The Indecomposable Solutions of Linear Congruences

Klaus Pommerening
Johannes-Gutenberg-Universität
Mainz, Germany

October 1986 – extended English version August 2016
last change: August 12, 2018

Abstract The linear congruence $a_1x_1+\cdots+a_nx_n \equiv 0 \pmod m$ for non-negative integer unknowns $x_1, \ldots, x_n$ is easily reduced to the standard congruence
$(\mathbf{C}_m) \quad 1 \cdot x_1 + \cdots + (m-1) \cdot x_{m-1} \equiv 0 \pmod m$.

This survey article derives the Eggleton-Erdős bound for the indecomposable (= minimal non-zero) solutions of $(\mathbf{C}_m)$, characterizes the solutions among them that attain this bound, and derives upper and lower bounds for the number of indecomposable solutions.

Among the topics of additive number theory linear Diophantine problems play a prominent role. In particular getting an overview over all solutions in natural numbers turns out to be quite difficult.

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

Here is a sample of typical problems, for simplicity each one restricted to the case of a single equation or congruence:

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

$$a_1x_1 + \cdots + a_nx_n = 0. \tag{1}$$

The inhomogeneous equation: Given $a \in \mathbb{Z}^n$ and $q \in \mathbb{N}_1$, determine $x \in \mathbb{N}^n$ with

$$a_1x_1 + \cdots + a_nx_n = q. \tag{2}$$

A well-studied special case is $a \in \mathbb{N}^n$, that is the coefficients are ≥ 0 (or > 0).

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

$$a_1x_1 + \cdots + a_nx_n \equiv 0 \pmod m. \tag{3}$$

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

The existing literature has a lot of results on the inhomogeneous equation (2) in the special case of positive coefficients—good starting points are Chapter 3 of [1], furthermore [24], [7], [8]. Here are some typical questions: For which q do solutions exist (the stamp or coin problem), and what is the number of solutions (analysis of the counting function)? Especially well-known is the case $a_1 = 1, \ldots, a_n = n$, where the solutions x exactly correspond to the partitions of q into parts $\leq n$.

In general, for the homogeneous or inhomogeneous problems, it's trivial to find lots of single solutions, and there are several algorithms that produce all indecomposable solutions, see [11] for the equation (1) or (2), and [32] for the congruence (3). But it seems difficult to get an overview over the complete solution set, in particular estimates for the numbers of indecomposable solutions. The reason might be that even simple examples show a confused image and evident general principles are hardly discernible. The OEIS [23] has the sequence `A096337` that indicates the numbers of indecomposable solutions of what we call the standard linear congruence ($\mathbf{C}_m$) below, for $m \leq 38$. In [12] these numbers (+1) are even stated for m upto 60. The paper [5] gives a weak asymptotic lower bound. Most results are found by more or less tricky applications of elementary methods.

This article derives some results on the linear congruence, in particular algorithms for finding all indecomposable solutions, geometric bounds for their coordinates, and bounds for their number. A following one [30] treats the linear equation. Since the bounds are far from optimal I ask some questions whose further pursuit seems promising.

Both the linear congruence and the linear equation have direct applications to invariant theory, my motivation to consider them, see [31]. Another application domain is the theory of zero-sum multisets, see [3, 13, 14, 38, 39], that is essentially another view at the same mathematical subject.

1 Indecomposable Solutions

Let us be more specific about the main tasks of this article. For both homogeneous problems (1) and (3) the solution set is a sub-monoid $H \leq \mathbb{N}^n$ with the property

$$x, y \in H,\ x - y \in \mathbb{N}^n \Longrightarrow x - y \in H,$$

that is a "full" sub-monoid in the sense of [18]. The monoid $\mathbb{N}^n$ has the (partial) order $x \leq y :\Longleftrightarrow x - y \in \mathbb{N}^n$. Consider the set B of minimal elements > 0 of H. From Dickson's lemma [25], see also [4] or [33, p. 52], we know that B is finite, consists of the indecomposable, or irreducible, elements of H, and generates H. Thus H has a canonical minimal system of generators that is finite.

> *Caution*: Not every sub-monoid of $\mathbb{N}^n$ is finitely generated. As an example take $H = \{(p, q) \mid q \geq 1\} \cup \{(0, 0)\}$.

Thus the main tasks for the linear equation (1) and the linear congruence (3) are: Determine the indecomposable solutions. Meaningful partial tasks are:

(I) *Find bounds for the coordinates of the indecomposable solutions that are as strong as possible.*

(II) *Identify and characterize indecomposable solutions with special properties.*

(III) *Find algorithms that construct all indecomposable solutions and analyze their efficiency.*

(IV) *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 on the relevant parameters such as the number of variables or the size of the coefficients. In particular an algorithm as in (III) must have exponential complexity and cannot be efficient in the proper sense of polynomial complexity.

The case $n = 1$ of the linear congruence (3) 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 next case to consider is $n = 2$. The results are known and resumed in a separate article, see [29].

2 A Naive Algorithm

Let $n \in \mathbb{N}_1$, $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$. We want to determine the indecomposable solutions $x \in \mathbb{N}^n$ of the linear congruence (formerly labeled by (3))

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

An obvious algorithm for finding them 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.

The number of integer points in $\mathcal{D}$ is a coarse upper bound, the number of special solutions as in (II), a coarse lower bound for the number of indecomposable solutions.

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"

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

The Python (or SageMath) function `dlist0()` from Appendix C.1 produces a list of all vectors in $\mathcal{D}_0$.

Another subroutine we need compares two vectors $\in \mathbb{N}^n$ with respect to the natural order

$$x = (x_1, \ldots, x_n) \leq y = (y_1, \ldots, y_n) \Longleftrightarrow x_i \leq y_i \text{ for all } i = 1, \ldots n.$$

This is implemented as the Python function `smaller()` given in Appendix C.1.

Then we need a subroutine that checks if a given integer vector satisfies a given linear congruence, and another one that reduces a list of vectors in $\mathbb{N}^n$ to its minimal elements with respect to the natural order, see the Python functions `chkcong()` given in Appendix C.2 and `minelts()` in Appendix C.1.

The Python program in Appendix C.3.1 then solves **(A)**. Here are the indecomposable solutions of some instances for small values of m.

