

The Indecomposable Solutions of Linear Congruences

Klaus Pommerening
 Johannes-Gutenberg-Universität
 Mainz, Germany
 pommeren@uni-mainz.de

Abstract The linear congruence $a_1x_1 + \cdots + a_nx_n \equiv 0 \pmod{m}$ for unknown non-negative integers x_1, \dots, x_n is easily reduced to the standard congruence $1 \cdot x_1 + \cdots + (m-1) \cdot x_{m-1} \equiv 0 \pmod{m}$. This article gives a tight new geometric bound for the minimal non-zero solutions of this standard congruence and derives bounds for their number.

Among the topics of additive number theory linear Diophantine problems play a prominent role. Here are two typical problems, for simplicity each one restricted to the case of a single equation or congruence:

The homogeneous equation: Given a coefficient vector $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$, determine (some or all) $x = (x_1, \dots, x_n) \in \mathbb{N}^n$ with

$$\text{(E)} \quad a_1x_1 + \cdots + a_nx_n = 0.$$

The linear congruence: Given $m \in \mathbb{N}_2$ and $a \in \mathbb{Z}^n$, determine $x \in \mathbb{N}^n$ with

$$\text{(A)} \quad a_1x_1 + \cdots + a_nx_n \equiv 0 \pmod{m}.$$

(Without loss of generality we may assume that $0 \leq a_i < m$ for all i .)

Note that in this article \mathbb{N} stands for the numbers $\{0, 1, 2, \dots\}$, and \mathbb{N}_k for $\{k, k+1, \dots\}$. Think of 0 as being the most natural number.

In general it's trivial to find lots of single solutions, and there are several algorithms that produce all indecomposable solutions, see [4] for the equation (E) and [11] for the congruence (A). But it seems difficult to get an

overview over the complete solution set, in particular to estimate the numbers of indecomposable solutions. For $m \leq 38$ the sequence A096337 of OEIS [9] indicates the number of indecomposable solutions of what we call the standard linear congruence (\mathbf{C}_m). In [5] these numbers (+1) are even listed for m up to 60. The paper [2] gives a weak asymptotic lower bound.

This article derives some new results on the linear congruence, in particular a geometric bound for the coordinates of indecomposable solutions, and bounds for their number. A following one will treat the linear equation in a similar way.

Both the linear congruence and the linear equation have direct applications to invariant theory, my motivation to consider them, see [7].

1 Indecomposable Solutions

For both problems (**E**) and (**A**) the solution set is the kernel of a homomorphism, hence a sub-semigroup $H \leq \mathbb{N}^n$ with the property

$$x, y \in H, \quad x - y \in \mathbb{N}^n \implies x - y \in H.$$

The semigroup \mathbb{N}^n has the (partial) order $x \leq y \iff x - y \in \mathbb{N}^n$. Consider the set B of minimal elements > 0 of H . From Dickson's lemma [1] we get that B is finite, consists of the indecomposable elements of H , and generates H . Therefore H has a canonical minimal system of generators that is finite.

Thus solving the linear equation (**E**) or the linear congruence (**A**) boils down to determining the indecomposable solutions. Meaningful partial tasks are:

- (I) *Find bounds for the coordinates of the indecomposable solutions that are as strong as possible.*
- (II) *Find algorithms that construct all indecomposable solutions, and analyze their efficiency.*
- (III) *Determine the number of indecomposable solutions, at least give good estimates of this number.*

We expect an exponential dependency of the number of indecomposable solutions from the relevant parameters such as the number of variables or the size of the coefficients. In particular an algorithm as in (II) must have exponential complexity and cannot be efficient in the proper sense.

The case $n = 1$ of the linear congruence (**A**) is trivial. Here is the result:

Proposition 1 *Let $m \in \mathbb{N}_2$ and $a \in \mathbb{N}_1$. Then the only indecomposable solution of the congruence $ax \equiv 0 \pmod{m}$ is the minimal integer $x > 0$ with $m|ax$. If m and a are coprime, $x = m$.*

The results for the case $n = 2$ are considerably more complex but known, see [12].

2 A Naive Algorithm

Let $n \in \mathbb{N}_1$, $a = (a_1, \dots, a_n) \in \mathbb{N}^n$. An obvious algorithm for finding the indecomposable solutions $x \in \mathbb{N}^n$ of the linear congruence **(A)** works as follows:

1. Given a finite subset $\mathcal{D} \subseteq \mathbb{N}^n$ that is guaranteed to contain all indecomposable solutions, enumerate all vectors > 0 in \mathcal{D} .
2. Test each vector whether it satisfies **(A)** to get the list of all solutions > 0 in \mathcal{D} .
3. Eliminate all vectors from the list that are not minimal.

Since subtracting m from a coordinate $> m$ of a solution yields another solution, indecomposable solutions have all their coordinates $\leq m$. Thus the first natural candidate for \mathcal{D} is the “hypercube”

$$\mathcal{D}_0 = \{0, \dots, m\}^n.$$

The following theorem (from [13]) gives a bound on the set of indecomposable solutions of **(A)** that improves the trivial bound $x_i \leq m$ (and thereby reduces the search space from a hypercube to a simplex, or the bound for the maximum norm $\|\bullet\|_\infty$ to a bound for the sum norm $\|\bullet\|_1$).

