

ON A LINEAR HOMOGENEOUS CONGRUENCE

BY

A. SCHINZEL (Warszawa) and M. ZAKARCZEMNY (Kraków)

Abstract. The number of solutions of the congruence $a_1x_1 + \dots + a_kx_k \equiv 0 \pmod{n}$ in the box $0 \leq x_i \leq b_i$ is estimated from below in the best possible way, provided for all i, j either $(a_i, n) \mid (a_j, n)$ or $(a_j, n) \mid (a_i, n)$ or $n \mid [a_i, a_j]$.

1. Introduction. We shall consider the following conjecture proposed in [1]:

CONJECTURE. Let k, n and b_i ($1 \leq i \leq k$) be positive integers, and let a_i ($1 \leq i \leq k$) be any integers. The number $N(n; a_1, b_1, \dots, a_k, b_k)$ of solutions of the congruence

$$(1) \quad \sum_{i=1}^k a_i x_i \equiv 0 \pmod{n} \quad \text{in the box } 0 \leq x_i \leq b_i$$

satisfies the inequality

$$(2) \quad N(n; a_1, b_1, \dots, a_k, b_k) \geq 2^{1-n} \prod_{i=1}^k (b_i + 1).$$

Since for $k = n - 1$,

$$N(n; 1, 1, \dots, 1) = 2^{1-n} \prod_{i=1}^k (1 + 1),$$

if the above conjecture is true, then 2^{1-n} is the best possible coefficient independent of a_i, b_i , and dependent only on n , with which the inequality (2) holds. The first named author proved in [1] that (2) holds if $(n, a_i) = 1$ for all $i \leq k$. The aim of this paper is to prove

THEOREM. The inequality (2) holds if for all $i, j \leq k$ we have either $(n, a_i) \mid (n, a_j)$ or $(n, a_j) \mid (n, a_i)$, or $n \mid [a_i, a_j]$.

COROLLARY 1. The inequality (2) holds for $n = p^\alpha$ and for $n = pq$ (p, q primes).

2000 *Mathematics Subject Classification*: Primary 11D79.

Key words and phrases: linear homogeneous congruence.

2. Lemmas. We shall use the following lemmas taken from [1]:

LEMMA A. *Inequality (2) holds for $n = 4$, a_1 and a_2 odd, $b_1 = b_2 = 2$.*

LEMMA B. *Let B be a set of residues mod m , and let $a, b \in \mathbb{N}$ with $(a, m) = 1$. If x runs through the integers of the interval $[0, b]$ and y through the elements of B , then $ax + y$ gives at least $\min\{m, |B| + b\}$ residues mod m .*

LEMMA C. *For positive integers a and $x \leq a$ we have*

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

except for $a = 2$ and $x = 1$.

From Lemma B we deduce

LEMMA 1. *Let A be a set of residues mod m , and let $a, b \in \mathbb{N}$ with $(a, m) = 1$ and $b \geq m - |A|$. For every r the number of solutions of the congruence $ax + y \equiv r \pmod{m}$ such that $0 \leq x \leq b$, $y \in A$ is at least*

$$s = \left\lceil \frac{b + 1}{m + 1 - |A|} \right\rceil \geq \max \left\{ 1, \frac{b + 1}{2(m + 1 - |A|) - 1} \right\}.$$

Proof. Put $m - |A| = c$ and consider the intervals (reduced to a point for $c = 0$)

$$I_i = [ci + i, c(i + 1) + i], \quad 0 \leq i \leq s - 1.$$

Each interval I_i contains $c + 1$ consecutive integers, hence by Lemma B, $ax + y$ with $y \in A$ gives $c + |A| = m$ residues mod m , thus in particular r . Since the s intervals I_i are disjoint we obtain the first part of the lemma. The second part (the inequality) follows from the inequality

$$u \geq \frac{uv + v - 1}{2v - 1}$$

valid for $u, v \geq 1$, in which we take $u = \left\lceil \frac{b+1}{m+1-|A|} \right\rceil$, $v = m + 1 - |A|$.

We have further

LEMMA 2. *If $a > (\log 2)^{-1}$, then the function $(a - x)2^x$ is unimodal in the interval $[0, a]$ with the maximum at $x = a - (\log 2)^{-1}$.*

Proof. By differentiation.