- $m = 3$, $a = (1, 2)$:

  ```
  [0,3], [1,1], [3,0]
  ```

- $m = 4$, $a = (1, 2, 3)$:

  ```
  [0,0,4], [0,1,2], [0,2,0], [1,0,1], [2,1,0], [4,0,0]
  ```

- $m = 5$, $a = (1, 2, 3, 4)$:

  ```
  [0,0,0,5], [0,0,1,3], [0,0,2,1], [0,0,5,0], [0,1,0,2],
  [0,1,1,0], [0,3,0,1], [0,5,0,0], [1,0,0,1], [1,0,3,0],
  [1,2,0,0], [2,0,1,0], [3,1,0,0], [5,0,0,0]
  ```

- $m = 5$, $a = (1, 2, 4)$:

  ```
  [0,0,5], [0,1,2], [0,3,1], [0,5,0], [1,0,1], [1,2,0],
  [3,1,0], [5,0,0]
  ```

  Note that we get this list from the former example by omitting all vectors with third coordinate $\neq 0$, and deleting the third coordinate 0 from the remaining ones.

- $m = 6$, $a = (1, 2, 3, 4, 5)$:

  ```
  [0,0,0,0,6], [0,0,0,1,4], [0,0,0,2,2], [0,0,0,3,0],
  [0,0,1,0,3], [0,0,1,1,1], [0,0,2,0,0], [0,1,0,0,2],
  [0,1,0,1,0], [0,2,1,0,1], [0,3,0,0,0], [1,0,0,0,1],
  [1,0,1,2,0], [1,1,1,0,0], [2,0,0,1,0], [2,2,0,0,0],
  [3,0,1,0,0], [4,1,0,0,0], [6,0,0,0,0]
  ```

3 A Geometric Restriction for Indecomposable Solutions

The following theorem (that is also in [36]) 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 (NOETHER/TINSLEY) *Let $x \in \mathbb{N}^n$ be an indecomposable solution of* **(A)**. *Then*

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

Proof. Let x be a solution of **(A)** with $x_1 + \cdots + x_n \geq m + 1$. *Claim*: x is not minimal.

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

$$0,\ e_1,\ \ldots,\ u_1e_1,\ u_1e_1 + e_2,\ \ldots,\ u_1e_1 + u_2e_2,$$
$$\ldots,\ u_1e_1 + \cdots + u_ne_n = u$$

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

$$\alpha \colon \mathbb{Z}^n \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad x \mapsto a_1x_1 + \cdots + a_nx_n \bmod m.$$

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

Remark 1 In an analoguous 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 $r_1, \ldots, r_n \in \mathbb{N}$, $r_1 + \cdots + r_n = m$. 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

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

Remark 2 There is an older, 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 $\mathbb{C}[T_1, \ldots, T_n]$ 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, see for example [31], implies $x_1 + \cdots + x_n \leq m$. Therefore it seems adequate to call this bound also NOETHER's bound.

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 $\mathcal{D}_0 = \{0, \ldots, m\}^n$, that is by $(m + 1)^n$.

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

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

For the distribution of k identical balls into r urns there are exactly $\binom{r+k-1}{k}$ different possibilities. This is also the number of partitions of r into exactly k parts $x_1, \ldots, x_k$, that is, partitions of the form

$$r = x_1 + \cdots + x_k \quad \text{with } x_i \in \mathbb{N},$$

or the number of solutions $(x_1, \ldots, x_{k-1}) \in \mathbb{N}^{k-1}$ of

$$x_1 + \cdots + x_{k-1} \leq r.$$

Note that this bound, although considerably smaller, asymptotically doesn't behave much better than m^n. To get an impression of the improvement we observed execution times (on an iMac with 2.93 GHz Intel Core 7 processor, using Python from the command line):

- $m = 8$, $a = (1, 2, 3, 4, 5, 6, 7)$: more than 1 minute for $\mathcal{D}_0$, immediate answer for $\mathcal{D}_1$, note that $8^7 = 2,097,152$, $\binom{15}{8} = 6435$.
- $m = 12$, $a = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$: less than 30 seconds for $\mathcal{D}_1$. Don't wait for the result for $\mathcal{D}_0$, note that $12^{11} = 743,008,370,688$, $\binom{23}{12} = 1,352,078$.

In the Python program for solving **(A)** we replaced the function `dlist0()` by `dlist1()`, also from Appendix C.1, that produces the list of all integer vectors in $\mathcal{D}_1$.

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

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

4 Reduction to Normal Form

Consider the congruence **(A)**. For $r = 0, \ldots, m-1$ let

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

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

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

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

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

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 $y = (y_0, \ldots, y_{m-1}) \in \mathbb{N}^m$ of the special congruence

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

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

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

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 $(\mathbf{C}'_m)$ we conclude that each $y \in \mathcal{L}'_m$ has one of the forms

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

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

Let $\mathcal{L}_m$ be the set of indecomposable solutions of $(\mathbf{C}_m)$.

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

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

Call the congruences $(\mathbf{C}_m(J))$ for all subsets $J \subseteq \{1, \ldots, m-1\}$ the **normal forms** of linear congruences. Let $\mathcal{L}_m(J)$ be the set of indecomposable solutions of $(\mathbf{C}_m(J))$. 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 $i \in I_1 \cup \cdots \cup I_{m-1}$ with*

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

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

Corollary 1 *Let $N_m(a)$ be the number of indecomposable solutions of* **(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 involves 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 **(A)** that use at most analoguous estimates for $(\mathbf{C}_m(J))$ but not explicit knowledge of the solutions. Since this task might be too difficult in the general case results for special cases of coefficient tuples $a \in \mathbb{N}^n$ are also welcome. For the case $\#J = 2$ see [29].

The Standard Linear Congruence

For a subset $J \subseteq \{1, \ldots, m-1\}$ 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

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

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 $(\mathbf{C}_m)$, and justifies calling $(\mathbf{C}_m)$ **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 $(\mathbf{C}_m)$ 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.