Theorem 1 (TINSLEY) *Let $x \in \mathbb{N}^n$ be an indecomposable solution of **(A)**. Then*

$$x_1 + \dots + x_n \leq m.$$

Proof. Let x be a solution of **(A)** with $x_1 + \dots + x_n \geq m + 1$. *Claim:* x is decomposable.

There is a $u \in \mathbb{N}^n$ with $0 \leq u_i \leq x_i$ and $u_1 + \dots + u_n = m$. Let $e_1 = (1, 0, \dots, 0), \dots, e_n$ be the canonical unit vectors. The elements of the linearly ordered set M consisting of

$$0, e_1, \dots, u_1 e_1, u_1 e_1 + e_2, \dots, u_1 e_1 + u_2 e_2,$$

$$\dots, u_1e_1 + \dots + u_n e_n = u$$

are different in \mathbb{N}^n . Since their number is $m + 1$ we find two of them that map to the same residue class mod m under the homomorphism

$$h: \mathbb{Z}^n \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad x \mapsto a_1x_1 + \dots + a_nx_n \pmod{m}.$$

Their difference in any order is in the kernel of h , and one of the two differences, v , is positive since M is linearly ordered. This v yields a solution of **(A)** with $0 < v < x$. \diamond

Remark 1 In an analogous way we get: Let $\Omega \subseteq \mathbb{Z}^n$ be a lattice of index $\leq m$. Let $Q = [0, r] \subseteq \mathbb{R}^n$ be a closed rectangular parallelepiped with $r_1, \dots, r_n \in \mathbb{N}$, $r_1 + \dots + r_n = m$. Then Q contains a lattice point $\neq 0$ of Ω . To apply the reasoning of Theorem 1 observe that Ω is the kernel of the natural homomorphism

$$h: \mathbb{Z}^n \longrightarrow \mathbb{Z}^n/\Omega \quad \text{where } \#(\mathbb{Z}^n/\Omega) \leq m.$$

Remark 2 There is another simple but less elementary proof of Theorem 1: The indecomposable solutions x of **(A)** are the exponents of a minimal generating system of the invariants of the cyclic group of order m operating on the polynomial algebra $\mathbb{C}[T_1, \dots, T_n]$ by $T_j \mapsto \varepsilon^{a_j} T_j$ where $\varepsilon = e^{2\pi i/m}$ is a primitive m -th root of unity. Noether's bound for the invariants of finite groups [8] implies $x_1 + \dots + x_n \leq m$.

Let $N_m(a)$ be the number of indecomposable solutions of **(A)** for $a \in \mathbb{N}^n$. The trivial bound $x_i \leq m$ for indecomposable solutions bounds their number by the cardinality of $\mathcal{D}_0 = \{0, \dots, m\}^n$, that is by $(m + 1)^n$.

The theorem improves this bound to the number $\binom{n+m}{m}$ of integer points in the simplex

$$\mathcal{D}_1 = \{x \in \mathbb{R}^n \mid x \geq 0, \|x\|_1 \leq m\}.$$

Note that this bound, although considerably smaller, asymptotically doesn't behave much better than m^n . There is a marginally tighter bound:

Corollary 1 *The number of indecomposable solutions of **(A)** is bounded by*

$$N_m(a) \leq \binom{n+m-1}{m}.$$

For certain choices of a this bound is attained.

Proof. For given x_1, \dots, x_{n-1} there is at most one x_n such that $(x_1, \dots, x_{n-1}, x_n)$ is an indecomposable solution of (\mathbf{A}) , and then necessarily $x_1 + \dots + x_{n-1} \leq m$ by the theorem. Thus the number of indecomposable solutions is limited by the number of choices for x_1, \dots, x_{n-1} with $x_1 + \dots + x_{n-1} \leq m$, that is $\binom{n+m-1}{m}$.

The bound $\binom{n+m-1}{m}$ for $N(a)$ is attained if $a_1 = \dots = a_n = 1$: Since $x_1 + \dots + x_n \equiv 0 \pmod{m}$ and $x_1 + \dots + x_n \leq m$ imply $x_1 + \dots + x_n = m$, in this case we count the partitions of m into n parts. \diamond

3 Reduction to Normal Form

Consider the congruence (\mathbf{A}) . For $r = 0, \dots, m-1$ let

$$I_r := \{i = 1, \dots, n \mid a_i \equiv r \pmod{m}\}$$

be the set of all indices where the coefficient is congruent to r . Hence

$$\{1, \dots, n\} = I_0 \cup \dots \cup I_{m-1}.$$

Note that some of the sets I_r may be empty.

First Reduction

Every solution $x \in \mathbb{N}^n$ directly decomposes into two parts:

$$(x_i)_{i \in I_0} \in \mathbb{N}^{\#I_0} \quad \text{arbitrary,}$$

and a solution of the remaining congruence

$$\sum_{i \in I_1 \cup \dots \cup I_{m-1}} a_i x_i \equiv 0 \pmod{m}.$$

Therefore without loss of generality we may assume that all coefficients a_i are non-zero.