For the proof of further lemmas we need the following definitions and corollaries.

DEFINITION 1. $d_i = (n, a_i)$, $n_i = n/d_i$ ($1 \leq i \leq k$).

COROLLARY 2. *Under the assumption of the Theorem we have for all $i, j \leq k$ either $n_i | n_j$ or $n_j | n_i$ or $(n_i, n_j) = 1$.*

DEFINITION 2. We write $i \prec j$ if $n_i | n_j$ and either $n_i < n_j$ or $i < j$.

COROLLARY 3. \prec is a partial ordering of the set $\{1, \dots, k\}$.

DEFINITION 3. N_l is the number of residues mod n given by the numbers $\sum_{i \prec l} a_i x_i$, where $0 \leq x_i \leq b_i$.

DEFINITION 4. $c(i)$ is the number of $j \leq i$ such that $n_j = n_i$.

Now we can formulate

LEMMA 3. If for $0 \leq x_i \leq b_i$ the sum $\sum_{i \prec l} a_i x_i$ gives at least $1 + \sum_{i \prec l} b_i$ residues mod n , then

$$N_l \geq \min \left\{ n_l, 1 + \sum_{i \prec l} b_i \right\}.$$

Proof. Since $(n, a_l) = d_l$ divides a_i for $i \prec l$,

$$\sum_{i \prec l} \frac{a_i}{d_l} x_i \text{ gives at least } 1 + \sum_{i \prec l} b_i \text{ residues mod } n_l.$$

We apply Lemma B with B being the set of these residues and with $m = n_l$, $a = a_l/d_l$. The assumptions are satisfied, since

$$\left(\frac{a_l}{d_l}, n_l \right) = \frac{(a_l, n)}{d_l} = 1.$$

Therefore, the number of residues mod n_l of $\sum_{i \prec l} (a_i/d_l)x_i$ is at least

$$\min \left\{ n_l, 1 + \sum_{i \prec l} b_i \right\}$$

and hence

$$\sum_{i \prec l} a_i x_i \text{ gives at least } \min \left\{ n_l, 1 + \sum_{i \prec l} b_i \right\} \text{ residues mod } n.$$

LEMMA 4. If for an $l \leq k$ and all $g \prec l$ we have

$$(3) \quad \sum_{i \leq g} b_i \leq n_g - 1,$$

then

$$N_l \geq \min \left\{ n_l, 1 + \sum_{i \prec l} b_i \right\}.$$

Proof. Let I_h be the set of $i \leq k$ for which there exists a sequence i_1, \dots, i_h such that $i_1 = i$, $n_{i_\nu} | n_{i_{\nu+1}}$, $n_{i_\nu} < n_{i_{\nu+1}}$ ($1 \leq \nu < h$) and there exists no longer sequence with this property. Clearly, for a certain s ,

$$\{1, \dots, k\} = \bigcup_{h=1}^s I_h$$

and $I_g \cap I_h = \emptyset$ for $g \neq h$. Moreover, by Corollary 2,

$$(4) \quad \text{if } i, j \in I_h \text{ and } n_i \neq n_j, \text{ then } (n_i, n_j) = 1.$$

If $l \in I_h$ we shall write $h(l) = h$. We shall prove the lemma by a double induction, with respect to $s - h(l)$ and with respect to $c(l)$. If $s - h(l) = 0$ and $c(l) = 1$, then $i \preceq l$ implies $i = l$. We have two possibilities.

If $b_l + 1 \geq n_l$, then $(a_l/d_l)x_l$ ($0 \leq x_l \leq b_l$) gives all residues mod n_l , hence $a_l x_l$ gives n_l residues mod n , thus $N_l = n_l$.

