Number of solutions in a box of a linear homogeneous equation in an Abelian group

by

MACIEJ ZAKARCEMNY (Warszawa)

1. Introduction. K. Cwalina and T. Schoen have recently proved the following conjecture of A. Schinzel: the number of solutions of the congruence $a_1x_1 + \cdots + a_kx_k \equiv 0 \pmod{n}$ in the box $0 \leq x_i \leq b_i$, where $b_i$ are positive integers, is at least $2^{1-n} \prod_{i=1}^{k}(b_i + 1)$. Using a completely different method we shall prove the following more general statement, also conjectured by Schinzel ([3 p. 364]).

Theorem 1.1. For every finite Abelian group $\Gamma$, for all $a_1, \ldots, a_k \in \Gamma$, and for all positive integers $b_1, \ldots, b_k$ the number of solutions of the equation $\sum_{i=1}^{k} a_ix_i = 0$ in nonnegative integers $x_i \leq b_i$ is at least

\[ 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1), \]

where $D(\Gamma)$ is the Davenport constant of $\Gamma$ (see Definition 2.1 below).

2. Lemmas and definitions. Let $\Gamma$ be a finite Abelian group, with multiplicative notation.

Definition 2.1. Define the Davenport constant $D(\Gamma)$ to be the smallest positive integer $n$ such that, for any sequence $g_1, \ldots, g_n$ of group elements, there exist indices

\[ 1 \leq i_1 < \cdots < i_t \leq n \quad \text{for which} \quad g_{i_1} \cdot \cdots \cdot g_{i_t} = 1. \]

For a group with multiplicative notation, Theorem 1.1 has the form: for every finite Abelian group $\Gamma$, for all $a_1, \ldots, a_k \in \Gamma$, and for all positive integers $b_1, \ldots, b_k$ the number of solutions of the equation $\prod_{i=1}^{k} a_i x_i = 1$ in

2010 Mathematics Subject Classification: Primary 11D79; Secondary 20K01.

Key words and phrases: Abelian group, linear homogeneous equation, box, number of solutions.

DOI: 10.4064/aa155-2-10
nonnegative integers $x_i \leq b_i$ is at least
\[(2.1) \quad 2^{1-D(\Gamma)} \prod_{i=1}^{k} (b_i + 1).\]

By the definition of the Davenport constant, we may find $g_1, \ldots, g_{D(\Gamma)-1} \in \Gamma$ such that any product of a nonempty subsequence of this sequence is not equal to 1 in $\Gamma$. As the number of solutions of the equation $\prod_{i=1}^{D(\Gamma)-1} g_i^{x_i} = 1$, where $x_i = 0$ or $x_i = 1$, is equal to $1 = 2^{1-D(\Gamma)} \prod_{i=1}^{D(\Gamma)-1} (1 + 1)$, we obtain:

Remark 2.2. In Theorem 1.1, $2^{1-D(\Gamma)}$ is the best possible coefficient independent of $a_i, b_i$ and depending only on $\Gamma$.

Lemma 2.3. For $n \geq 1$ we have the following identity in $\mathbb{Q}[x]$ and in $\mathbb{Q}[\Gamma]$:
\[(2.2) \quad 1 + x + x^2 + \cdots + x^n = \sum_{j=0}^{n} 2^{j-n-1} (1 + x^j)(1 + x)^{n-j}.\]

Proof. We proceed by induction on $n$. For $n = 1$ we have
$$
\sum_{j=0}^{1} 2^{j-1-1} (1 + x^j)(1 + x)^{1-j} = 2^{-2}(1 + 1)(1 + x) + 2^{-1}(1 + x) = 1 + x
$$
and the assertion is true.

Assume it is true for degrees less than $n$, where $n > 1$. Then
$$
1 + x + x^2 + \cdots + x^n = \frac{1}{2}\left((1 + x)(1 + x + \cdots + x^{n-1}) + (1 + x^n)\right)
$$
$$
= \frac{1}{2}\left((1 + x) \sum_{j=0}^{n-1} 2^{j-(n-1)-1} (1 + x^j)(1 + x)^{n-1-j} + (1 + x^n)\right)
$$
$$
= \sum_{j=0}^{n-1} 2^{j-n-1} (1 + x^j)(1 + x)^{n-j} + \frac{1}{2}(1 + x^n)
$$
$$
= \sum_{j=0}^{n} 2^{j-n-1} (1 + x^j)(1 + x)^{n-j}. \quad \blacksquare
$$

Definition 2.4. For an element $\sum_{g \in \Gamma} N_g g$ of the group ring $\mathbb{Q}[\Gamma]$ and a number $n \in \mathbb{Q}$ we write
$$
\sum_{g \in \Gamma} N_g g \geq n \quad \text{iff} \quad N_1 \geq n.
$$

Lemma 2.5. Theorem 1.1 in multiplicative notation is equivalent to the statement: for every finite Abelian group $\Gamma$, for all $a_1, \ldots, a_k \in \Gamma$, and for
all positive integers \( b_1, \ldots, b_k \) we have

\[
\prod_{i=1}^k (1 + a_i + \cdots + a_i^{b_i}) \geq 2^{1-D(\Gamma)} \prod_{i=1}^k (b_i + 1),
\]

where \( D(\Gamma) \) is the Davenport constant of \( \Gamma \).