5 The Support of an Indecomposable Solution

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

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

be its support and

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

the cardinality of its support, called the **width** of x. We abbreviate

$$\alpha(x) := x_1 + \cdots + n \cdot x_n$$

and call it the **weight** of x. Moreover we call

- $\|x\|_1 = x_1 + \cdots + x_n$ the **length** (sometimes [17] also called the degree),
- $\|x\|_\infty$ the **height**,
- $\|x\|_1 + \sigma(x)$ the **total size** (= length + width)

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

$$(\mathbf{C}_m) \qquad x_1 + \cdots + (m-1) \cdot x_{m-1} \equiv 0 \bmod m$$

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

Lemma 1 *Let r and m be natural numbers with $2r \le m$. 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:

(i) *Then the 2^r sums S_I represent at least $2r$ different classes* mod m.

(ii) *If $r \ge 4$, then S_I represent at least $2r+1$ different classes.*

(iii) *If $r = 3$, then S_I represent at least 7 different classes except in the case $\{t_1, t_2, t_3\} = \{a, m/2, a + m/2\}$ with $1 \le a < m/2$, $a \neq m/4$.*

Proof. See [6] or [26]. $\diamond$

Note 1 (without proof) A result by Olson [22, Theorem 3.2] implies that the S_I even represent more than $r^2/9$ different classes mod m (of course only if $r^2 < 9m$). See also the notes in Section 9.

We'll prove that the larger the width of an indecomposable solution $x \in \mathbb{N}^{m-1}$ of $(\mathbf{C}_m)$ the tighter is the bound for 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 $\sigma(x) \ge s$. Then:*

(i) $\|x\|_1 \le m - s + 1$.

(ii) $\|x\|_1 = m - s + 1$ *can occur only for* $\sigma(x) = s$.

(iii) $2s \le m + 1$; *even* $2s \le m$ *except in the case* $m = 3$ *and* $x = (1, 1)$.

(iv) *If $m \ge 4$ and $\|x\|_1 = m - s + 1$, then $s \le 3$ and there is exactly one index j with $x_j \ge 2$.*

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 $s \ge 1$.

(i) Since a forteriori $\sigma(x) \ge s - 1$, we already have $\|x\|_1 \le m - s + 2$ 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 $\|x\|_1 \le m - s + 1$.

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

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

hence $2s \le m$.

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

$$0 < u^{(1)} < ... < u^{(s)} < u^{(s+1)} = y < \ldots < u^{(m-s+1)} = x \tag{4}$$

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 $\bmod m$ 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 $\alpha(u) \bmod m$ for $0 \leq u \leq y$.

Since $\alpha(e_i) = i$, the $s+1$ values $t_0 = \alpha(e_{i_0}), \ldots, t_s = \alpha(e_{i_s})$ 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 $\alpha \bmod m$ 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 $i, m-i \in \mathrm{supp}(x)$ 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 $y = x$, $\mathrm{supp}(x) = \{i, m-i\}$, $s = 2$, $m = 3$, $x = (1,1)$.

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

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

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 $\bmod m$. In each chain

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

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.

For $s \geq 4$ the values $\alpha(u)$ in the previous paragraph represent at least $2s+1$ different residue classes, leaving not enough room for the values between y and x, contradiction.

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 $i = j$.

Finally assume no coordinate is ≥ 2, hence all $x_i \leq 1$. Then $\|x\|_1 = \sigma(x) = s$, hence $s = m-s+1$, $2s = m+1$, contradicting (iii). $\diamond$

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

Theorem 2 *Let $m \in \mathbb{N}_2$, and let x be an indecomposable solution of the standard linear congruence $(\mathbf{C}_m)$. Then:*

(i) *The width of x is bounded by $\sigma(x) \leq \frac{m}{2}$, except for $m = 3$, $x = (1, 1)$.*

(ii) (Eggleton-Erdős) *The total size of x is bounded by $\|x\|_1 + \sigma(x) \leq m + 1$.*

Note 2 (without proof) Olson's result, see Note 1, implies that $\sigma(x) \leq \lceil 3\sqrt{m}\,\rceil$ if x is an indecomposable solution of $(\mathbf{C}_m)$. However this bound is smaller than $\frac{m}{2}$ only for $m > 36$.

A transfer of the theorem to the general congruence **(A)** results in a somewhat clumsy formulation, at least if we admit pairs (a_i, a_j) of coefficients with $a_i \equiv a_j \pmod m$. Consider the general case of

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

We should collect together indices where the coefficients a_i are identical mod m. Therefore we replace the support by the set

$$\begin{aligned}\operatorname{supp}'(x) &:= \{a_i \bmod m \mid i = 1, \ldots, n, x_i \neq 0\} \\ &= \{j \mid 1 \leq j \leq n, \bigvee_{i=1,\ldots,n} (a_i = j \wedge x_i \neq 0)\}.\end{aligned}$$

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

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

In the special case $(\mathbf{C}_m)$ of **(A)** (or if all coefficients a_i are different mod m) we have $\operatorname{supp}' = \operatorname{supp}$ and $\sigma' = \sigma$. Now our result reads:

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

(i) $\sigma'(x) \leq \frac{m}{2}$.

(ii) $\|x\|_1 + \sigma'(x) \leq m + 1$.

6 Extremal Solutions

Definition Call a solution x of $(\mathbf{C}_m)$ **extremal** if it is indecomposable and of total size $\|x\|_1 + \sigma(x) = m + 1$.

Example 1 If x is extremal and $\sigma(x) = 1$, then $\|x\|_1 = m$, thus $x = m\,e_i$ where i is coprime with m, see Proposition 1. There are exactly $\varphi(m)$ extremal solutions of width 1 (where φ is the Euler function).

Example 2 If x is extremal and $\sigma(x) = 2$ (hence $m \geq 3$), then by the corollaries of Theorem 2 in [29] $x = (m-2)\,e_i + e_j$ where i is coprime with m and $j \equiv 2i \pmod m$. There are exactly $\varphi(m)$ extremal solutions of width 2.

Lemma 2 (iv) implies:

Corollary 2 *Let $m \geq 4$ and x be an extremal solution of $(\mathbf{C}_m)$. Then $\sigma(x) \leq 3$ and there is exactly one index j with $x_j \geq 2$.*

However this is not yet the last word on extremal solutions.