If $b_l + 1 < n_l$, then $(a_l/d_l)x_l$ ($0 \leq x_l \leq b_l$) gives $b_l + 1$ residues mod n_l , hence $a_l x_l$ gives $b_l + 1$ residues mod n , thus $N_l \geq b_l + 1$. Assume now that the assertion is true for $s - h(l') = 0$ and $c(l') = c - 1$ ($c \geq 2$), and that $s - h(l) = 0$, $c(l) = c$. Then $i \prec l$ if and only if $i \preceq l'$, where $n_{l'} = n_l$ and $c(l') = c - 1$. Clearly $s - h(l') = 0$ and by the inductive assumption and by (3) with $g = l'$,

$$N_{l'} \geq \min \left\{ n_{l'}, 1 + \sum_{i \preceq l'} b_i \right\} \geq 1 + \sum_{i \preceq l'} b_i.$$

Hence, by Lemma 3,

$$N_l \geq \min \left\{ n_l, 1 + \sum_{i \preceq l} b_i \right\}.$$

Assume now that the assumption is true for $s - h(l') = s - h - 1$ and that $h(l) = h$, $c(l) = 1$. Put

$$A_l = \{i \prec l : i \in I_{h+1} \wedge i = \max\{q : n_q = n_i\}\} = \{i_1, \dots, i_t\}.$$

If $t = 0$, then $i \preceq l$ implies $i = l$ and the proof proceeds as above for $s - h(l) = 0$, $c(l) = 1$. Therefore we assume that $t > 0$ and infer from (4) that

$$(5) \quad (n_{i_\mu}, n_{i_\nu}) = 1 \quad \text{for } \mu \neq \nu.$$

Since $c(l) = 1$, $i \prec l$ implies $i \preceq i_u$ for some $u \leq t$. By the inductive assumption the assertion is true for every $l' = i_u \in A_l \subset I_{h+1}$, hence by (3) for all $u \leq t$,

$$(6) \quad N_{i_u} \geq 1 + \sum_{i \preceq i_u} b_i.$$

For $i \preceq i_u$ we have

$$n_i \mid n_{i_u}, \quad d_{i_u} \mid d_i \mid a_i,$$

hence for each $u \leq t$,

$$\sum_{i \preceq i_u} \frac{a_i}{d_{i_u}} x_i \quad (0 \leq x_i \leq b_i) \quad \text{gives} \quad N_{i_u} \geq 1 + \sum_{i \preceq i_u} b_i \text{ residues mod } n_{i_u}.$$

Now, by (5) for all integers $z_1, \dots, z_t, r_1, \dots, r_t$ we have

$$\sum_{u=1}^t \frac{n}{n_{i_u}} z_u \equiv \sum_{u=1}^t \frac{n}{n_{i_u}} r_u \pmod{n}$$

if and only if $z_u \equiv r_u \pmod{n_{i_u}}$ for all $u \leq t$. It follows that the number of residues mod n given by

$$\sum_{u=1}^t \frac{n}{n_{i_u}} \sum_{i \preceq i_u} \frac{a_i}{n_{i_u}} x_i = \sum_{u=1}^t d_{i_u} \sum_{i \preceq i_u} \frac{a_i}{d_{i_u}} x_i = \sum_{u=1}^t \sum_{i \preceq i_u} a_i x_i = \sum_{i \prec l} a_i x_i$$

for $0 \leq x_i \leq b_i$ is equal to $\prod_{u=1}^t N_{i_u}$, hence by (6) it is at least

$$\prod_{u=1}^t \left(1 + \sum_{i \preceq i_u} b_i\right) \geq 1 + \sum_{u=1}^t \sum_{i \preceq i_u} b_i = 1 + \sum_{i \prec l} b_i.$$

Using Lemma 3 we obtain

$$N_l \geq \min \left\{ n_l, 1 + \sum_{i \prec l} b_i \right\},$$

which proves the assertion for $s - h(l) = s - h$, $c(l) = 1$.

Assume now that the assertion is true for $s - h(l') = s - h$ and $c(l') = c - 1$ ($c \geq 2$) and that $s - h(l) = s - h$, $c(l) = c$. Then $i \prec l$ if and only if $i \preceq l'$, where $n_{l'} = n_l$ and $c(l') = c - 1$. Clearly $s - h(l') = s - h$, thus by the inductive assumption and by (3),

$$N_{l'} \geq \min \left\{ n_{l'}, 1 + \sum_{i \preceq l'} b_i \right\} \geq 1 + \sum_{i \prec l'} b_i.$$

Hence, by Lemma 3,

$$N_l \geq \min \left\{ n_l, 1 + \sum_{i \prec l} b_i \right\}.$$

DEFINITION 5. $M = \bigcup_{i=1}^k \{n_i\}$.