Proof. Indeed, the number of solutions of the equation \( \prod_{i=1}^k a_i^{x_i} = 1 \) in nonnegative integers \( x_i \leq b_i \) is equal to \( N_1 \), where

\[
\prod_{i=1}^k (1 + a_i + \cdots + a_i^{b_i}) = \sum_{g \in \Gamma} N_g g.
\]

We have

\[
N_1 \geq 2^{1-D(\Gamma)} \prod_{i=1}^k (b_i + 1)
\]

if and only if (2.3) holds. \( \square \)

Lemma 2.6. Let \( \Gamma \) be a finite Abelian group. For all \( a_1, \ldots, a_k \in \Gamma \) we have

\[
(1 + a_1) \cdot \ldots \cdot (1 + a_k) \geq 2^{1-D(\Gamma)} \cdot 2^k.
\]

Proof. For the completeness of exposition we provide Olson’s proof \[2\].

We proceed by induction on \( k \). For \( k \leq D(\Gamma) - 1 \) we have

\[
(1 + a_1) \cdot \ldots \cdot (1 + a_k) \geq 1 \geq 2^{1-D(\Gamma)} \cdot 2^k
\]

and the assertion is true.

Assume it is true for the number of factors less than \( k \), where \( k > D(\Gamma) - 1 \). Hence \( k \geq D(\Gamma) \). By the definition of the Davenport constant we may assume, without loss of generality, that

\[
a_1 \cdot \ldots \cdot a_t = 1 \quad \text{for some } 1 \leq t \leq D(\Gamma).
\]

By the inductive assumption

\[
\prod_{i=2}^t (1 + a_i^{-1}) \prod_{i=t+1}^k (1 + a_i) \geq 2^{1-D(\Gamma)} \cdot 2^{k-1},
\]

\[
\prod_{i=2}^k (1 + a_i) \geq 2^{1-D(\Gamma)} \cdot 2^{k-1}.
\]
Hence
\[
\prod_{i=1}^{k}(1 + a_i) = \prod_{i=2}^{k}(1 + a_i) + a_1 \prod_{i=2}^{k}(1 + a_i) \\
= \prod_{i=2}^{k}(1 + a_i) + a_1 \cdot \ldots \cdot a_t \prod_{i=2}^{t}(1 + a_i^{-1}) \prod_{i=t+1}^{k}(1 + a_i) \\
= \prod_{i=2}^{k}(1 + a_i) + \prod_{i=2}^{t}(1 + a_i^{-1}) \prod_{i=t+1}^{k}(1 + a_i) \\
\geq 2^{1-D(\Gamma)} \cdot 2^{k-1} + 2^{1-D(\Gamma)} \cdot 2^{k-1} = 2^{1-D(\Gamma)} \cdot 2^k. \]

3. Proof of Theorem 3.1. By Lemma 2.5 it suffices to prove:

\[\text{Theorem 3.1. For every finite Abelian group } \Gamma, \text{ for all } a_1, \ldots, a_k \in \Gamma, \text{ and for all positive integers } b_1, \ldots, b_k \text{ we have}
\]
\[\prod_{i=1}^{k}(1 + a_i + \cdots + a_i^{b_i}) \geq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1),\]

where \( D(\Gamma) \) is the Davenport constant of \( \Gamma \).

\[\text{Proof. We use the identity (2.2) to get}
\]
\[P(a_1, \ldots, a_k) = \prod_{i=1}^{k}(1 + a_i + \cdots + a_i^{b_i}) = \prod_{i=1}^{k} \sum_{j=0}^{b_i} 2^{j-b_i-1}(1 + a_i^j)(1 + a_i)^{b_i-j}.
\]

Hence for a certain \( s \) we obtain
\[P(a_1, \ldots, a_k) = \sum_{1 \leq i \leq s} v_i P_i(a_1, \ldots, a_k),\]

where \( v_i \) are positive rational numbers and each \( P_i(a_1, \ldots, a_k) \) has the form
\[(1 + c_1) \cdot \ldots \cdot (1 + c_m),\]

where \( c_1, \ldots, c_m \in \Gamma \).

For \( P_i(a_1, \ldots, a_k) \) we use Lemma 2.6 to get
\[P_i(a_1, \ldots, a_k) \geq 2^{1-D(\Gamma)} P_i(1, \ldots, 1), \quad 1 \leq i \leq s.
\]

Note that we use \( P, P_i \) in two different domains at the same time, in \( \mathbb{Q}[\Gamma] \) and in \( \mathbb{Q}[x] \).

It follows that \( P(a_1, \ldots, a_k) \geq 2^{1-D(\Gamma)} P(1, \ldots, 1). \) Thus
\[\prod_{i=1}^{k}(1 + a_i + \cdots + a_i^{b_i}) \geq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1). \]
Acknowledgements. Prof. A. Schinzel’s help in the presentation of the above results is gratefully acknowledged. Thanks are also due to the referee for his comments.

References


Maciej Zakarczemny
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: M.Zakarczemny@impan.pl

Received on 17.2.2012
and in revised form on 27.6.2012

(6980)