ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

Karol Cwalina

Uniwersytet Warszawski

The number of solutions of a homogeneous linear congruence

Praca semestralna nr 2

(semestr zimowy 2010/11)

Opiekun pracy: Tomasz Schoen

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

THE NUMBER OF SOLUTIONS OF A HOMOGENEOUS LINEAR CONGRUENCE

KAROL CWALINA AND TOMASZ SCHOEN

Abstract. We prove an optimal lower bound on the number of solutions of a homogeneous linear congruence $a_1x_1+\ldots+a_kx_k \equiv 0 \pmod{n}$. This confirms Schinzel's conjecture.

1. Introduction

Let n, k be positive integers and $\boldsymbol{a} = (a_1, \ldots, a_k)$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$ be sequences of integers and naturals respectively. We are interested in the number of solutions of the congruence

$$a_1x_1 + \ldots + a_kx_k \equiv 0 \pmod{n},$$

for integer coefficients $x_1, \ldots, x_k$ satisfying $0 \leq x_i \leq b_i$. We denote this number by $N_n(\boldsymbol{a}, \boldsymbol{b})$.

Intuitively, by an averaging argument, we can hope to prove a bound of the form

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geq \gamma \cdot \prod_{i=1}^{k}(1 + b_i),$$

for a suitably chosen γ. On the other hand, since for $a_i = b_i = 1$, for $i = 1, \ldots, k$, and $k = n - 1$ we have $N_n(\boldsymbol{a}, \boldsymbol{b}) = N_n(\mathbf{1}, \mathbf{1}) = 1$, we can see that $\gamma(n) = 2^{1-n}$ would be the best possible coefficient, provided we restricted ourselves to those dependent only on n.

We shall prove the following theorem conjectured by Schinzel [3, 5]. We present it here in the setting of the group $\mathbb{Z}_n$, which is obviously equivalent to that of the congruence (mod n).

Date: December, 2010 (revised in September, 2011).
2010 *Mathematics Subject Classification.* 11D79.
Key words and phrases. linear homogeneous equation.

Theorem 1.1. *Let n, k be positive integers, sequences $\boldsymbol{a} = (a_1, \ldots, a_k)$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$ be such that $a_i \in \mathbb{Z}_n$ and $b_i \in \mathbb{N}$ for $i = 1, \ldots, k$. Then*

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-n} \prod_{i=1}^{k} (1 + b_i).$$

Schinzel and Zakarczemny [5] proved this theorem in the case of $a_1, \ldots, a_k$ satisfying for all i, j the following: $(n, a_i)|(n, a_j)$ or $(n, a_j)|(n, a_i)$, or $n|[a_i, a_j]$. Later Schinzel [4] established the following result.

Theorem 1.2 (Schinzel [4, Theorem 1 and Corollary])**.** *Let*

$$n = \prod_{\lambda=1}^{l} q_\lambda^{\alpha_\lambda},$$

where q_λ are distinct primes, $\alpha_\lambda > 0$ and

$$\sum_{\lambda=1}^{l} \frac{1}{q_\lambda} \leq 1 + \frac{\min(l, 2l - 5)}{n}.$$

Then, under the assumptions of Theorem 1.1,

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-n} \prod_{i=1}^{k} (1 + b_i).$$

In particular, Schinzel's conjecture holds for $n < 60$.

This theorem will serve us when proving Theorem 1.1 for $n < 22$.

In the appendix to the same paper Kaczorowski [1] proposed an elegant, purely combinatorial method, which allowed him to establish the bound

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geq \frac{1}{n\binom{n+k-1}{k}} \prod_{i=1}^{k} (1 + b_i).$$

Our proof of the theorem will be founded on the idea of Kaczorowski.

If $b_i = 1$ $(i = 1, \ldots, k)$ then Theorem 1.1 follows from a more general result of Olson. We keep here, mutatis mutandis, the notation from the above theorems.

Definition. Let G be a finite abelian group. We define *Davenport's constant* $D(G)$ of the group G to be the smallest integer s such that every s-element sequence of elements of G has a nontrivial subsequence that sums to zero.