LEMMA 5. Let us order a_i in such a way that $i \leq j$ implies $n_i \leq n_j$. Under the assumption of the Theorem, for every $l \preceq k$ either

(7) $\text{there exists } m' | n_l, m' \in M \setminus \{n_l\}$

such that

$$\sum_{n_i | m'} b_i \geq m',$$

or

(8) $\sum_{n_i | n_l, i \leq l} a_i x_i$ ($0 \leq x_i \leq b_i$) gives at least

$$\min \left\{ n_l, 1 + \sum_{n_i | n_l, i \leq l} b_i \right\} \text{ residues mod } n.$$

Proof. We apply Lemma 4. If there exists g not satisfying (3) such that $n_g | n_l, n_g < n_l$ then (7) holds with $m' = n_g$. If there exist g not satisfying (3)

with $n_g \mid n_l$, but for all of them $n_g = n_l$, then taking the least such g , by Lemma 4 we obtain

$$N_l \geq N_g \geq \min \left\{ n_g, \sum_{n_i \mid n_g, i \leq g} b_i \right\} = n_g = \min \left\{ n_l, \sum_{n_i \mid n_l, i \leq l} b_i \right\},$$

thus (8) holds.

Finally, if (3) is satisfied by all g with $n_g \mid n_l$, $g < l$, then (8) holds by Lemma 4.

LEMMA 6. *Let t, x_1, \dots, x_t be integers greater than 1. Then*

$$\sum_{u=1}^t (x_u - 2) \leq \frac{1}{2} \prod_{u=1}^t x_u - 2.$$

Proof. Since $x + y \leq xy$ for $x, y \geq 2$, we have

$$\sum_{u=1}^t (x_u - 2) = \sum_{u=1}^t x_u - 2t \leq \prod_{u=1}^{t-1} x_u + x_t - 2t.$$

Since $x + y - 2 \leq xy/2$ for $x, y \geq 2$, we have

$$\prod_{u=1}^{t-1} x_u + x_t - 2t \leq \frac{1}{2} \prod_{u=1}^t x_u - 2(t-1) \leq \frac{1}{2} \prod_{u=1}^t x_u - 2.$$

Combining both inequalities we obtain the lemma.

3. Proof of the Theorem. We may assume without loss of generality that if $i \leq j$ then either $n_i < n_j$, or $n_i = n_j$ and $b_i \geq b_j$. By Corollary 2, for all $i, j \leq k$ we have

$$(9) \quad \text{either } n_i \mid n_j \text{ or } n_j \mid n_i \text{ or } (n_i, n_j) = 1.$$

We proceed by induction on k . For $k = 1$, (2) is trivially true. Assume it is true for all $k' < k$. If $n_1 = 1$ then

$$N(n; a_1, b_1, \dots, a_k, b_k) = (b_1 + 1)N(n; a_2, b_2, \dots, a_k, b_k),$$

hence (2) follows from the inductive assumption.

Therefore assume that $n_i \geq 2$, and $n \geq 4$ by the result of [1]. Suppose that there exist $\bar{m} \in M$ such that $\sum_{n_i \mid \bar{m}} b_i \geq \bar{m} - 1$ and let m be the least number with this property. Hence for all $m' < m$, $m' \in M$ we have

$$(10) \quad \sum_{n_i \mid m'} b_i \leq m' - 2.$$

Let m_u ($1 \leq u \leq t$) be all maximal elements with respect to divisibility in the set $\{\mu \in M \setminus \{m\} : \mu \mid m\}$. We have $m_u \in M \setminus \{m\}$, $m_u \mid m$, and the m_u are not divisible by one another, hence by (9), $(m_u, m_v) = 1$ for $u \neq v$. It follows that

$$(11) \quad \prod_{u=1}^t m_u \mid m.$$

We take the least j such that

$$(12) \quad \sum_{n_i \mid m, i \leq j} b_i \geq m - 1.$$

By (10) we have

$$\sum_{n_i \mid m_u} b_i \leq m_u - 2,$$

hence by Lemma 6,

$$(13) \quad \sum_{u=1}^t \sum_{n_i \mid m_u} b_i \leq \sum_{u=1}^t (m_u - 2) \leq \frac{1}{2} \prod_{u=1}^t m_u - 2 \leq \frac{1}{2} m - 2,$$

unless $t \leq 1$. However, for $t \leq 1$ the inequality

$$\sum_{u=1}^t (m_u - 2) \leq \frac{1}{2} m - 2$$

is also true, thus (12) and (13) imply $n_j \nmid m_u$ ($1 \leq u \leq t$), hence $n_j = m$.