For an extremal solution x we denote the one coordinate $x_j \geq 2$ by u, all other coordinates are $x_i \leq 1$. Multiplying the congruence $(\mathbf{C}_m)$ by an integer that is relatively prime with m (and reducing the coefficients mod m) doesn't change the solutions (up to a permutation of the indices $1, \ldots, m-1$) nor their widths or lengths. Therefore we may assume that $j = d \,|\, m$, see [28]. In this situation $(\mathbf{C}_m)$ has the form

$$d \cdot u + \Sigma(S) \equiv 0 \pmod m \tag{5}$$

where $S \subseteq \{1, \ldots, m-1\} - \{d\}$ and $\Sigma(S) = \sum_{i \in S} i$ is the sum of the elements of S, and x has the form

$$x = u \cdot e_d + \sum_{i \in S} e_i.$$

Let $s := \#S$ be the size of S, so $\sigma(x) = s + 1$. Since the cases $\sigma(x) = 2$ and $\sigma(x) \geq 4$ are settled by Example 2 and Corollary 2 we may assume that $s = 2$ (and $m \geq 4$). Since $\|x\|_1 = u + s$ and $\sigma(x) = 1 + s$, the extremality condition translates to the equation $m + 1 = u + 2 + 1 + 2$, or

$$u + 4 = m \tag{6}$$

(and $m \geq 6$). We have $u < m' := m/d$ for otherwise the solution $m'\,e_d < x$ contradicts the minimality of x. In particular

$$du < m. \tag{7}$$

(By the way this implies that $d \leq 2$.) We may shrink the potential range of S due to the observation

$$m - wd \notin S \quad \text{for } w = 1 \ldots, u,$$

for otherwise $m - wd \in S$ makes $w\,e_d + e_{m-wd}$ a solution that is $< x$ except in the case $w = u$ and $m - ud = d$—but then also $m - wd = d \notin S$.

Now we consider the set

$$R := \{0, \ldots, m-1\} - \{m - wd \,|\, 1 \leq w \leq u\}$$

with $S \subseteq R - \{0, d\}$ (note that maybe $d \in R$ and that the removed elements $m - wd$ are multiples of d). Its size is $\#R = m - u = 4$. Let $T := S \cup \{d\} = \mathrm{supp}(x)$. Then $r := \#T = s + 1 = 3$, $2r \leq m$. If we let U run through all the 8 subsets of T, Lemma 1 applies, and one of the following two statements must be true:

1. There is a subset $U \subseteq T$, $U \neq \emptyset$, with $m \,|\, \Sigma(U)$.
2. The sums $\Sigma(U)$ represent ≥ 6 different residue classes mod m, even ≥ 7 different classes, except when T is one of the exceptional sets from Lemma 1.

Statement 1 makes $\sum_{i \in U} e_i$ a solution of $(\mathbf{C}_m)$ that is $\leq e_d + \sum_{i \in S} e_i < x$, contradiction. Hence statement 2 is true.

Case I, the $\Sigma(U)$ represent at least seven classes, thus at least three outside of R. Then at least two have the form $\Sigma(U) \equiv m - wd \pmod{m}$ with $1 \leq w < u$. If $d \notin U$, then $U \subseteq S$, and $w\, e_d + \sum_{i \in U} e_i$ is a solution $< u\, e_d + \sum_{i \in S} e_i = x$ of $(\mathbf{C}_m)$, contradiction.

If however $d \in U$, then

$$y = w\, e_d + \sum_{i \in U} e_i = (w+1)\, e_d + \sum_{i \in U - \{d\}} e_i$$

is a solution $\leq x$. The minimality of x enforces $w\, e_d + \sum_{i \in U} e_i = x$, that is $w = u - 1$, and $U = S \cup \{d\}$. But there is yet another residue class outside of R of the form $\Sigma(V) \equiv m - vd$ with $1 \leq v < u$, $v \neq w = u - 1$, hence $v \leq u - 2$. Thus $v\, e_d + \sum_{i \in V} e_i$ is a solution $< x$, contradiction.

Case II, $T = \{a, m/2, a + m/2\}$ with $1 \leq a < m/2$ and $a \neq m/4$. In particular m is even and $d = a$:

> We know that $d \in T$. Since $d \leq m/2$, d cannot be $a + m/2$. The assumption $d = m/2$ implies
>
> $$x = e_a + (m-4)\, e_{m/2} + e_{a+m/2},$$
>
> $$0 \equiv \alpha(x) = a + \frac{m}{2} \cdot (m-4) + a + \frac{m}{2} \equiv 2a + \frac{m}{2}.$$
>
> Since $0 < a < m/2$, this implies $2a = m/2$, contradicting $a \neq m/4$.

Since $T = S \cup \{d\}$ we conclude that $S = \{m/2, a + m/2\}$ and

$$x = (m-4)\, e_a + e_{m/2} + e_{a+m/2},$$

$$0 \equiv \alpha(x) = a \cdot (m-4) + \frac{m}{2} + a + \frac{m}{2} \equiv -3a,$$

hence $3a = m$, $d = a = m/3$, and m is a multiple of 6, say $m = 6n$. Then $u = 6n - 4$, $a = 2n$, $S = \{3n, 5n\}$,

$$x = (6n-4)\, e_{2n} + e_{3n} + e_{5n}.$$

Since $2 \cdot 2n + 3n + 5n = 12n$ the vector $2\, e_{2n} + e_{3n} + e_{5n}$ is a solution $\leq x$, hence $= x$, $6n - 4 = 2$, $n = 6$.

We summarize our analysis:

Theorem 3 *Assume $m \geq 3$, $m \neq 6$. Then all extremal solutions of $(\mathbf{C}_m)$ have widths $\sigma(x) = 1$ or 2. There are exactly $2\,\varphi(m)$ extremal solutions.*

In other words, there are no other extremal solutions than those in Example 1 and Example 2 of this section.

For $m = 6$ there are exactly two additional extremal solutions: $2\,e_2 + e_3 + e_5$ and $e_1 + e_3 + 2\,e_4$, thus the number of extremal solutions is $2\,\varphi(6) + 2 = 6$.