Theorem (Olson [2, Theorem 2])**.** *Let G be a finite abelian group, k be a positive integer and a sequence $\boldsymbol{a} = (a_1, \ldots, a_k)$ be such that $a_i \in G$*

for $i = 1, \dots, k$. *Then*

$$N_G(\boldsymbol{a}, \mathbf{1}) \geq 2^{1-D(G)} \cdot 2^k.$$

A natural conjecture, which would unify these results, calls for the following.

Conjecture. *Let* G *be a finite abelian group,* k *be a positive integer,* $\boldsymbol{a} = (a_1, \dots, a_k)$ *and* $\boldsymbol{b} = (b_1, \dots, b_k)$ *be sequences such that* $a_i \in G$ *and* $b_i \in \mathbb{N}$ *for* $i = 1, \dots, k$. *Then*

$$N_G(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-D(G)} \prod_{i=1}^{k} (1 + b_i).$$

Since, at present, very little is known about $D(G)$, any attempt at this conjecture would probably require an indirect approach.

We discuss some generalizations of Theorem 1.1 in the final section of the paper.

2. Notation and a sketch of the argument

In the paper we shall adopt the following non-standard notation.

Definition. Let n be a positive integer, I be any set, and sequences of integers $\boldsymbol{b}^- = (b_i^-)_{i \in I}, \boldsymbol{b}^+ = (b_i^+)_{i \in I}$ satisfy $0 \leq b_i^- \leq b_i^+$. Let c and all the elements a_i of a sequence $\boldsymbol{a} = (a_i)_{i \in I}$ belong to $\mathbb{Z}_n$.

We define $N_{c;n}(\boldsymbol{a}, \boldsymbol{b}^- \leq \boldsymbol{b}^+)$ as the number of solutions, for integer coefficients $b_i^- \leq x_i \leq b_i^+$, of the equation

$$\sum_{i \in I} a_i x_i = c.$$

Likewise, for a sequence of naturals $\boldsymbol{b} = (b_i)_{i \in I}$, we denote by $C_n(\boldsymbol{a}, \boldsymbol{b})$ the set

$$C_n(\boldsymbol{a}, \boldsymbol{b}) = \Big\{ \sum_{i \in I} a_i x_i \ : \ 0 \leq x_i \leq b_i \Big\}.$$

We shall also denote by $\boldsymbol{e_j}$ the sequence $(e_i)_{i \in I}$ such that $e_j = 1$ and $e_i = 0$ for $i \neq j$. Finally, $\mathbf{0}$ and $\mathbf{1}$ denote the sequences consisting exclusively of zeros and ones respectively, while $\mathbf{1}_A$ stands for the characteristic sequence of a subset $A \subset I$.

Whenever we perform an arithmetic operation on two sequences this is meant to be performed coordinatewise.

By convention, we shall use the element of the sequence to denote a one-element sequence. Also, when considered elements split in families, we shall write them by semicolon, e.g. $N_{c;n}(\boldsymbol{a}, \boldsymbol{t} \leq \boldsymbol{b}; \boldsymbol{a}', \boldsymbol{t}' \leq \boldsymbol{b}')$. In all

cases, indexing sets will be given implicitly. Finally, we shall usually drop "zeros" from the notation, therefore $N_n(\boldsymbol{a},\boldsymbol{b}) = N_{0;n}(\boldsymbol{a},\boldsymbol{0}\le\boldsymbol{b})$.

Let us now briefly sketch our argument. Following the idea of Kaczorowski [1] we look for a sequence $\boldsymbol{t}=(t_i)$ such that $C_n(\boldsymbol{a},\boldsymbol{t}) = C_n(\boldsymbol{a},\boldsymbol{b})$ and the sum $\sum t_i$ is possibly small (it can be easily chosen to be at most $n-1$). Obviously $N_{c;n}(\boldsymbol{a},\boldsymbol{t}\le\boldsymbol{b}) \ge \frac{1}{n}\prod(1+b_i-t_i)$ for some residue class c. If $\sum t_i$ is considerably smaller than n, then we can easily conclude that

$$N_n(\boldsymbol{a},\boldsymbol{b}) \ge N_{c;n}(\boldsymbol{a},\boldsymbol{t}\le\boldsymbol{b}) \ge 2^{1-n}\prod(1+b_i)$$

for sufficiently large n.