Also, by Lemma 5, inequality (10) and the choice of j the number of residues mod n given by $\sum_{n_i \mid m, i < j} a_i x_i$ ($0 \leq x_i \leq b_i$) is at least $1 + \sum_{n_i \mid m, i < j} b_i$. For every choice of x_i ($n_i \nmid m$ or $i > j$) such that

$$(14) \quad \sum_{n_i \nmid m \text{ or } i > j} a_i x_i \equiv 0 \pmod{\frac{n}{m}}$$

there exist, by Lemma 1, at least

$$\max \left\{ 1, \frac{b_j + 1}{2(m - \sum_{n_i \mid m, i < j} b_i) - 1} \right\}$$

solutions of the congruence

$$\frac{m}{n} \sum_{n_i \mid m, i < j} a_i x_i + \frac{m a_j}{n} x_j + \frac{m}{n} \sum_{n_i \nmid m \text{ or } i > j} a_i x_i \equiv 0 \pmod{m},$$

satisfying $0 \leq x_i \leq b_i$ ($n_i \mid m$ and $i \leq j$). However, the number of summands in (14) is less than k , hence, by the inductive assumption, the number of solutions of (14) with $0 \leq x_i \leq b_i$ is at least

$$2^{1-n/m} \prod_{n_i \nmid m \text{ or } i > j} (b_i + 1).$$

Thus we obtain

$$(15) \quad N(n; a_1, b_1, \dots, a_k, b_k) \\ \geq 2^{1-n/m} \prod_{n_i \nmid m \text{ or } i > j} (b_i + 1) \max \left\{ 1, \frac{b_j + 1}{2(m - \sum_{n_i | m, i < j} b_i) - 1} \right\}.$$

We consider three cases:

$$(16) \quad m < n,$$

$$(17) \quad m = n \quad \text{and} \quad \text{either } j = 1 \text{ or } n_{j-1} < n,$$

$$(18) \quad m = n, \quad j \geq 2 \quad \text{and} \quad n_{j-1} = n.$$

In the case (16) we have, by (15) and Bernoulli's inequality,

$$(19) \quad N(n; a_1, b_1, \dots, a_k, b_k)^{-1} \prod_{i=1}^k (b_i + 1) \\ \leq 2^{n/m} \left(m - \sum_{n_i | m, i < j} b_i - \frac{1}{2} \right) \prod_{n_i | m, i < j} (b_i + 1) \\ \leq 2^{n/m} \left(m - b - \frac{1}{2} \right) 2^b,$$

where $b = \sum_{n_i | m, i < j} b_i$. By the choice of j we have

$$b \leq m - 2 < m - \frac{1}{2} - \frac{1}{\log 2},$$

hence by Lemma 2,

$$\left(m - b - \frac{1}{2} \right) 2^b \leq 3 \cdot 2^{m-3} < 2^{m-1},$$

and by (19),

$$N(n; a_1, b_1, \dots, a_k, b_k)^{-1} \prod_{i=1}^k (b_i + 1) < 2^{n/m+m-1} \leq 2^{n-1},$$

because $n - n/m - m = (n/m - 1)(m - 1) - 1 \geq 0$.

In the case (17) we have again (19), but now, by (13),

$$b \leq \frac{1}{2}n - 2 \leq n - \frac{1}{2} - \frac{1}{\log 2},$$

hence by Lemma 2 and Bernoulli's inequality

$$\left(m - b - \frac{1}{2} \right) 2^b \leq \left(\frac{n}{2} + \frac{3}{2} \right) 2^{n/2-2} \leq 2^{n-3/2}.$$

In the case (18) we have, by (15),

$$\begin{aligned}
 (20) \quad N(n; a_1, b_1, \dots, a_k, b_k)^{-1} \prod_{i=1}^k (b_i + 1) &\leq \prod_{n_i|m, i \leq j} (b_i + 1) \\
 &\leq \prod_{n_i|m, n_i < m} (b_i + 1) \cdot \prod_{n_i=m, i \leq j} (b_i + 1) \\
 &\leq 2^{\sum_{n_i|m, n_i < m} b_i} \prod_{n_i=m, i \leq j} (b_i + 1).
 \end{aligned}$$

