lemma 1. Since we have

\[ B(A) \geq \frac{1}{2} \sqrt{\sum_{i=1}^{|A|} i^2} > \frac{1}{2} \sqrt{\frac{|A|^3}{3}} > \frac{1}{2\sqrt{3}} \epsilon^{1+\frac{3}{2}\epsilon} \]

and every $M$ from the interval $(\frac{1}{2} S(A) - B(A), \frac{1}{2} S(A) + B(A))$ belong to $A^*$, there exists an arithmetic progression in $A^*$ of the length $2B(A) > \ell$, if $\ell > \ell_0 = \ell_1(\epsilon)$.

Now we study the case when $A$ does not satisfy (1). We can then find an integer $g_1 \geq 2$ such that $B_1 \subset A = A_0$ and $B_1$ contains those elements of $A_0$ which are divisible by $g_1$ and for the set $A_1 = \{x / g_1 | x \in B_1$ and $x \equiv 0 \pmod{g_1}\}$ we have

\[ |A_1| > |A_0| - \epsilon^{\frac{3}{2} + \frac{\epsilon}{2}}. \]

Suppose that this process was repeated $s$ times and numbers $g_1, g_2, \ldots, g_s$ were found and sets $A_1, A_2, \ldots, A_s$ defined inductively, $B_j$ being a subset of $A_{j-1}$ containing those elements of $A_{j-1}$ which are divisible by $g_j$ and

\[ A_j = \{x / g_j | x \in B_j$ and $x \equiv 0 \pmod{g_j}\} \]

so that we have

\[ |A_j| > |A_{j-1}| - \ell_j^{\frac{3}{2} + \frac{\epsilon}{2}}, \quad j = 1, 2, \ldots, s. \]

From

\[ |A_s| \geq |A_{s-1}| - \ell_j^{\frac{3}{2} + \frac{\epsilon}{2}} > |A| - s\ell_j^{\frac{3}{2} + \frac{\epsilon}{2}} \]

and

\[ \ell_s = \left\lfloor \frac{\ell_{s-1}}{q_s} \right\rfloor \leq \frac{\ell}{2s} \]

it follows that

\begin{equation}
 |A_s| \geq \frac{1}{2} |A| \geq \frac{1}{2} \ell_j^{\frac{3}{2} + \frac{\epsilon}{2}} > \ell_s^{\frac{3}{2} + \epsilon}. \tag{4}
\end{equation}

The condition (2) of Lemma 2 for $A_s$ is verified, for some sufficiently large $s$ the condition (3) is fulfilled and thus $A_\ast$ contains an interval

\[ \left( \frac{1}{2} S(A_s) - B(A_s), \frac{1}{2} S(A_s) + B(A_s) \right). \]

We have, in view of (4),

\[ B(A_s) \geq \frac{1}{2} \sqrt{\sum_{i=1}^{|A_s|} i^2} > \frac{1}{2} \sqrt{\frac{|A_s|^3}{3}} \]

\[ \geq \frac{1}{4\sqrt{6}} \ell^{1+\frac{3}{2}\epsilon} > \ell. \tag{5} \]

\[ \text{SOCIÉTÉ MATHÉMATIQUE DE FRANCE 1999} \]
We have shown that $A^*$ contains an arithmetic progression of length $\ell$ and difference $d = g_1g_2 \cdots g_s$, and thus $A^*$ has the same property.

We now prove (2). From

$$\ell_s = \left\lfloor \frac{\ell}{d} \right\rfloor, \quad \ell_s \geq |A_s| \geq \frac{1}{2}|A|$$

we have

$$\left\lfloor \frac{\ell}{d} \right\rfloor \geq \frac{1}{2}|A|$$

or

$$d \leq \frac{2\ell}{|A|}.$$  

Lemma 2 is proved.

**Lemma 3 (M. Chaimovich [6]). —** Let $B = \{b_i\}$ be a multiset, $B \subset \mathbb{Z}_q$. Suppose that for every $s \geq 2$, $s$ dividing $q$, we have

$$|B\setminus B(s)| \geq s - 1.$$  

There exists $F \subset B$ for which

$$|F| \leq q - 1,$$

$$F^* = \mathbb{Z}_q.$$  

**Proof of Theorem 1.** — Let $q = p_1p_2 \cdots p_k$, $k \geq 4$, $p = p_1 \leq p_2 \leq \cdots \leq p_k$. We have

$$p^k \leq q \Rightarrow p \leq q^{1/4}.$$  

Let $A \subset \mathbb{Z}_q$ be such that $0 \not\in A$ and

$$|A| \geq \frac{q}{p} + p - 2;$$

we have to prove that $A^* = \mathbb{Z}_p$.

From (7) and (8) we get

$$|A| > \frac{q}{p} \geq q^{3/4}.$$  

Let us consider some divisor $d$ of $q$, and denote by $A_d$ a multiset $A$ viewed as a multiset of residues mod $d$. Let us show that for every $\delta$ dividing $d$ the number of residues in $A_d$ which are not divisible by $\delta$ satisfies the condition of Lemma 3.

The number of residues in $\mathbb{Z}_q$ which are divisible by $\delta$ is equal to $q/\delta$. Therefore the number of such residues in $A$ (which are all different) is not larger than $q/\delta - 1$, because $0 \not\in A$.

From this reasoning and from (7) we get the estimate

$$|A_d\setminus A(\delta)| \geq |A| - \left( \frac{q}{\delta} - 1 \right) \geq$$

$$\frac{q}{p} + p - 2 - \frac{q}{\delta} + 1 = \frac{q}{p} + p - \left( \frac{q}{\delta} + \delta \right) + \delta - 1.$$  

The function $x + q/x$ is decreasing on the segment $[1, \sqrt{q}]$. 