In the subsequent parts of the paper we shall encounter various inequalities claimed to hold for sufficiently large integers. In all cases an easy inductive argument proves the claim. Similarly, we shall use several times a particular, yet well known, form of Bernoulli's inequality, i.e. $(1+a/x)^x \le 2^a$ for any real numbers $0 < x \le a$.

3. Lemmas

Of course, it is sufficient to consider the problem if $a_i \neq 0$ for all i. Similarly, we can assume that $(a_1,\dots,a_k)=1$.

We can also restrict our attention to the case when $0<b_i<n$ for all i. It basically follows from the observation that both the function $N_n(\cdot)$ and the requested bound are "additive" as functions of b_i for every i. Let us make this more explicit by the analysis of the case $b_1 = Bn+r$. We assume here that the bound holds for $b_1 < n$.

$$\begin{aligned}
N_n(a_1,b_1;\boldsymbol{a}',\boldsymbol{b}') &= N_n(a_1,0\le n-1;\boldsymbol{a}',\boldsymbol{b}') + N_n(a_1,n\le 2n-1;\boldsymbol{a}',\boldsymbol{b}') + \\
&\quad \dots + N_n(a_1,Bn\le Bn+r;\boldsymbol{a}',\boldsymbol{b}') \\
&= N_n(a_1,n-1;\boldsymbol{a}',\boldsymbol{b}') + N_n(a_1,n-1;\boldsymbol{a}',\boldsymbol{b}') + \\
&\quad \dots + N_n(a_1,r;\boldsymbol{a}',\boldsymbol{b}') \\
&\ge 2^{1-n}n\prod_{i\neq 1}(1+b_i) + 2^{1-n}n\prod_{i\neq 1}(1+b_i) + \\
&\quad \dots + 2^{1-n}(1+r)\prod_{i\neq 1}(1+b_i) \\
&= 2^{1-n}(1+Bn+r)\prod_{i\neq 1}(1+b_i) \\
&= 2^{1-n}\prod(1+b_i).
\end{aligned}$$

We shall now show an easy lemma which will turn out useful in our proof of the theorem. It also justifies the claim, appearing in the

preceding section, saying that we can select a sequence $\boldsymbol{t} = (t_i)$ such that $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ and $\sum t_i \leq n - 1$.

Lemma 3.1. *If we have $0 \leq t_i \leq b_i$ and $C_n(\boldsymbol{a}, \boldsymbol{t}) \neq C_n(\boldsymbol{a}, \boldsymbol{b})$ then there exists some j such that $t_j < b_j$ and $|C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_j})| > |C_n(\boldsymbol{a}, \boldsymbol{t})|$.*

Proof. Observe that $C_n(\boldsymbol{a}, \boldsymbol{t}+\boldsymbol{e_j}) = C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \{0, a_j\}$, where $\oplus$ denotes the Minkowski sum, defined as $A \oplus B = \{a + b : \ a \in A, b \in B\}$.

Let us now suppose that $C_n(\boldsymbol{a}, \boldsymbol{t}+\boldsymbol{e_j}) = C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \{0, a_j\} = C_n(\boldsymbol{a}, \boldsymbol{t})$ for all j such that $t_j < b_j$. Since Minkowski's sum is associative, we have the following:

$$\begin{aligned} C_n(\boldsymbol{a}, \boldsymbol{b}) &= C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \bigoplus_{j:t_j<b_j} \bigoplus_{l=0}^{b_j - t_j} \{0, a_j\} \\ &= C_n(\boldsymbol{a}, \boldsymbol{t}) \end{aligned}$$

— a contradiction. □

The following lemma will allow us to deal with some structured cases in our proof of the main result.