Now, by the choice of j ,

$$\sum_{n_i|m, i < j} b_i \leq n - 2, \quad \sum_{n_i=m, i < j} b_i \leq n - 2 - \sum_{n_i|m, n_i < m} b_i,$$

thus $b_j \leq b_{j-1} \leq a/x$, where

$$a = n - 2 - \sum_{n_i|m, n_i < m} b_i, \quad x = \sum_{n_i=m, i < j} 1.$$

By the inequality for the arithmetic and geometric mean and by Lemma C,

$$\prod_{n_i=m, i \leq j} (b_i + 1) \leq \left(1 + \frac{a}{x}\right)^{x+1} \leq 2^{a+1},$$

unless $a = 2, x = 1$. Leaving this case for a further consideration we obtain from (20),

$$\begin{aligned}
 N(n; a_1, b_1, \dots, a_k, b_k)^{-1} \prod_{i=1}^k (b_i + 1) \\
 \leq 2^{\sum_{n_i|m, n_i < m} b_i} \cdot 2^{n-1-\sum_{n_i|m, n_i < m} b_i} = 2^{n-1}.
 \end{aligned}$$

If $a = 2, x = 1$ we obtain, because of (13),

$$n - 4 = \sum_{n_i|m, n_i < m} b_i \leq \frac{1}{2}n - 2,$$

hence $n \leq 4$, that is, $n = 4$; moreover, $j = 2, n_1 = n_2 = 4, b_2 \leq b_1 \leq 2$ and

$$N(n; a_1, b_1, \dots, a_k, b_k)^{-1} \prod_{i=1}^k (b_i + 1) \leq (b_1 + 1)(b_2 + 1) \leq 2^{n-1}$$

unless $b_1 = b_2 = 2$. However, the last case is covered by Lemma A.

Assume now that for every $m \in M$ we have

$$(21) \quad \sum_{n_i|m} b_i \leq m - 2.$$

If $n \in M$ it follows that

$$(22) \quad \sum_{i=1}^k b_i \leq n - 2.$$

If $n \notin M$, then for every n_i there exists the greatest $m \in M$ such that $n_i \mid m$. Put $m = f(n_i)$ and $M_0 = f(M)$. It follows from (9) that the elements of M_0 are coprime. Hence

$$\prod_{m \in M_0} m \mid n$$

and, by Lemma 6,

$$\sum_{n \in M_0} (m - 2) \leq \frac{1}{2} \prod_{m \in M_0} m - 2 \leq \frac{1}{2} n - 2$$

unless M_0 has just one element m_0 .

However, $m_0 \leq \frac{1}{2}n$, thus in each case, by (21),

$$\sum_{i=1}^k b_i \leq \sum_{m \in M_0} \sum_{n_i \mid m} b_i \leq \sum_{m \in M_0} (m - 2) \leq \frac{1}{2} n - 2$$

and (22) holds generally. It follows by Bernoulli's inequality that

$$N(n; a_1, b_1, \dots, a_k, b_k)^{-1} \prod_{i=1}^k (b_i + 1) \leq 2^{\sum_{i=1}^k b_i} \leq 2^{n-2}.$$

Added in proof. As proved in [2], the inequality (2) holds if $n = \prod_{j=1}^l q_j^{\alpha_j}$, where q_j are primes and $\sum_{j=1}^l 1/q_j < 1$.

REFERENCES

- [1] A. Schinzel, *The number of solutions of a linear homogeneous congruence*, the volume in honour of Wolfgang M. Schmidt (to appear).
- [2] —, *The numbers of solutions of a linear homogeneous congruence II*, the volume in honour of Klaus F. Roth (to appear).

Institute of Mathematics
Polish Academy of Sciences
P.O. Box 21
00-956 Warszawa, Poland
E-mail: schinzel@impan.gov.pl

Institute of Mathematics
Jagiellonian University
Reymonta 4
30-059 Kraków, Poland
E-mail: hhuugg@wp.pl

Received 9 September 2005;
revised 10 February 2006

(4661)