Second Reduction

Let \mathcal{L}'_m be the set of indecomposable solutions $y = (y_0, \dots, y_{m-1}) \in \mathbb{N}^m$ of the special congruence

$$(\mathbf{C}'_m) \quad 0 \cdot y_0 + 1 \cdot y_1 + \dots + (m-1) \cdot y_{m-1} \equiv 0 \pmod{m}.$$

For each $y \in \mathcal{L}'_m$ choose arbitrary $x_1, \dots, x_n \in \mathbb{N}$ with

$$\sum_{i \in I_r} x_i = y_r \quad \text{for } r = 0, \dots, m-1.$$

Clearly then $x \in \mathbb{N}^n - 0$ is minimal among the solutions of **(A)**, and each minimal solution x is obtained this way. Therefore without loss of generality we (often) may assume that all coefficients a_i are different.

In summary the congruence **(A)** is reduced to the special case where all coefficients a_i are different and non-zero.

Applying the first reduction to **(C'_m)** we conclude that each $y \in \mathcal{L}'_m$ has one of the forms

- $y_0 = 1, y_1 = \dots = y_{m-1} = 0,$
- $y_0 = 0,$ and $(y_1, \dots, y_{m-1}) \in \mathbb{N}^{m-1}$ an indecomposable solution of the congruence

$$(\mathbf{C}_m) \quad 1 \cdot y_1 + \dots + (m-1) \cdot y_{m-1} \equiv 0 \pmod{m}.$$

Normal Forms

For the general case of **(A)** consider the set J of indices $r > 0$ where $I_r \neq \emptyset$. Then solving **(A)** is reduced to the congruence

$$(\mathbf{C}_m(J)) \quad \sum_{r \in J} r \cdot y_r \equiv 0 \pmod{m}.$$

Call the congruences **(C_m(J))** for all subsets $J \subseteq \{1, \dots, m-1\}$ the **normal forms** of linear congruences. Let $\mathcal{L}_m(J)$ be the set of indecomposable solutions of **(C_m(J))**. Then we have shown:

Proposition 2 *All indecomposable solutions x of **(A)** arise in one of the two following ways:*

- (i) *For $i \in I_0$ set $x_i = 1$, and $x_j = 0$ for $j \neq i$.*
- (ii) *For each $y = (y_r)_{r \in J} \in \mathcal{L}_m(J)$ choose $x_i \in \mathbb{N}$ for $i \in I_1 \cup \dots \cup I_{m-1}$ with*

$$\sum_{i \in I_r} x_i = y_r \quad \text{for } r = 1, \dots, m-1.$$

Proposition 2 implies a formula for the number of indecomposable solutions.

Corollary 1 Let $N_m(a)$ be the number of indecomposable solutions of (\mathbf{A}) for $a \in \mathbb{N}^n$. Then

$$N_m(a) = n_0 + \sum_{y \in \mathcal{L}_m(J)} \left(\prod_{r=1}^{m-1} \binom{n_r + y_r - 1}{y_r} \right)$$

with $n_r = \#I_r$.

Proof. There are $\binom{n_r + y_r - 1}{y_r}$ possibilities for splitting y_r into x_i with $\sum_{i \in I_r} x_i = y_r$. \diamond

However the use of this formula to estimate the number of indecomposable solutions is rather limited since it presupposes knowledge of all the indecomposable solutions of $(\mathbf{C}_m(J))$.

Problem Find methods for estimating the number of indecomposable solutions for the general case (\mathbf{A}) that use at most analogous estimates for $(\mathbf{C}_m(J))$ but not explicit knowledge of the solutions.

The Standard Linear Congruence

For a subset $J \subseteq \{1, \dots, m-1\}$ consider the embedding

$$\tau : \mathbb{N}^J \longrightarrow \mathbb{N}^{m-1}, \quad (x_j)_{j \in J} \mapsto \bar{x},$$

that consists of filling up the positions different from J with zeros, that is

$$\bar{x} = (\bar{x}_1, \dots, \bar{x}_{m-1}) \quad \text{where } \bar{x}_i = \begin{cases} x_i & \text{for } i \in J, \\ 0 & \text{otherwise.} \end{cases}$$

Then clearly x is a solution of $(\mathbf{C}_m(J))$ if and only if $\tau(x)$ is a solution of (\mathbf{C}_m) , and x is an indecomposable solution of $(\mathbf{C}_m(J))$ if and only if $\tau(x)$ is an indecomposable solution of (\mathbf{C}_m) . Therefore the following procedure gives all indecomposable solutions of $(\mathbf{C}_m(J))$ under the assumption that the complete set M of indecomposable solutions of (\mathbf{C}_m) is known:

- Remove the vectors from M that have at least one non-zero entry at an index not belonging to J .
- From the remaining vectors remove the (zero) components for indices not belonging to J .

This reduces the search for the indecomposable solutions of **(A)** to the special case **(C_m)**, and justifies calling **(C_m)** **the standard linear congruence** for the module m .

From a theoretical standpoint the breakdown of the general case of **(A)** to an instance of a well-arranged set of standard cases **(C_m)** might seem interesting. But note that this reduction doesn't make it easy to find all indecomposable solutions nor does it help with counting them.