ASTÉRISQUE 258
The least divisor of \( g \) is equal to \( p \), and the maximal one to \( q/p \). Therefore
\[
p \leq \delta \leq \frac{q}{p}.
\]
If \( p \leq \delta \leq \sqrt{q} \), we have
\[
\frac{q}{p} + p \geq \frac{q}{\delta} + \delta.
\]
In the case \( \sqrt{q} \leq \delta \leq \frac{q}{p} \), let \( \rho = \frac{q}{\delta} \). Then \( \delta = \frac{a}{\rho}, \sqrt{q} \leq \frac{q}{\rho} \leq \frac{q}{p} \) and \( p \leq \rho \leq \sqrt{q} \) and we have
\[
\frac{q}{p} + p \geq \frac{q}{\rho} + \rho = \delta + \frac{q}{\rho}.
\]
From (11) and (12) it follows from (10) that we have
\[
|A_d \setminus A(\delta)| \geq \delta - 1.
\]
Let us apply the Lemma 3 to \( A_d \). Condition (13) is condition (6) of Lemma 3. Therefore there exists \( F_d \subset A_d \) such that \( |F_d| \leq d - 1 \) and \( F_d^* = \mathbb{Z}_d \).

Viewing \( F_d \) as a set of residues mod \( q \), let
\[
A' = \bigcup_{d/q \leq d < q^{1/3}} F_d.
\]
It is well known that the number of divisors \( d(q) = O(q^\varepsilon) \) for every \( \varepsilon > 0 \) so that
\[
|A'| < q^{1/3 + \varepsilon}
\]
for sufficiently large \( q \).

Take now \( A'' = A \setminus A' \). Take the least positive integer from each class of residues of the set \( A'' \) and denote this set by \( \tilde{A}'' \). We have \( \tilde{A}'' \subset [1, q - 1] \). We set \( \ell = q \) and see that all conditions of Lemma 1 are valid for \( \tilde{A}'' \). Thus, \( (\tilde{A}'')^* \) contains an arithmetic progression \( \mathcal{L} \) with a length \( q \) and a difference \( \Delta \) such that
\[
\Delta < \frac{2q}{q^{\delta}} = 2q^{1/4}.
\]
If \( (\Delta, q) = 1 \) then \( (\tilde{A}'')^* = \mathbb{Z}_q \). Suppose that \( D = (\Delta, q) > 1 \). Then \( \mathcal{L} \) (and therefore \( (\tilde{A}'')^* \) which contains \( \mathcal{L} \)) contains the residues of \( \mathbb{Z}_q \) which are divisible by \( D \). If \( \mathbb{Z}_D \) is a system of residues mod \( q \) representing a system of all residues mod \( D/q \), then \( (\tilde{A}'')^* + \mathbb{Z}_D = \mathbb{Z}_q \). But \( F_D \subset A' \) and \( F_D^* = \mathbb{Z}_D \). Thus
\[
A^* \supset (\tilde{A}'')^* + (A')^* = \mathbb{Z}_q.
\]
Theorem 1 is proved in the case \( k \geq 4 \).

Now we have to study the case when \( q \) is a product of three primes. Let \( q = p_1 p_2 p_3 \), \( p = p_1 \leq p_2 \leq p_3 \). Suppose that for some positive \( \varepsilon \) we have \( p < p^{1/3 + \varepsilon} \). The proof may be completed in a similar way to what was done.

In the general case we can use a stronger result than Lemma 2. Namely, the formulation of Lemma 2 is valid if in (2) we replace the number 2/3 in the exponent by 1/2 (see G. Freiman [7] and A. Sárközy [8]). So, in the case of \( q \) being a product of three primes, we can use this stronger version and prove Theorem 1.
As we have seen, the version of Lemma 1 with the exponent 2/3 was sufficient in the majority of cases. It is preferable to use this version, for its proof is much simpler than the case 1/2. Secondly, in the case 2/3 estimates of error terms have been obtained explicitly by M. Chaimovich. It provides us with the possibility to get an explicit range of validity for Theorem 1.

**Lemma 4.** Define a function of \( \ell \) in the following manner:

\[
m_0(\ell) = \left( \frac{12}{\pi^2} \right)^{1/3} \ell^{2/3} (\log \ell + 1/6)^{1/3} \left( 2 - \frac{4\gamma}{3} \right)^{1/3}
\]

where \( \gamma = \left( \frac{12}{\pi^2} \frac{\log \ell + 1/6}{\ell} \right)^{1/3} \).

Then for \( \ell > 155 \) a subset sum of each subset \( A \subset \{1, 2, \ldots, \ell\} \) with \( |A| = m > m_0(\ell) \) contains an arithmetic progression of cardinality \( \ell \).

Simplifying (15) we can take

\[
m_0(\ell) = 1.3 \ell^{2/3} (\log \ell + 1/6)^{1/3}.
\]

In the case of four or more primes in a representation of \( q \) we have to verify an inequality

\[
\ell^{3/4} > 1.3 \ell^{2/3} (\log \ell + 1/6)^{1/3}
\]

which is fulfilled for

\( \ell \geq 3000. \)

In some special cases we can give better estimates. For example, if \( p = 3 \) we have \( m > q/3 \) and instead of (16) we have

\[
\ell/3 > 1.3 \ell^{2/3} (\log \ell + 1/6)^{1/3},
\]

\( \ell > 64(\log \ell + 1/6) \)

which is valid for

\( \ell \geq 500. \)

**References**


---

E. Lipkin, School of Mathematical Sciences, Sackler Faculty of Exact Sciences, Tel Aviv University, Tel-Aviv, Israel