Corollary 3 *Let $m \geq 7$ and x be an indecomposable solution of $(\mathbf{C}_m)$ of width $\sigma(x) \geq 3$. Then the total size is $\|x\|_1 + \sigma(x) \leq m$, and the length is $\|x\|_1 \leq m - 3$.*

Corollary 4 *Let $m \geq 3$, $m \neq 6$, and x be an extremal solution of $(\mathbf{C}_m)$. Then the height is $\|x\|_\infty \geq m - 2$.*

7 The Action of the Multiplicative Group

Let $G = (\mathbb{Z}/m\mathbb{Z})^\times$ be the multiplicative group of the ring $\mathbb{Z}/m\mathbb{Z}$. By abuse of notation we usually represent the group elements by the integers a with $1 \leq a \leq m-1$ that are coprime with m. The order of G is $\#G = \varphi(m)$, the Euler phi-function.

The element $a \in G$ acts on $\mathbb{Z}^{m-1}$ by the formula

$$(x_1, \ldots, x_{m-1}) \mapsto (x_{a\cdot 1}, \ldots, x_{a\cdot(m-1)})$$

where the indices are reduced $\bmod m$ (another abuse of notation that we'll commit repeatedly). By the way this defines a permutation representation

$$\rho : G \longrightarrow \mathrm{Hom}(\mathbb{Z}^{m-1}, \mathbb{Z}^{m-1}), \quad \rho(a)\left(\sum x_i e_i\right) = \sum x_{ai} e_i = \sum x_j e_{cj}$$

where c is the $\bmod m$-inverse of a, that is $ca \equiv 1 \pmod m$. Note that $\rho(a)(e_i) = e_{ci}$.

The solutions of $(\mathbf{C}_m)$ constitute the kernel of the weight (monoid) homomorphism

$$\bar\alpha = \alpha \bmod m : \mathbb{N}^{m-1} \longrightarrow \mathbb{Z}/m\mathbb{Z}.$$

Let x be a solution of $(\mathbf{C}_m)$. Then

$$\alpha(\rho(a)\,x) = \sum_{i=1}^{m-1} i\,x_{ai} \equiv c \cdot \sum_{i=1}^{m-1} ai\,x_{ai} \equiv c \cdot \sum_{j=1}^{m-1} j\,x_j = c \cdot \alpha(x) \equiv 0 \pmod m$$

since $\bmod m$ multiplication by a permutes the indices $1, \ldots, m-1$.

Lemma 3 *G permutes the solutions of $(\mathbf{C}_m)$, as well as the indecomposable solutions.*

Proof. The consideration above shows that $\rho(a)$ maps the solution monoid $H = \ker(\bar\alpha)$ to itself, hence induces an automorphism of it, hence maps its canonical system B of generators—the set of indecomposable solutions—to itself. $\diamond$

Note 1 In [9] it is shown that G is the full autorphism group of the solution monoid H.

Invariants The length $\| \bullet \|_1$ and the width σ are invariant under the action of G, hence the total size $\| \bullet \|_1 + \sigma$ is also invariant. The weight α is not invariant, nor is its reduced version $\bar{\alpha}$.

Stabilizers An element $a \in G$ stabilizes $x = (x_1, \ldots, x_{m-1}) \in \mathbb{N}^{m-1}$ if and only if for all indices $i = 1, \ldots, m-1$:

$$x_{ai} = x_i.$$

Remark 1 For $a \in G$ the first coordinate of $\rho(a)\, x$ is x_a. Hence if $a \in G_x$, the stabilizer of x, then $x_a = x_1$. Thus a vector x with $x_i \neq x_1$ for $i \neq 1$ has a trivial stabilizer. More generally this is true when x has a coordinate x_j with j coprime with m and $x_i \neq x_j$ for $i \neq j$. Having a trivial stabilizer implies having an orbit of size $\varphi(m)$.

Definition We call the elements of the G-orbit of x the **conjugates** of x, analogously for subsets of $\mathbb{Z}/m\mathbb{Z}$.

Examples The orbit of $x = m\, e_1$ exactly consists of the $\varphi(m)$ extremal solutions of $(\mathbf{C}_m)$ of width 1. If $m \geq 4$, then the orbit of $x = (m-2)\, e_1 + e_2$ exactly consists of the $\varphi(m)$ extremal solutions of width 2.

For $m = 6$ we have the additional two extremal solutions $(0, 2, 1, 0, 1)$ and $(1, 0, 1, 2, 0)$. They are conjugates (choose $a = 5 \equiv -1$) and make up the whole orbit since the group order is $\varphi(6) = 2$.

Definition If x is a solution of $(\mathbf{C}_m)$, then the weight $\alpha(x)$ is a multiple km of m. Call $k = \alpha(x)/m$ the **multiplicity** (or type [2]) of x. The **index** (or level) of x is the minimum of the multiplicities taken over the G-orbit [2]:

$$\iota(x) := \min \left\{ \frac{\alpha(\rho(a)\, x)}{m} \;\middle|\; a \in (\mathbb{Z}/m\mathbb{Z})^\times \right\}.$$

Remark 2 If x is a solution of $(\mathbf{C}_m)$, then its index $\iota(x)$ is an integer. Thus we have a map

$$\iota : \ker(\bar{\alpha}) \longrightarrow \mathbb{N}.$$

By definition ι is invariant under the action of G.

Examples If x is an extremal solution of $(\mathbf{C}_m)$, and $m \neq 6$, then $\iota(x) = 1$, since $\alpha(me_1) = \alpha((m-2)\, e_1 + e_2) = m$.

In the case $m = 6$ the two exceptional extremal solutions have index 2 since $\alpha(0, 2, 1, 0, 1) = \alpha(1, 0, 1, 2, 0) = 12$.

Remark 3 For $m \leq 7$, $m \neq 6$, all indecomposable solutions of $(\mathbf{C}_m)$ have index one—see the complete list of indecomposable solutions. For $m = 6$ only the two exceptional solutions have index $\neq 1$.

Note 2 (ESCY Theorem) If x is an indecomposable solution of $(\mathbf{C}_m)$ of length $\|x\|_1 \geq \lfloor m/2 \rfloor + 2$, then $\iota(x) = 1$. ("Long solutions have index one.")

If $k \geq \lfloor m/2 \rfloor + 2$, then there are exactly $\varphi(m) \cdot P(m-k)$ indecomposable solutions of length k.

This was conjectured by Elashvili and independently proved by Savchev/Chen [34] and Yuan [37]—whence the acronym ESCY.