4 The Support of an Indecomposable Solution

For a vector $x \in \mathbb{N}^n$ let

$$\text{supp}(x) := \{i = 1, \dots, n \mid x_i \neq 0\},$$

be its support and

$$\sigma(x) := \#\text{supp}(x)$$

the cardinality of its support, called the **width** of x . Moreover we call

- $\|x\|_1 = x_1 + \dots + x_n$ the **length** (sometimes also called the degree [6]),
- $\|x\|_\infty = \max\{x_1, \dots, x_n\}$ the **height**,
- $\|x\|_1 + \sigma(x)$ the **total size** (= length + width),
- $\alpha(x) := x_1 + \dots + n \cdot x_n$ the **weight**

of x . Clearly in \mathbb{N}

$$\sigma(x) = \sum_{x_i \neq 0} 1 \leq \sum_{x_i \neq 0} x_i = \|x\|_1 \leq \sum_{x_i \neq 0} i \cdot x_i = \alpha(x).$$

We consider the standard linear congruence

$$(\mathbf{C}_m) \quad x_1 + \dots + (m-1) \cdot x_{m-1} \equiv 0 \pmod{m}$$

By Theorem 1 each of its indecomposable solutions $x \in \mathbb{N}^{m-1}$ is contained in the simplex \mathcal{D}_1 : $x_1 + \dots + x_{m-1} \leq m$. Here we derive a stronger restriction. We start with a lemma.

Lemma 1 *Let r and m be natural numbers with $2r \leq m$. Let $t_1, \dots, t_r \in \{1, \dots, m-1\}$ be r distinct numbers. For any subset $I \subseteq \{1, \dots, r\}$ let*

$$S_I := \sum_{i \in I} t_i.$$

Assume that no sum S_I , $I \neq \emptyset$, is divisible by m . (Note that $S_\emptyset = 0$.)

Then the 2^r sums S_I represent at least $2r$ distinct classes mod m .

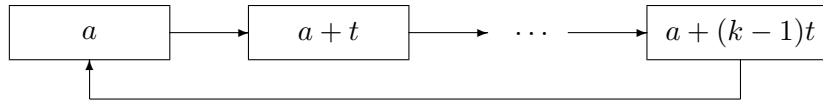
Proof. Induction on r . For $r = 1$ we have two sums, 0 and t_1 , that represent two different residue classes mod m .

Now assume $r \geq 2$. Let $N = 2r - 2$. By induction the sums S_I where $I \subseteq \{1, \dots, r - 1\}$ represent at least N different residue classes mod m . Adding t_r to each of these sums yields another set of at least N different residue classes. These two sets of residue classes might overlap, however the second set contains at least one new class, that of $t_1 + \dots + t_r$.

Otherwise $t_1 + \dots + t_r \equiv S_I \pmod{m}$ for some subset $I \subseteq \{1, \dots, r - 1\}$, but then $S_J \equiv 0 \pmod{m}$ for the complementary subset $J = \{1, \dots, r\} - I$, contradiction.

Thus the S_I represent at least $N + 1$ different residue classes. Assume there are no further ones. Then the S_I with $r \notin I$ represent exactly N classes $0, a_1, \dots, a_{N-1}$. Let $A = \{a_1, \dots, a_{N-1}\}$. The S_I with $r \in I$ represent residue classes already contained in A except the new class $t_1 + \dots + t_r \pmod{m}$.

The cyclic group $\mathbb{Z}/m\mathbb{Z}$ acts on itself by translation. The translation by $t = t_r$ has exactly $e = \gcd(m, t)$ orbits of length $k = m/e$ that look like this:



For $j \in \{1, \dots, N - 1\}$ there are two possibilities: Either $(a_j + t) \pmod{m}$ is in A , or $a_j + t \equiv t_1 + \dots + t_r \pmod{m}$. Thus under translation with t the set A has exactly one exit, $t_1 + \dots + t_{r-1} \rightarrow t_1 + \dots + t_r$.

The orbit of 0 is $\{0, t, \dots, (k - 1)t\}$. It starts at 0, outside of A . Since $t = t_r \in A$ the orbit meets A in a segment $t, \dots, (p - 1)t$ with $p \leq k - 1$ and then leaves A . The only possible exit is $pt \equiv t_1 + \dots + t_r \pmod{m}$. After this point the orbit never meets A again because this would require another exit.

Besides there may exist some, say q , orbits completely contained in A , and these have the form $\{a_j, a_j + t, \dots, a_j + (k - 1)t\}$. We conclude that

$$N = \#A + 1 = qk + p,$$

and, using $kt \equiv 0 \pmod{m}$,

$$t_1 + \dots + t_r \equiv pt \equiv qkt + pt = Nt \pmod{m}.$$

The indexing of the t_i does not matter, we may go through the same reasoning with any t_i instead of t_r . If for some t_i we find at least $N + 2$ different residue classes, we are done. Otherwise we conclude as for t_r :

$$t_1 + \cdots + t_r \equiv Nt_i \pmod{m} \quad \text{for all } i = 1, \dots, r.$$

Now let $d = \gcd(N, m)$, and let $i, j \in \{1, \dots, r\}$ with $i \neq j$. Then $N \cdot (t_i - t_j) \equiv 0 \pmod{m}$, whence $t_i \equiv t_j \pmod{m/d}$. Each class mod m/d consists of d classes mod m . Thus, if $r > d$, then two of the t_i must agree even mod m , contradiction.