Lemma 3.2. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\delta)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_\delta)$ be sequences such that $\alpha_i \in \mathbb{Z}_n$ and $\beta_i \in \mathbb{N}$ for $i = 1, \ldots, \delta$, and*

$$\delta \leq \sum \beta_i \leq \min(\lfloor n/2 \rfloor, |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})| - 1).$$

Moreover, let $\boldsymbol{a} = (a_1, \ldots, a_d)$ and $\boldsymbol{b} = (b_1, \ldots, b_d)$ be such that a_i generates $\mathbb{Z}_n$ and $b_i \in \mathbb{N}$ for $i = 1, \ldots, d$. Then, if $n \geq 9$, Schinzel's conjecture holds, i.e.

$$N_n(\boldsymbol{\alpha}, \boldsymbol{\beta}; \boldsymbol{a}, \boldsymbol{b}) \geq \frac{1}{2^{n-1}} \prod (1 + \beta_i) \prod (1 + b_i).$$

Proof. First, we shall quote a lemma from Schinzel's paper [3].

Lemma ([3, lemma 5])**.** *For positive integers a and $x \leq a$ we have*

$$\left(1 + \frac{a}{x}\right)^{x+1} \leq 2^{a+1},$$

except for the pair $a = 2$, $x = 1$.

If $C_n(\boldsymbol{\alpha}, \boldsymbol{\beta}; \boldsymbol{a}, \boldsymbol{b}) \neq \mathbb{Z}_n$ then, since every a_i generates $\mathbb{Z}_n$, we have

$$\sum b_i < n - |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})| \leq n - \sum \beta_i - 1.$$

Henceforth, in this case, by the arithmetic mean-geometric mean and Bernoulli's inequalities,

$$\begin{aligned}\prod(1+\beta_i)\prod(1+b_i) &\leq \Big(1+\frac{\sum\beta_i+\sum b_i}{\delta+d}\Big)^{\delta+d}\\ &\leq 2^{\sum\beta_i+\sum b_i}\leq 2^{n-1}\\ &\leq 2^{n-1}\cdot N_n(\boldsymbol{\alpha},\boldsymbol{\beta};\boldsymbol{a},\boldsymbol{b}).\end{aligned}$$

Let us now assume that $n>b_1\geq b_2\geq\ldots$ and $l\leq n-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|$ is the smallest number such that $C_n(\boldsymbol{\alpha},\boldsymbol{\beta};a_1,b_1;\ldots;a_l,b_l)=\mathbb{Z}_n$.

Obviously, because $C_n(\boldsymbol{\alpha},\boldsymbol{\beta};a_1,b_1;\ldots;a_l,b_l)=\mathbb{Z}_n$, every choice of $0\leq x_i\leq b_i$ for $i=l+1,\ldots,d$ leads to at least one solution of the considered equation. Therefore

$$N_n(\boldsymbol{\alpha},\boldsymbol{\beta};\boldsymbol{a},\boldsymbol{b})\geq\prod_{i>l}(1+b_i)$$

and it is now sufficient to prove that

$$\prod_{i=1}^{\delta}(1+\beta_i)\prod_{i=1}^{l}(1+b_i)\leq 2^{n-1}.$$

If $l=1$ then, using the same inequalities again, for $n\geq 7$,

$$\begin{aligned}\prod_{i=1}^{\delta}(1+\beta_i)\prod_{i=1}^{l}(1+b_i) &\leq \Big(1+\frac{\sum\beta_i}{\delta}\Big)^{\delta}(1+b_1)\\ &\leq 2^{\sum\beta_i}(1+b_1)\leq 2^{\lfloor n/2\rfloor}\cdot n\leq 2^{n-1}.\end{aligned}$$

