ACTA ARITHMETICA
153.3 (2012)

The number of solutions of a homogeneous linear congruence

by

KAROL CWALINA (Warszawa) and TOMASZ SCHOEN (Poznań)

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 $(x_1, \ldots, x_k)$ of the congruence

$$a_1x_1 + \cdots + a_kx_k \equiv 0 \pmod{n}$$

in integers satisfying $0 \le x_i \le b_i$. 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

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

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 $N_n(\boldsymbol{a}, \boldsymbol{b}) = N_n(\boldsymbol{1}, \boldsymbol{1}) = 1$, we can see that $\gamma(n) = 2^{1-n}$ would be the best possible coefficient, provided we restrict ourselves to those depending 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.

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

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

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

2010 *Mathematics Subject Classification*: Primary 11D79.
Key words and phrases: linear homogeneous equation.

DOI: 10.4064/aa153-3-3

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

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

Then, under the assumptions of Theorem 1.1,

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

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

We will use this theorem to prove Theorem 1.1 for $n < 22$.

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

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

Our proof of Theorem 1.1 will be based on Kaczorowski's idea.

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 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 $\boldsymbol{a} = (a_1, \ldots, a_k)$ be a sequence such that $a_i \in G$ for $i = 1, \ldots, k$. Then*

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

A natural conjecture which would unify these results is the following.

Conjecture. *Let G be a finite abelian group, k be a positive integer, and $\boldsymbol{a} = (a_1, \ldots, a_k)$ 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*

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

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. We adopt the following non-standard notation.

Definition. Let n be a positive integer, I be any set, and $\boldsymbol{b}^- = (b_i^-)_{i\in I}$, $\boldsymbol{b}^+ = (b_i^+)_{i\in I}$ be sequences of integers satisfying $0 \le b_i^- \le b_i^+$. 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 $N_{c;n}(\boldsymbol{a}, \boldsymbol{b}^- \le \boldsymbol{b}^+)$ as the number of integer solutions $(x_i)_{i\in I}$ with $b_i^- \le x_i \le b_i^+$ of the equation

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

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

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

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 $i \ne j$. 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 $A \subset I$.

Arithmetic operations on sequences are meant to be performed coordinatewise.

We identify an element with a one-element sequence. When the elements considered split into subfamilies, we separate them by semicolons, e.g. $N_{c;n}(\boldsymbol{a}, \boldsymbol{t} \le \boldsymbol{b}; \boldsymbol{a}', \boldsymbol{t}' \le \boldsymbol{b}')$. In all cases, indexing sets will be given implicitly. Finally, we shall usually drop zeros from the notation, therefore $N_n(\boldsymbol{a}, \boldsymbol{b}) = N_{0;n}(\boldsymbol{a}, \mathbf{0} \le \boldsymbol{b})$.

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 $N_{c_0;n}(\boldsymbol{a}, \boldsymbol{t} \le \boldsymbol{b}) \ge \frac{1}{n}\prod(1 + b_i - t_i)$ for some residue class c_0. If $\sum t_i$ is considerably smaller than n, then we can easily conclude that

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \ge N_{c_0;n}(\boldsymbol{a}, \boldsymbol{t} \le \boldsymbol{b}) \ge 2^{1-n} \prod (1 + b_i)$$

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: $(1 + a/x)^x \le 2^a$ 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 $\gcd(a_1, \ldots, a_k) = 1$.

We can also restrict our attention to the case when $0 < b_i < n$ for all i. This basically follows from the observation that both the function $N_n(\cdot)$ and the desired 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 $b_1 < n$. Then

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

We now prove an easy lemma which will turn out useful in our proof of the theorem. It also justifies the claim, appearing in the preceding section, 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 $\sum t_i \le n - 1$.

Lemma 3.1. *If* $0 \le t_i \le b_i$ *and* $C_n(\boldsymbol{a}, \boldsymbol{t}) \neq C_n(\boldsymbol{a}, \boldsymbol{b})$ *then there exists* 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 $A \oplus B = \{a + b : a \in A,\ b \in B\}$.