What if $d \geq r$? Since $d|N$ and $d > N/2 = r - 1$, necessarily $d = N$, whence $N|m$. Let $m = cN$, $m/d = m/N = c$, hence $t_i \equiv t_j \pmod{c}$ for all i and j . Thus there is an $a \in \{0, \dots, c - 1\}$ and r different numbers $s_1, \dots, s_r \in \{0, \dots, N - 1\}$ such that $t_i = a + cs_i$ for $i = 1, \dots, r$. Assume $a = 0$. Then all $t_i = cs_i$,

$$t_1 + \cdots + t_r \equiv Nt_i = Ncs_i = ms_i \equiv 0 \pmod{m},$$

contradiction. Therefore $a \neq 0$. But then $a \not\equiv 2a \pmod{c}$, and

$$t_i + t_j \equiv 2a \not\equiv a \equiv t_k \pmod{c},$$

and a fortiori $t_i + t_j \not\equiv t_k \pmod{m}$, for different indices i and j , and any k . Thus the following numbers represent $2r$ different residue classes mod m :

- (1) the empty sum 0,
- (2) t_1, \dots, t_r ,
- (3) the $r - 1$ sums $t_1 + t_j$, $j = 2, \dots, r$. \diamond

We'll prove that the larger the width of an indecomposable solution $x \in \mathbb{N}^{m-1}$ of (\mathbf{C}_m) the tighter bounded is its length:

Lemma 2 *Let x be an indecomposable solution of (\mathbf{C}_m) , and let $s \in \mathbb{N}$. Assume the width of x is $\sigma(x) \geq s$. Then:*

- (i) $\|x\|_1 \leq m - s + 1$.
- (ii) $\|x\|_1 = m - s + 1$ can occur only for $\sigma(x) = s$.
- (iii) $2s \leq m + 1$; even $2s \leq m$ except in the case $m = 3$ and $x = (1, 1)$.
- (iv) If $\|x\|_1 = m - s + 1$, then at most one coordinate $x_j \geq 2$.

Proof. We prove (i) and (ii) together by induction over s . For $s = 0$ we have $\|x\|_1 < m + 1 = m - s + 1$. Now assume $s \geq 1$.

(i) Since a fortiori $\sigma(x) \geq s - 1$, we already have $\|x\|_1 \leq m - s + 2$ by induction from (i) for $s - 1$. The assumption $\|x\|_1 = m - s + 2$ yields the contradiction $\sigma(x) = s - 1$ by induction from (ii) for $s - 1$. Hence $\|x\|_1 \leq m - s + 1$.

(ii) Let $\|x\|_1 = m - s + 1$, and assume that $\sigma(x) \geq s + 1$. Then a fortiori

$$s + 1 \leq \sigma(x) \leq \|x\|_1 = m - s + 1$$

hence $2s \leq m$.

Consider an $(s + 1)$ -element subset $\{i_0, \dots, i_s\} \subseteq \text{supp}(x)$, and let $y := e_{i_0} + \dots + e_{i_s}$, where we use the notation e_i for the canonical unit vectors. We consider an ascending chain

$$(1) \quad 0 < u^{(1)} < \dots < u^{(s)} < u^{(s+1)} = y < \dots < u^{(m-s+1)} = x$$

where $\|u^{(\nu)}\|_1 = \nu$ for $1 \leq \nu \leq m - s + 1$. In particular for $1 \leq \nu \leq s + 1$ each $u^{(\nu)}$ results from $u^{(\nu-1)}$ by adding a single canonical unit vector.

The $\alpha(u^{(\nu)})$ for $1 \leq \nu \leq m - s + 1$ are pairwise incongruent mod m for otherwise one of the differences $u^{(\mu)} - u^{(\nu)}$ would yield a solution $< x$ of (\mathbf{C}_m) .

Now we fix the chain between y and x . Then the $\alpha(u^{(\nu)})$ for $s + 2 \leq \nu \leq m - s + 1$ represent exactly $m - 2s$ different residue classes. This leaves exactly $2s$ different possible values of $\alpha(u)$ mod m for $0 \leq u \leq y$.

Since $\alpha(e_i) = i$, the $s + 1$ values $t_0 = \alpha(e_{i_0}), \dots, t_s = \alpha(e_{i_s})$ are different. Lemma 1 implies that the $\alpha(u)$ for $0 \leq u \leq y$ take at least $2s + 2$ different values. Hence at least one of these values $\alpha(u)$ must occur among the $\alpha(u^{(\nu)})$ for $s + 2 \leq \nu \leq m - s + 1$. Constructing the chain in such a way that it contains this vector u the chain yields the same value for α mod m at two different positions, contradiction.

Hence $\sigma(x) = s$.

(iii) By (i) we have $s \leq \sigma(x) \leq \|x\|_1 \leq m - s + 1$, hence $2s \leq m + 1$.