If $l>1$ then $\sum_{i<l}b_i\leq n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|$, because every a_i generates $\mathbb{Z}_n$, and $b_l\leq\left(\sum_{i<l}b_i\right)/(l-1)$. This leads, much the same way as above, to

$$\begin{aligned}\prod_{i=1}^{\delta}(1+\beta_i)\prod_{i=1}^{l}(1+b_i) &= \prod_{i=1}^{\delta}(1+\beta_i)\prod_{i=1}^{l-1}(1+b_i)\cdot(1+b_l)\\ &\leq \Big(1+\frac{\sum\beta_i}{\delta}\Big)^{\delta}\Big(1+\frac{\sum_{i<l}b_i}{l-1}\Big)^{l-1}\Big(1+\frac{\sum_{i<l}b_i}{l-1}\Big)\\ &\leq \Big(1+\frac{\sum\beta_i}{\delta}\Big)^{\delta}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}\\ &\leq 2^{\sum\beta_i}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}\end{aligned}$$

which we conclude either applying the aforementioned lemma if its assumptions hold

$$2^{\sum\beta_i}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}\leq 2^{\sum\beta_i}\cdot 2^{n-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}\leq 2^{n-1}$$

or, otherwise, $l = 2$, $n - 1 - |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})| = 2$ and we just write for $n \geq 9$

$$2^{\sum \beta_i}\Big(1 + \frac{n - 1 - |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})|}{l - 1}\Big)^l \leq 2^{\lfloor n/2 \rfloor} \cdot 3^2 \leq 2^{n-1}.$$

□

In the following lemma we present the procedure which we use to find a proper sequence $\boldsymbol{t} = (t_i)$. If this procedure fails the previous lemma applies and, therefore, Schinzel's conjecture holds.

Lemma 3.3. *Under the assumptions of Theorem 1.1, assuming that* $(a_1, \ldots, a_k) = 1$, *either there exists some sequence* $\boldsymbol{t} = (t_i)$ *such that* $0 \leq t_i \leq b_i$, $\sum t_i \leq 3n/4$ *and* $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$, *or there exists some generator* a *of* $\mathbb{Z}_n$ *such that*

$$\sum_{i: a_i \neq \pm a} b_i \leq \min(\lfloor n/2 \rfloor, |C_n(\boldsymbol{a}, \boldsymbol{b} \cdot \mathbf{1}_{\{i: a_i \neq \pm a\}})| - 1).$$

Proof. Let us choose a sequence $\boldsymbol{t} = (t_i)$, $0 \leq t_i \leq b_i$, to be any minimal sequence with respect to $\sum t_i$ among maximal with respect to $|C_n(\boldsymbol{a}, \boldsymbol{t})|$ sequences satisfying $|C_n(\boldsymbol{a}, \boldsymbol{t})| \geq 2 \sum t_i$.

If $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ then

$$\sum t_i \leq |C_n(\boldsymbol{a}, \boldsymbol{b})|/2 \leq n/2.$$

Similarly, by Lemma 3.1, if $|C_n(\boldsymbol{a}, \boldsymbol{t})| = |C_n(\boldsymbol{a}, \boldsymbol{b})| - 1$ then for some j such that $t_j < b_j$ we have $C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_j}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ and

$$\sum t_i + (\boldsymbol{e_j})_i = 1 + \sum t_i \leq 1 + |C_n(\boldsymbol{a}, \boldsymbol{t})|/2 \leq (n+1)/2 \leq 3n/4$$

and we are done.

Let us now assume that none of the above cases holds. Therefore, $t_{j^*} < b_{j^*}$ and $|C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_{j^*}})| = |C_n(\boldsymbol{a}, \boldsymbol{t})| + 1$, for some particular j^*. Let us write $a = a_{j^*}$.

$C_n(\boldsymbol{a}, \boldsymbol{t})$ is therefore a union of fully filled cosets of some subgroup H of $\mathbb{Z}_n$ and an arithmetic progression P with common difference a, which is contained in another coset of H. In the subsequent parts of this argument we shall call any involved coset of H (fully or partially filled) an *active* one. Obviously, $|H| \geq 2$ and $|C_n(\boldsymbol{a}, \boldsymbol{t})| \geq 2$. A natural choice of H is simply $a\mathbb{Z}_n$ but we prefer to consider possibly large subgroup, so we shall assume that H is maximal.

