ACTA ARITHMETICA
155.2 (2012)

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

by

MACIEJ ZAKARCZEMNY (Warszawa)

1. Introduction. K. Cwalina and T. Schoen [1] have recently proved the following conjecture of A. Schinzel [3]: the number of solutions of the congruence $a_1x_1 + \cdots + a_kx_k \equiv 0 \pmod{n}$ in the box $0 \le x_i \le b_i$, 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 Γ, 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 $x_i \le b_i$ is at least*

$$2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1), \tag{1.1}$$

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

2. Lemmas and definitions. Let Γ 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

$$1 \le i_1 < \cdots < i_t \le n \quad \text{for which} \quad g_{i_1} \cdot \ldots \cdot g_{i_t} = 1.$$

For a group with multiplicative notation, Theorem 1.1 has the form: for every finite Abelian group Γ, 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 $x_i \le b_i$ is at least

$$2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1). \tag{2.1}$$

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 Γ. 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 Γ.

LEMMA 2.3. *For $n\ge 1$ we have the following identity in $\mathbb{Q}[x]$ and in $\mathbb{Q}[\Gamma]$:*

$$1+x+x^2+\cdots+x^n=\sum_{j=0}^{n}2^{j-n-1}(1+x^j)(1+x)^{n-j}. \tag{2.2}$$

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

$$\begin{aligned}1+x+x^2+\cdots+x^n&=\frac{1}{2}\big((1+x)(1+x+\cdots+x^{n-1})+(1+x^n)\big)\\&=\frac{1}{2}\Big((1+x)\sum_{j=0}^{n-1}2^{j-(n-1)-1}(1+x^j)(1+x)^{n-1-j}+(1+x^n)\Big)\\&=\sum_{j=0}^{n-1}2^{j-n-1}(1+x^j)(1+x)^{n-j}+\frac{1}{2}(1+x^n)\\&=\sum_{j=0}^{n}2^{j-n-1}(1+x^j)(1+x)^{n-j}.\ \blacksquare\end{aligned}$$

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

$$\sum_{g\in\Gamma}N_g g\succeq n \quad\text{iff}\quad N_1\ge n.$$

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

$$\prod_{i=1}^{k}(1 + a_i + \dots + a_i^{b_i}) \succeq 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1), \tag{2.3}$$

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

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

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

We have

$$N_1 \ge 2^{1-D(\Gamma)} \prod_{i=1}^{k}(b_i + 1)$$

if and only if (2.3) holds. ∎

Lemma 2.6. *Let* Γ *be a finite Abelian group. For all* $a_1, \dots, a_k \in \Gamma$ *we have*

$$(1 + a_1) \cdot \ldots \cdot (1 + a_k) \succeq 2^{1-D(\Gamma)} \cdot 2^k. \tag{2.4}$$

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

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

$$(1 + a_1) \cdot \ldots \cdot (1 + a_k) \succeq 1 \ge 2^{1-D(\Gamma)} \cdot 2^k$$

and the assertion is true.

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

$$a_1 \cdot \ldots \cdot a_t = 1 \quad \text{for some } 1 \le t \le D(\Gamma).$$

By the inductive assumption

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

$$\prod_{i=2}^{k}(1 + a_i) \succeq 2^{1-D(\Gamma)} \cdot 2^{k-1}.$$

Hence

$$\begin{aligned}\prod_{i=1}^{k}(1+a_i) &= \prod_{i=2}^{k}(1+a_i) + a_1\prod_{i=2}^{k}(1+a_i)\\ &= \prod_{i=2}^{k}(1+a_i) + a_1\cdot\ldots\cdot a_t\prod_{i=2}^{t}(1+a_i^{-1})\prod_{i=t+1}^{k}(1+a_i)\\ &= \prod_{i=2}^{k}(1+a_i) + \prod_{i=2}^{t}(1+a_i^{-1})\prod_{i=t+1}^{k}(1+a_i)\\ &\succeq 2^{1-D(\Gamma)}\cdot 2^{k-1} + 2^{1-D(\Gamma)}\cdot 2^{k-1} = 2^{1-D(\Gamma)}\cdot 2^{k}. \ \blacksquare\end{aligned}$$

3. Proof of Theorem 1.1. By Lemma 2.5 it suffices to prove:

THEOREM 3.1. *For every finite Abelian group Γ, for all $a_1, \ldots, a_k \in \Gamma$, and for all positive integers $b_1, \ldots, b_k$ we have*

$$\prod_{i=1}^{k}(1+a_i+\cdots+a_i^{b_i}) \succeq 2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1).$$

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

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

$$P(a_1,\ldots,a_k) = \sum_{1\le i\le s} v_i P_i(a_1,\ldots,a_k),$$

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

$$P_i(a_1,\ldots,a_k) \succeq 2^{1-D(\Gamma)}P_i(1,\ldots,1), \qquad 1\le i\le s.$$

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 $P(a_1,\ldots,a_k) \succeq 2^{1-D(\Gamma)}P(1,\ldots,1)$. Thus

$$\prod_{i=1}^{k}(1+a_i+\cdots+a_i^{b_i}) \succeq 2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1). \ \blacksquare$$

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

[1] K. Cwalina and T. Schoen, *The number of solutions of a homogeneous linear congruence*, Acta Arith. 153 (2012), 271–279.

[2] J. E. Olson, *A combinatorial problem on finite abelian groups, II*, J. Number Theory 1 (1969), 195–199.

[3] A. Schinzel, *The number of solutions of a linear homogeneous congruence*, in: Diophantine Approximation: Festschrift for Wolfgang Schmidt (H.-P. Schlickewei et al., eds.), Developments Math. 16, Springer, 2008, 363–370.

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)