If $2s = m + 1$, then m is odd, $s = m - s + 1$, and thus $s = \sigma(x) = \|x\|_1 = m - s + 1$. There are $s - 1$ pairs $(i, m - i)$ of indices with $1 \leq i \leq \frac{m-1}{2} = s - 1$. Hence $i, m - i \in \text{supp}(x)$ for at least one i . Then $y = e_i + e_{m-i}$ is a solution $\leq x$ of (\mathbf{C}_m) since $\alpha(e_i + e_{m-i}) = i + m - i = m$. Hence $y = x$, $\text{supp}(x) = \{i, m - i\}$, $s = 2$, $m = 3$, $x = (1, 1)$.

(iv) The statement is trivial for $m = 2$. For $m = 3$ it follows directly from the explicit enumeration of all indecomposable solutions: $(3, 0), (1, 1), (0, 3)$.

So let $m \geq 4$. Then $2s \leq m$ by (iii), and $\sigma(x) = s$ by (ii). Let

$$y = \sum_{i \in \text{supp}(x)} e_i.$$

If $x = y$ we are done. Otherwise by Lemma 1 the 2^s values $\alpha(u)$ for $0 \leq u \leq y$ represent at least $2s$ different residue classes mod m . In each chain

$$0 < u^{(1)} < \dots < u^{(s)} = y < u^{(s+1)} < \dots < u^{(m-s+1)} = x$$

there remain only $m - 2s$ possible values $\alpha(u^{(j)})$ for the $m - 2s$ indices j with $s + 1 \leq j < m - s + 1$. So if we exchange a single element of the chain between y and x , the α -values of the old and of the new element must coincide.

Now assume $x_i \geq 2$ and $x_j \geq 2$ with $i \neq j$. Then $y + e_i + e_j \leq x$, and for the intermediate step between y and $y + e_i + e_j$ we have the two choices $y + e_i$ and $y + e_j$. Hence $\alpha(y + e_i) \equiv \alpha(y + e_j)$. This implies $i = \alpha(e_i) \equiv \alpha(e_j) = j$, whence $i = j$. \diamond

Here is a concise reformulation of the essential statements of Lemma 2:

Theorem 2 *Let $m \in \mathbb{N}_4$, and let x be an indecomposable solution of the standard linear congruence (\mathbf{C}_m) . Then:*

- (i) *The width of x is bounded by $\sigma(x) \leq \frac{m}{2}$.*
- (ii) *The total size of x is bounded by $\|x\|_1 + \sigma(x) \leq m + 1$, and in the case of equality at most one coordinate $x_j \geq 2$.*

A transfer of this result to the general congruence (\mathbf{A}) results in a somewhat clumsy formulation. We should collect together indices where the coefficients a_i are identical mod m . Therefore we replace the support by the set

$$\begin{aligned} \text{supp}'(x) &:= \{a_i \bmod m \mid i = 1, \dots, n, x_i \neq 0\} \\ &= \{j \mid 1 \leq j \leq n \text{ and } a_i = j \text{ and } x_i \neq 0 \text{ for some } i\}. \end{aligned}$$

Note that this is defined as a set of coefficients of (\mathbf{A}) , not as a set of indices in \mathbb{N}^n , and repeated coefficients are counted only once. Furthermore let

$$\sigma'(x) := \# \text{supp}'(x).$$

In the special case (\mathbf{C}_m) of (\mathbf{A}) we have $\text{supp}' = \text{supp}$ and $\sigma' = \sigma$. Then our result reads:

Table 1: Numbers of indecomposable solutions and their logarithms

m	2	3	4	5	6	7	8	9	10	11	12
$\ell(m)$	1	3	6	14	19	47	64	118	165	347	366
$\log_2 \ell(m)$	0	1.5	2.6	3.8	4.2	5.6	6.0	6.9	7.4	8.4	8.5
m	13	14	15	16	17	18	19	20	21	22	23
$\ell(m)$	826	973	1493	2134	3912	4037	7935	8246	12966	17475	29161
$\log_2 \ell(m)$	9.7	9.9	10.5	11.1	11.9	12.0	13.0	13.0	13.7	14.1	14.8

Corollary 1 *Let $m \in \mathbb{N}_4$ and $a = (a_1, \dots, a_n) \in \mathbb{N}^n$. Let $x \in \mathbb{N}^n$ be an indecomposable solution of the linear congruence (\mathbf{A}) . Then:*

- (i) $\sigma'(x) \leq \frac{m}{2}$.
- (ii) $\|x\|_1 + \sigma'(x) \leq m + 1$.

Theorem 2 leads to a significant speedup of the algorithm from Section 2. We won't pursue this aspect since [11] has a quite fast algorithm.

5 An Upper Bound for the Number of Indecomposable Solutions

Let $\ell(m)$ be the number of indecomposable solutions of the standard linear congruence (\mathbf{C}_m) . From the On-line Encyclopedia of Integer Sequences [9] we have the explicit values for small m , see Table 1. The corresponding logarithmic plot (base 2) in Figure 1 lets us hope for a slightly sublinear growth, or a slightly subexponential growth of ℓ itself. Since [2] gives a lower bound we'll look for an upper bound only.