If $P = C_n(\boldsymbol{a}, \boldsymbol{t})$ then, because $|P| = |C_n(\boldsymbol{a}, \boldsymbol{t})| \geq 2$, for any j such that $t_j < b_j$ we have $a_j \in a\mathbb{Z}_n$, as otherwise $C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_j})$ would be the disjoint union of $C_n(\boldsymbol{a}, \boldsymbol{t})$ and $C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \{a_j\}$. Since $0 \in P$, necessarily $C_n(\boldsymbol{a}, \boldsymbol{t}) \subseteq a\mathbb{Z}_n$ and consequently $C_n(\boldsymbol{a}, \boldsymbol{b}) \subseteq a\mathbb{Z}_n$. Therefore

$|C_n(\boldsymbol{a},\boldsymbol{t})| < |C_n(\boldsymbol{a},\boldsymbol{b})| - 1 \le |a\mathbb{Z}_n| - 1$, so $a_j = \pm a$. Hence $a_j \neq \pm a$ implies $t_j = b_j$ and

$$\sum_{i:a_i\neq\pm a} b_i = \sum_{i:a_i\neq\pm a} t_i \le \min(\lfloor n/2\rfloor, |C_n(\boldsymbol{a},\boldsymbol{b}\cdot\mathbf{1}_{\{i:a_i\neq\pm a\}})| - 1).$$

Here, the first inequality stems from $\sum t_i \le \lfloor n/2\rfloor$ and the second, by Lemma 3.1, from minimality of the chosen sequence $\boldsymbol{t}$. Furthermore, a generates $\mathbb{Z}_n$ by our assumption that $(a_1,\dots,a_k) = 1$.

In the case when $P \neq C_n(\boldsymbol{a},\boldsymbol{t})$ we know that every fully filled coset of H is mapped onto some other such coset under the mapping $x \mapsto x+a_j$. If it was not so, the above would apply to the active cosets of $C_n(\boldsymbol{a},\boldsymbol{t})$. Moreover, by maximality of $\boldsymbol{t}$, we would have $|P| = |H|-1$. This would, however, contradict the assumption that $C_n(\boldsymbol{a},\boldsymbol{t}) < C_n(\boldsymbol{a},\boldsymbol{b})-1$. Hence, by maximality of H, we get $a_j \in H$.

This allows us to invoke Lemma 3.1 in order to find a sequence $\boldsymbol{\tau} = (\tau_i)$ such that $0 \le \tau_i \le b_i - t_i$, $C_n(\boldsymbol{a},\boldsymbol{t}+\boldsymbol{\tau}) = C_n(\boldsymbol{a},\boldsymbol{b})$ and $\sum\tau_i \le |C_n(\boldsymbol{a},\boldsymbol{b})| - |C_n(\boldsymbol{a},\boldsymbol{t})|$. In particular

$$\sum t_i \le \frac{1}{2}|C_n(\boldsymbol{a},\boldsymbol{t})| \le \frac{1}{2}(|C_n(\boldsymbol{a},\boldsymbol{b})| - \sum\tau_i) \le \frac{1}{2}(n - \sum\tau_i).$$

Then, because $|C_n(\boldsymbol{a},\boldsymbol{b})| - |C_n(\boldsymbol{a},\boldsymbol{t})| \le |H|$, we have $\sum\tau_i \le |H|$ and, by a simple calculation,

$$\begin{aligned}\sum t_i + \sum\tau_i &\le \frac{1}{2}(n - \sum\tau_i) + \sum\tau_i\\ &= \frac{n}{2} + \frac{1}{2}\sum\tau_i\\ &\le \frac{n}{2} + \frac{1}{2}\cdot|H| \le \frac{n}{2} + \frac{1}{2}\cdot\frac{n}{2}\\ &\le \frac{3}{4}n.\end{aligned}$$

The sequence $\boldsymbol{t}+\boldsymbol{\tau}$ is just a one we look for. □

4. Proof of the theorem

We deal with the cases when $n < 22$ by referring to Schinzel's Theorem 1.2. For $n \ge 22$ we apply Lemma 3.3. If the lemma results in some generator a of $\mathbb{Z}_n$, we can apply Lemma 3.2, which readily shows the theorem.