An implication is (Harris and Wehlau [17]): If x is an indecomposable solution of length $\|x\|_1 = k \geq \lfloor m/2 \rfloor + 2$, then the orbit $G \cdot x$ contains exactly one vector of multiplicity 1, and has size $\#G \cdot x = \varphi(m)$.

Lemma 4 *Let $m \geq 3$ and x be an extremal solution of $(\mathbf{C}_m)$ of weight $\alpha(x) = m$. Then $x = me_1$ or $x = (m-2)\, e_1 + e_2$.*

Proof. Let $s = \sigma(x)$. If $s = 1$, then we have $\|x\|_1 = m$, $x = me_i$, $m = \alpha(x) = mi$, hence $i = 1$, $x = me_1$.

Now assume $s \geq 2$ and

$$\operatorname{supp}(x) = \{i_1, \ldots, i_s\} \quad \text{with } 1 \leq i_1 \leq \ldots \leq i_s \leq m-1.$$

In particular $i_\nu \geq \nu$ for $\nu = 1, \ldots, s$. Extremality means

$$\sum_{\nu=1}^{s} x_{i_\nu} = \|x\|_1 = m + 1 - s.$$

From the chain

$$\begin{aligned} m = \alpha(x) = \sum_{\nu=1}^{s} i_\nu x_{i_\nu} \geq \sum_{\nu=1}^{s} \nu x_{i_\nu} = \sum_{\nu=1}^{s} x_{i_\nu} + \sum_{\nu=1}^{s} (\nu-1)\, x_{i_\nu} \\ = m - (s-1) + \sum_{\nu=2}^{s} (\nu-1)\, x_{i_\nu} \geq m - (s-1) + (s-1) = m \end{aligned}$$

of equalities and inequalities we conclude that

$$\sum_{\nu=2}^{s} (\nu-1)\, x_{i_\nu} = s - 1,$$

which is possible only if $s = 2$ and $x_{i_2} = 1$. Set $i_1 = i$ and $i_2 = j$. Since $x_j = 1$ and $m - 1 = \|x\|_1 = x_i + x_j$ we have $x_i = m - 2$, thus $x = (m-2)\, e_i + e_j$ and $\alpha(x) = i \cdot (m-2) + j$. The case $m = 3$ being settled we may assume that $m \geq 4$. Then necessarily $i = 1$ and consequently $j = 2$. $\diamond$

Corollary 1 *If $m \geq 3$ and x is an extremal solution of $(\mathbf{C}_m)$ of index one, then x has one of the forms*

(i) $x = me_i$ *where* i *is coprime with* m,

(ii) $x = (m-2)\,e_i + e_j$ *where* i *is coprime with* m *and* $j = 2i \bmod m$.

Proof. These are the conjugates of $x = me_1$ and $x = (m-2)\,e_1 + e_2$. $\diamond$

From this result we derive an alternative proof of Theorem 3:

Let x be an extremal solution of $(\mathbf{C}_m)$, and $s = \sigma(x)$. Then the length of x is $\|x\|_1 = m + 1 - s$, and

$$m + 1 - s \geq \left\lfloor \frac{m}{2} \right\rfloor + 2 \quad \Longleftrightarrow \quad s \leq m - \left\lfloor \frac{m}{2} \right\rfloor - 1 = \left\lceil \frac{m}{2} \right\rceil - 1. \tag{8}$$

If m is odd, then $\lceil m/2 \rceil - 1 = \lfloor m/2 \rfloor$, hence (except for the trivial case $m = 3$) the condition in (8) is satisfied by Theorem 2 (i). The ESCY Theorem applies and settles Theorem 3 for this case.

If m is even, then $\lceil m/2 \rceil - 1 = m/2 - 1$, and by the same reasoning we are done except in the case $s = m/2$. In this case $\|x\|_1 = 1 + m/2$, and x has one coordinate $x_i = 2$, all other coordinates $x_j = 1$ or 0 (for $j \neq i$). Corollary 2 of Theorem 2 implies that $s = 3$, thus $m = 6$.

The alternative proof of Theorem 3 is complete.

8 Glueing and Splitting of Solutions

Definition The **glueing operator** η_{ij} for $1 \leq i, j \leq m-1$ with $i + j \neq m$ acts on the set of vectors $x \in \mathbb{N}^{m-1}$ with $e_i + e_j \leq x$ by the formula

$$\eta_{ij}(x) = x + e_{i+j} - e_i - e_j$$

where as usual the indices are reduced mod m. (The operator η_{ij} "glues" e_i and e_j together to e_{i+j}.)

The condition for x being in the definition domain of η_{ij} is

- either $i, j \in \operatorname{supp}(x)$ and $j \neq i$,
- or $i = j \in \operatorname{supp}(x)$ and $x_i \geq 2$.

Example 1 $m = 5$, $x = (3, 1, 0, 0) = 3e_1 + e_2$, $i = 1$, $j = 2$: The operator η_{12} replaces (one pair of) e_1 and e_2 by e_3, hence $\eta_{13}(x) = 2e_1 + e_3 = (2, 0, 1, 0)$.

We may also choose $i = j = 1$: The operator η_{11} replaces $2e_1$ by e_2, hence $\eta_{11}(x) = e_1 + 2e_2 = (1, 2, 0, 0)$.

Lemma 5 *Let* $x \in N^{m-1}$ *have* $i, j \in \operatorname{supp}(x)$. *Then:*

(i) $\|\eta_{ij}(x)\|_1 = \|x\|_1 - 1$.

(ii) $\alpha(\eta_{ij}(x)) = \alpha(x) - m\delta_{ij}$ *where*

$$\delta_{ij} = \begin{cases} 0 & \text{if } i+j < m, \\ 1 & \text{if } i+j > m. \end{cases}$$

In particular $\eta_{ij}(x)$ *solves* $(\mathbf{C}_m)$ *if and only if* x *does.*

(iii) $\iota(x) - 1 \le \iota(\eta_{ij}(x)) \le \iota(x)$.

(iv) $\sigma(\eta_{ij}(x)) = \sigma(x) + \varepsilon_{ij}(x)$ *where* $\varepsilon_{ij}(x) \in \{-2, -1, 0, 1\}$.