By the corollary of Theorem 1 we have $\ell(m) \leq \binom{2m-2}{m}$. By Theorem 2 we even have $x_1 + \dots + x_{m-1} \leq m - 1$ for indecomposable solutions x with at least two-element support, that is for all indecomposable solutions except the $x = me_j$ with indices j that are coprime with m . Counting the unit vectors e_j instead of these, we get the somewhat stronger bound $\ell(m) \leq \binom{2m-3}{m-1}$ —the e_j are not solutions but satisfy the stronger bound $\|x\|_1 \leq m - 1$.

By standard methods we easily derive an upper bound for the growth of $\ell(m)$: We use a corollary of Stirling's formula, see [10]:

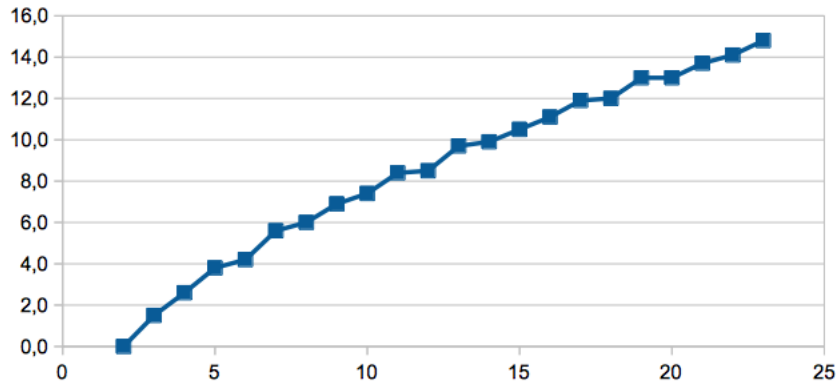


Figure 1: 2-logarithm of the number of indecomposable solutions

Lemma 3

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{4^n}{\sqrt{\pi n}} \cdot E_n,$$

where the error term E_n is bounded by

$$e^{-\frac{1}{6n}} < E_n < 1.$$

Since $\ell(m) \leq \binom{2m-3}{m-1} = \frac{(2m-3) \cdots (m-1)}{1 \cdots (m-1)} = \frac{1}{2} \binom{2m-2}{m-1}$ we have shown:

Proposition 3 For $m \geq 2$ the number $\ell(m)$ of indecomposable solutions of (\mathbf{C}_m) satisfies

$$\ell(m) < \frac{1}{2\sqrt{\pi}} \cdot \frac{1}{\sqrt{m-1}} \cdot 4^{m-1}.$$

This is at most a slightly subexponential growth. We expect Theorem 2 to yield a sharper bound, however without improving the asymptotical behaviour in an essential way. To apply it we assume $m \geq 4$. Then the support of an indecomposable solution has at most $\lfloor \frac{m}{2} \rfloor$ elements. For each $s \in \{1, \dots, \lfloor \frac{m}{2} \rfloor\}$ we have exactly $\binom{m-1}{s}$ choices for an s -element subset $S = \{i_1, \dots, i_s\} \subseteq \{1, \dots, m-1\}$ that serves as support. Such a set S might support three types of indecomposable solutions x :

Type 0: Call a solution **flat** if all of its non-zero coordinates are 1. If S supports a flat solution, then no superset of S can support an indecomposable solution.

Type I: $\|x\|_1 = m - s + 1$. Then $x_i = 1$ for all $i \in S$ except one, say x_{i_ν} , and necessarily $x_{i_\nu} = (m - s + 1) - (s - 1) = m - 2s + 2$. Thus there are at most s indecomposable solutions of this type.

Type II: $\|x\|_1 \leq m - s$. If we choose arbitrary $x_{i_1}, \dots, x_{i_{s-1}}$, then there is at most one x_{i_s} that complements them for an indecomposable solution. Therefore we catch all indecomposable solutions on S with $\|x\|_1 \leq m - s$ by choosing arbitrary $y_1, \dots, y_{s-1} \geq 0$ with $y_1 + \dots + y_{s-1} \leq m - 2s$, defining $x_{i_\nu} = y_\nu + 1$, and choosing x_{i_s} appropriately, that is, minimal such that $m \mid \alpha(x)$.

Lemma 4 *Let $m \in \mathbb{N}_4$, and let $s \in \mathbb{N}_1$, $s \leq \frac{m}{2}$. Let $S = \{i_1, \dots, i_s\} \subseteq \{1, \dots, m - 1\}$ be an s -element subset. Then S supports at most $\binom{m-s-1}{s-1}$ indecomposable solutions of (\mathbf{C}_m) .*

Proof. The assertion is true for $s = 1$, since $\binom{m-2}{0} = 1$. The assertion is also true if S supports a flat solution since this, if indecomposable, is the only one.

Thus we may assume that $s \geq 2$ and that S doesn't support a flat solution. Hence all indecomposable solutions are of type I or type II.

Each solution of type II is characterized by a choice of $y_1, \dots, y_{s-1} \in \mathbb{N}$ with $y_1 + \dots + y_{s-1} \leq m - 2s$. The number of such choices is $\binom{m-2s+s-1}{s-1} = \binom{m-s-1}{s-1}$.