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 obtain

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

— 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*

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

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

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

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

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

$$(1 + a/x)^{x+1} \leq 2^{a+1},$$

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_j generates $\mathbb{Z}_n$, we have

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

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

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

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

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

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

and it is now sufficient to prove that

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

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

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

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

$$\begin{aligned}\prod_{i=1}^{\delta}(1+\beta_i)\prod_{j=1}^{l}(1+b_j) &= \prod_{i=1}^{\delta}(1+\beta_i)\prod_{j=1}^{l-1}(1+b_j)\cdot(1+b_l)\\ &\le \left(1+\frac{\sum\beta_i}{\delta}\right)^{\delta}\left(1+\frac{\sum_{j<l}b_j}{l-1}\right)^{l-1}\left(1+\frac{\sum_{j<l}b_j}{l-1}\right)\\ &\le \left(1+\frac{\sum\beta_i}{\delta}\right)^{\delta}\left(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\right)^{l}\\ &\le 2^{\sum\beta_i}\left(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\right)^{l}.\end{aligned}$$

Now we can conclude, since either we can apply the aforementioned lemma, if its assumptions hold, and then

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

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

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

In the following lemma we present a procedure 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 moreover that* $\gcd(a_1,\dots,a_k)=1$, *either there exists some sequence* $\boldsymbol{t}=(t_i)$ *such that* $0\le t_i\le b_i$, $\sum t_i\le 3n/4$ *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*

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

Proof. Choose $\boldsymbol{t}=(t_i)$, $0\le t_i\le b_i$, to be any sequence minimal with respect to $\sum t_i$ among the sequences maximal with respect to $|C_n(\boldsymbol{a},\boldsymbol{t})|$ and satisfying $|C_n(\boldsymbol{a},\boldsymbol{t})|\ge 2\sum t_i$.

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

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

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

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

and we are done.

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

$C_n(\boldsymbol{a},\boldsymbol{t})$ is therefore a union of 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 coset of H involved an *active* one and any such coset contained in $C_n(\boldsymbol{a},\boldsymbol{t})$ a *full* 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 a 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

$$|C_n(\boldsymbol{a},\boldsymbol{t})| < |C_n(\boldsymbol{a},\boldsymbol{b})| - 1 \leq |a\mathbb{Z}_n| - 1,$$

so $a_j = \pm a$. Consequently, $a_j \neq \pm a$ implies $t_j = b_j$ and

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

Here, the first inequality stems from $\sum t_i \leq \lfloor n/2 \rfloor$ 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 $\gcd(a_1,\ldots,a_k) = 1$.

In the case when $P \neq C_n(\boldsymbol{a},\boldsymbol{t})$ every full coset of H is mapped onto some other such coset under the mapping $x \mapsto x + a_j$. If it were not so, the above would apply to the active cosets. Moreover, by maximality of $\boldsymbol{t}$, we would have $|P| = |H| - 1$. This, however, would 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 $C_n(\boldsymbol{a},\boldsymbol{t}+\boldsymbol{\tau}) = C_n(\boldsymbol{a},\boldsymbol{b})$ with $\sum \tau_i \leq |C_n(\boldsymbol{a},\boldsymbol{b})| - |C_n(\boldsymbol{a},\boldsymbol{t})|$ and $0 \leq \tau_i \leq b_i - t_i$. In particular

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

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

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

The sequence $\boldsymbol{t}+\boldsymbol{\tau}$ is just one we are looking for. ∎

4. Proof of the theorem. We deal with the cases when $n < 22$ by referring to Schinzel's Theorem 1.2. For $n \geq 22$ 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 $N_{c_0;n}(\boldsymbol{a}, \boldsymbol{t} \le \boldsymbol{b})$ we get at least $\prod(1 + b_i - t_i)/n$ solutions of the equation considered, so $N_n(\boldsymbol{a}, \boldsymbol{b}) \ge \prod(1 + b_i - t_i)/n$.

By Bernoulli's inequality,

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

Hence, for $n \ge 22$,

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

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, we obtain

THEOREM 5.1. *Let G be a finite abelian group, $|G| \ge 22$ or G cyclic, k be a positive integer, and $\boldsymbol{a} = (a_1, \dots, a_k)$ 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*

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

On the other hand, while an inspection of our method reveals that it still applies to the question of bounding the number $N_n(\boldsymbol{a}, \boldsymbol{b}^- \le \boldsymbol{b}^+)$, 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

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

even if there exists a solution of the corresponding equation.

Acknowledgments. 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, Poland, grant no. N N201 543538.

References

[1] J. Kaczorowski, Appendix to [4], 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, 2008, 363–370.

[4] —, *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 Univ. Press, 2009, 402–413.

[5] A. Schinzel and M. Zakarczemny, *On a linear homogeneous congruence*, Colloq. Math. 106 (2006), 283–292.

Karol Cwalina
Faculty of Mathematics,
Informatics and Mechanics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: cwalina@mimuw.edu.pl

Tomasz Schoen
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
Umultowska 87
61-614 Poznań, Poland
E-mail: schoen@amu.edu.pl

Received on 17.12.2010
and in revised form on 1.10.2011 and 5.1.2012 (6579)