(v) *If* x *is an indecomposable solution of* $(\mathbf{C}_m)$*, then so is* $\eta_{ij}(x)$.

Proof. (i) follows directly from the definition.

(ii) $\alpha(\eta_{ij}(x)) = \alpha(x + e_{i+j} - e_i - e_j) = \alpha(x) + (i + j \bmod m) - i - j$.

(iii) For $a \in G$ with mod m-inverse c we have

$$\begin{aligned} \rho(a)(\eta_{ij}(x)) &= \rho(a)(x) + \rho(a)(e_{i+j}) - \rho(a)(e_i) - \rho(a)(e_j) \\ &= \rho(a)(x) + e_{ci+cj} - e_{ci} - e_{cj} = \eta_{ci,cj}(\rho(a)(x)), \\ \alpha(\rho(a)(\eta_{ij}(x)))/m &= \alpha(\eta_{ci,cj}(\rho(a)(x)))/m = \alpha(\rho(a)(x))/m - \delta_{ci,cj} \end{aligned}$$

by (ii). Minimizing this expression over $a \in G$ yields $\iota(x)$ or $\iota(x) - 1$.

(iv) The extreme cases are $\varepsilon_{ij}(x) = -2$ if $(i + j \bmod m) \in \operatorname{supp}(x)$ and $x_i = x_j = 1$, and $\varepsilon_{ij}(x) = 1$ if $(i + j \bmod m) \notin \operatorname{supp}(x)$ and $x_i, x_j \ge 2$. In all other cases $\varepsilon_{ij}(x) = -1$ or 0.

(v) By (ii) $\eta_{ij}(x)$ is a solution since x is. Assume $\eta_{ij}(x) = u + v$ where both u and v are nonzero solutions. Then the index $i + j \bmod m$ must occur in at least one of u or v with a nonzero coordinate, say $i + j \bmod m \in \operatorname{supp}(u)$. Then $x = u' + v$ is a nontrivial decomposition where $u' = u - e_{i-j} + e_i + e_j$. $\diamond$

Definition An indecomposable solution u of $(\mathbf{C}_m)$ is called **splittable** [39] if there is an indecomposable solution x with $u = \eta_{ij}(x)$. Otherwise x is called **unsplittable**.

Example 2 The indecomposable solution $u = (2, 0, 1, 0)$ of $(\mathbf{C}_5)$ is splittable: It "splits" to the indecomposable solution $x = (3, 1, 0, 0)$ since $\eta_{13}(3e_1 + e_2) = 2e_1 + e_3$, see Example 1.

Example 3 The extremal solution $u = (m-2)\,e_1 + e_2$ is splittable: The operator η_{11} replaces $2e_1$ by e_2, hence transform $x = me_1$ to u.

Note 1 A result by Xia/Yuan, see [39], says that each indecomposable solution x of width $\sigma(x) = 2$ is splittable.

Note 2 The concept of splittability throws some light on the question about the index of indecomposable solutions of $(\mathbf{C}_m)$ that miss the ESCY bound $\lfloor m/2 \rfloor + 2$. The paper [38] considers the case $\|x\|_1 = \lfloor m/2 \rfloor + 1$ and proves:

- If x is splittable, then its index is $\iota(x) = 1$.
- If x is unsplittable, then its index is $\iota(x) \geq 2$.
- If m is odd and x is unsplittable, then its index is $\iota(x) = 2$.

In [39] this last result is extended to odd $m \geq 9$ and unsplittable indecomposable solutions x with $\lfloor m/3 \rfloor + 3 \leq \|x\|_1 \leq m - 1$, and the explicit form of the corresponding solutions is derived.

Together with the ESCY theorem this implies that indecomposable solutions x of lengths $\lfloor m/2 \rfloor + 2 \leq \|x\|_1 \leq m - 1$ are splittable.

9 Flat Solutions and the Strong Davenport Constant

Lemma 6 *For a solution $x \neq 0$ of $(\mathbf{C}_m)$ with support S the following statements are equivalent:*

(i) *All coordinates of x are 0 or 1.*

(ii) $\|x\|_\infty = 1$.

(iii) $\|x\|_1 = \sigma(x)$.

(iv) $m \,|\, \Sigma(S)$.

Proof. Trivial. $\diamond$

Definition Call a solution of $(\mathbf{C}_m)$ **flat** (or squarefree [13]) if it satisfies the equivalent conditions of Lemma 6.

Remark 1 If a subset $S \subseteq \{1, \ldots, m-1\}$ supports a flat solution, then no superset of S can support an indecomposable solution. In particular if $\#S \geq 3$ and j, $m - j \in S$ for some j with $1 \leq j < \frac{m}{2}$, then S doesn't support any indecomposable solution.

Remark 2 A flat solution x has $\sigma \geq 2$, since $\alpha(e_i) = i$ is not a multiplie of m.

Remark 3 A flat solution that is extremal occurs only for $m = 3$, namely $(1, 1)$. For the two conditions flat, $\|x\|_1 = \sigma(x)$, and extremal, $\|x\|_1 + \sigma(x) = m + 1$, together enforce $2\,\sigma(x) = m + 1$, a contradiction for $m \geq 4$.

Remark 4 Let x be an indecomposable solution of $(\mathbf{C}_m)$.

- If x is not extremal, then by definition $\|x\|_1 + \sigma(x) \leq m$.
- If x is not flat, then by definition $\sigma(x) \leq \|x\|_1 - 1$.

Hence if x is neither extremal nor flat, then $2\,\sigma(x) \leq \|x\|_1 - 1 + \sigma(x) \leq m - 1$, thus $\sigma(x) \leq (m-1)/2$, a slight improvement over the usual bound $\sigma(x) \leq m/2$. However this is superseded by Olson's results, see Note 2 in Section 5.

Note Gao et al proved, see [38], that for $m \geq 8$ an indecomposable solution x with $\|x\|_1 \geq \frac{6m+28}{19}$ (roughly $m/3$) is not flat—also superseded by Olson.

The **strong** Davenport **constant** of $\mathbb{Z}/m\mathbb{Z}$, see [2], is defined as the largest width of an indecomposable solution of $(\mathbf{C}_m)$:

$$\mathsf{SD}(m) := \max\{\sigma(x) \mid x \text{ indecomposable solution of } (\mathbf{C}_m)\}.$$

Equivalently it is the maximum number of *different* elements in a minimal zerosum multiset in $\mathbb{Z}/m\mathbb{Z}$. (Remember that the Davenport constant is the maximum number of not necessarily different elements in a minimal zerosum multiset.)