In the other case, there is a sequence $\boldsymbol{t} = (t_i)$, $0 \le t_i \le b_i$, such that $\sum t_i \le 3n/4$ and $C_n(\boldsymbol{a},\boldsymbol{t}) = C_n(\boldsymbol{a},\boldsymbol{b})$. Moreover

$$N_{c_0;n}(\boldsymbol{a},\boldsymbol{t}\le\boldsymbol{b}) \ge \prod(1+b_i-t_i)/n$$

for some $c_0 \in C_n(\boldsymbol{a},\boldsymbol{b}) = C_n(\boldsymbol{a},\boldsymbol{t})$.

By subtracting one particular solution represented in $N_{c_0;n}(\boldsymbol{a},\boldsymbol{t})$ from all those counted in $N_{c_0;n}(\boldsymbol{a},\boldsymbol{t}\leq\boldsymbol{b})$ we get at least $\prod(1+b_i-t_i)/n$ solutions of the considered equation, so $N_n(\boldsymbol{a},\boldsymbol{b})\geq\prod(1+b_i-t_i)/n$.

By Bernoulli's inequality

$$1+b_i-t_i\geq(1+b_i)^{1-t_i/b_i}\geq\frac{1+b_i}{2^{t_i}}$$

Hence, for $n\geq 22$,

$$\begin{aligned}N_n(\boldsymbol{a},\boldsymbol{b}) &\geq \frac{1}{n}\prod(1+b_i-t_i)\geq\frac{1}{n}\prod\frac{1+b_i}{2^{t_i}}\\ &\geq \frac{\prod(1+b_i)}{n\cdot 2^{\sum t_i}}\geq\frac{\prod(1+b_i)}{n2^{3n/4}}\\ &\geq 2^{1-n}\prod(1+b_i).\end{aligned}$$

5. Concluding remarks

The reasoning used in the proof of Lemma 3.3 can be easily adapted to the general abelian group case. We remark here that while we do not attempt to generalize Lemma 3.2, it is only applied if Lemma 3.3 results in some generator of a cyclic subgroup. Consequently, a theorem follows.

Theorem 5.1. *Let G be a finite abelian group, $|G|\geq 22$ or G cyclic, k be a positive integer, $\boldsymbol{a}=(a_1,\ldots,a_k)$ and $\boldsymbol{b}=(b_1,\ldots,b_k)$ be sequences such that $a_i\in G$ and $b_i\in\mathbb{N}$ for $i=1,\ldots,k$. Then*

$$N_G(\boldsymbol{a},\boldsymbol{b})\geq 2^{1-|G|}\prod_{i=1}^{k}(1+b_i).$$

On the other hand, while an inspection of our method reveals that it applies well to the question of bounding the number $N_n(\boldsymbol{a},\boldsymbol{b}^-\leq\boldsymbol{b}^+)$, the result of Schinzel that we rely on fails in this more general case. For this reason, we do not claim any bound of the form

$$N_n(\boldsymbol{a},\boldsymbol{b}^-\leq\boldsymbol{b}^+)\geq\gamma(n)\cdot\prod_{i=1}^{k}(1+b_i^+-b_i^-),$$

even if there exists a solution of the corresponding equation.

Acknowledgements

The first author is supported by the National PhD Programme in Mathematical Sciences at the University of Warsaw.

The second author is supported by the Ministry of Science and Higher Education, grant no. N N201 543538.

References

[1] J. Kaczorowski, Appendix to '*The number of solutions of a linear homogeneous congruence II*' by A. Schinzel, in: Analytic Number Theory: essays in honour of Klaus Roth, W. W. L. Chen et al. (eds.), Cambridge University Press, 2009, 411-413.

[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.), Springer-Verlag, 2008, 363-370.

[4] A. Schinzel, *The number of solutions of a linear homogeneous congruence II*, in: Analytic Number Theory: essays in honour of Klaus Roth, W. W. L. Chen et al. (eds.), Cambridge University Press, 2009, 402-413.

[5] A. Schinzel, M. Zakarczemny, *On a linear homogeneous congruence*, Colloq. Math. 106 (2006), no. 2, 283-292.

Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland

E-mail address: cwalina@mimuw.edu.pl

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland

E-mail address: schoen@amu.edu.pl