But we also have up to s indecomposable solutions of type I supported by S . To complete the proof we have to find a "gap" in our type-II-count for each of them. We consider the s vectors $z^{(\nu)} = (z_1^{(\nu)}, \dots, z_{m-1}^{(\nu)})$ for $\nu = 1, \dots, s$ with

$$z_i^{(\nu)} = \begin{cases} m - 2s + 2 & \text{for } i = i_\nu, \\ 1 & \text{for } i \in S \text{ otherwise,} \\ 0 & \text{for } i \notin S. \end{cases}$$

In the case $\nu = s$ we consider $y_1 = \dots = y_{s-1} = 0$, or equivalently $x_{i_1} = \dots = x_{i_{s-1}} = 1$, and find that for each of the (at least one) values $1, \dots, m - 2s + 1$ for x_{i_s} we have $x < z^{(\nu)}$. Hence if $z^{(\nu)}$ is an indecomposable solution, x is not a solution at all.

In the cases $1 \leq \nu \leq s - 1$ the choice $y_\nu = m - 2s$, $y_\mu = 0$ otherwise, or equivalently $x_{i_\nu} = m - 2s + 1$, $x_{i_\mu} = 1$ otherwise for $\mu = 1, \dots, s - 1$, admits only the choice $x_{i_s} = 1$ in the domain $\|x\|_1 \leq m - s$. Here again $x < z^{(\nu)}$, hence at most one of the two can be an indecomposable solution. \diamond

Table 2: Comparing $\ell(m)$ with bounds and possible bounds

m	4	5	6	7	8	9	10	11	12	13
$\ell(m)$	6	14	19	47	64	118	165	347	366	826
$m \cdot P(m)$	20	35	66	105	176	270	420	616	924	1313
$q(m)$	6	16	45	126	357	1016	2907	8350	24068	69576
$r(m)$	10	36	129	471	1746	6536	24649	93539	356745	[...]
m	14	15	16	17	18	19	20	21	22	23
$\ell(m)$	973	1493	2134	3912	4037	7935	8246	12966	17475	29161
$m \cdot P(m)$	1890	2640	3696	5049	6930	9310	12540	16632	22044	28865
$q(m)$	201643	[...]								

We resume:

Theorem 3 *The number $\ell(m)$ of indecomposable solutions of (\mathbf{C}_m) , $m \geq 4$, satisfies*

$$\ell(m) \leq \sum_{s=1}^{\lfloor \frac{m}{2} \rfloor} \binom{m-1}{s} \cdot \binom{m-s-1}{s-1}.$$

Table 2 shows some explicit values where $q(m)$ is the bound from Theorem 3, $r(m)$, the bound from Proposition 3, and P , the partition function.

Problems The bounds $r(m)$ and $q(m)$ are quite coarse.

- Is $\ell(m) \leq a \cdot e^{b\sqrt{m}}$ for certain constants a und b ?
- Is $\ell(m) \leq cm \cdot P(m)$ for $m \geq 2$ for some constant c ? (Note that this would imply the previous inequality. Unfortunately $\ell(23) > 23 \cdot P(23)$, thus $c > 1$ if it exists at all.)
- On the other hand $q(m)$ seems to grow much too fast, and $r(m)$ much much too fast.

References

- [1] L. E. Dickson: Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. Amer. J. Math. 35 (1913), 413–422.

- [2] J. Dixmier, P. Erdős, J.-L. Nicolas: Sur le nombre d'invariants fondamentaux des formes binaires. *C. R. Acad. Sc. Paris Série I* 305 (1987), 319–322.
- [3] A. Elashvili, M. Jibladze: Hermite reciprocity for the regular representations of cyclic groups. *Indag. Math.* 9 (1998), 233–238.
- [4] M. Filgueiras, A. P. Tomás: A fast method for finding the basis of non-negative solutions to a linear Diophantine equation. *J. Symbolic Comput.* 19 (1995), 507–526.
- [5] B. M. Finklea, T. Moore, V. Ponomarenko, Z. J. Turner: Invariant polynomials and minimal zero sequences. *Involve* 1 (2008), 159–165.
- [6] J. C. Harris, D. L. Wehlau: Non-negative integer linear congruences. *Indag. Math.* 17 (2006), 37–44.
- [7] V. G. Kac: Root systems, representations of quivers and invariant theory. *Invariant Theory*, Montecatini 1982, ed. by F. Gherardelli. Springer Lect. Notes 996 (1983).
- [8] E. Noether: Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* 77 (1916), 89–92.
- [9] The On-line Encyclopedia of Integer Sequences. Online: <http://oeis.org/>
- [10] K. Pommerening: Stirling's formula. Online: <http://www.staff.uni-mainz.de/pommeren/MathMisc/Stirling.pdf>
- [11] V. Ponomarenko: MZS. Online: <http://vadim.sdsu.edu/mzs.zip>
- [12] M. F. Tinsley: Permanents of cyclic matrices. *Pacific J. Math.* 10 (1960), 1067–1082.
- [13] M. F. Tinsley: A combinatorial theorem in number theory. *Duke Math. J.* 33 (1966), 75–79.