Examples From the complete lists of indecomposable solutions we know that

$$\mathsf{SD}(3) = \mathsf{SD}(4) = \mathsf{SD}(5) = 2.$$

For $m \geq 6$ we have $m - 3 \geq 3$, hence $x = e_1 + e_2 + e_{m-3}$ is an indecomposable solution of width $\sigma(x) = 3$. Therefore $\mathsf{SD}(m) \geq 3$.

By the next theorem it doesn't matter whether $\mathsf{SD}(m)$ is defined via multisets or via sets—in other words, the bound $\mathsf{SD}(m)$ is attained by flat indecomposable solutions. We start with two lemmas.

Lemma 7 *Let $m \geq 3$ and x be an indecomposable solution of $(\mathbf{C}_m)$ of maximal width $\sigma(x) = \mathsf{SD}(m)$.*

(i) *If $i \in \operatorname{supp}(x)$, then $ki \not\equiv 0 \pmod m$ for $1 \leq k \leq x_i$.*

(ii) *If $i, j \in \operatorname{supp}(x)$, $i \neq j$, and $m \geq 6$ or $\|x\|_1 \geq 3$, then $i + j \not\equiv 0 \pmod m$.*

Proof. (i) Otherwise ke_i is a solution $\leq x$, hence $= x$, hence $\sigma(x) = 1$, contradiction.

(ii) Otherwise $e_i + e_j$ is a solution $\leq x$, hence $= x$, hence $\sigma(x) = \|x\|_1 = 2$, contradiction in both cases. $\diamond$

Lemma 8 *Let $m \geq 3$ and x be an indecomposable solution of $(\mathbf{C}_m)$ of maximal width $\sigma(x) = \mathsf{SD}(m)$ with coordinate $x_i \geq 2$. Then for each $j \in S := \operatorname{supp}(x) - \{i\}$ at least one of the following statements holds:*

(i) $i + j \in \operatorname{supp}(x)$,

(ii) $x_j = 1$.

Proof. Since $\sigma(x) \geq 2$ and $x_i \geq 2$ we have $\|x\|_1 \geq 3$. Thus Lemma 7 (ii) implies that $i + j \not\equiv 0 \pmod m$ for $j \in S$.

Moreover the conditions $i + j \notin \operatorname{supp}(x)$ and $x_j \geq 2$ together would imply that $y = \eta_{ij}(x) = x - e_i - e_j + e_{i+j}$ is an indecomposable solution with i, j, and $i + j \bmod m$ in its support, hence $\sigma(y) = s + 1$, contradiction. Therefore x must satisfy at least one of the conditions (i) or (ii). $\diamond$

Theorem 4 (Chapman/Freeze/Smith) *Let $m \geq 3$ and $s = \mathsf{SD}(m)$. Let x be an indecomposable solution of $(\mathbf{C}_m)$ that assumes the maximal width $\sigma(x) = s$, and let the length $\|x\|_1$ be minimal under this condition. Then x is flat.*

Proof. We assume that x is not flat and derive a contradiction. Under this assumption x has a coordinate $x_i \geq 2$ for an $i \in \mathrm{supp}(x)$. Then $2i \not\equiv 0 \pmod m$ by Lemma 7 (i). The glueing operator η_{ii} produces an indecomposable solution $y = \eta_{ii}(x)$ with $\|y\|_1 = \|x\|_1 - 1$. The minimality of $\|x\|_1$ enforces $\sigma(y) < s$. Since $y = x - 2e_i + e_{2i}$ this implies that

$$2i \bmod m \in \mathrm{supp}(x) \tag{9}$$

and $i \notin \mathrm{supp}(y)$, hence $x_i = 2$. By Lemma 8 for each $j \in S = \mathrm{supp}(x) - \{i\}$ the vector x must satisfy at least one of the conditions $i + j \in \mathrm{supp}(x)$ or $x_j = 1$.

Case I: Assume $x_j \geq 2$ for some $j \in S$. Then $i + j \in \mathrm{supp}(x)$, and the support of $y = \eta_{ij}(x)$ contains i and j, hence $\sigma(y) = s$, but $\|y\|_1 = \|x\|_1 - 1$ contradicts the minimality of $\|x\|_1$.

Case II: $x_j = 1$ for all $j \in S$. Then $x = 2e_i + \sum_{j\in S} e_j$. For each $j \in S$ the solution $y = \eta_{ij}(x)$ with $\|y\|_1 = \|x\|_1 - 1$ has i and $i + j \bmod m$ in its support, but not j. Since $\sigma(y) = s - 1$ necessarily $i + j \bmod m \in \mathrm{supp}(x)$.

Using equation (9) we get $3i = i + 2i \not\equiv 0 \pmod m$ and $3i \bmod m \in \mathrm{supp}(x)$. Continuing iteratively we see that the whole arithmetic progression $ki \bmod m$ is in $\mathrm{supp}(x)$, hence

$$\mathrm{supp}(x) = \{ki \bmod m \mid 1 \leq k \leq s\}.$$

Continuing the iteration beyond s we also get $(s+1)\, i \bmod m \in \mathrm{supp}(x)$, hence $(s+1)\, i \equiv ki \pmod m$ for some k with $1 \leq k \leq s$, and from this the contradiction $(s+1-k)\, i \equiv 0 \pmod m$. $\diamond$

By Theorem 4, for determining $\mathsf{SD}(m)$ we need to consider only flat indecomposable solutions or, equivalently, minimal zerosum subsets of $\mathbb{Z}/m\mathbb{Z}$. Explicit values, easily determined by a simple program, see Appendix C.3.2, are

$$\mathsf{SD}(m) = \begin{cases} 2 & \text{for } m = 3,\ 4,\ 5, \\ 3 & \text{for } m = 6,\ 7, \\ 4 & \text{for } m = 8,\ 9,\ 10, \\ 5 & \text{for } m = 11,\ \ldots,\ 15, \\ 6 & \text{for } m = 16,\ \ldots,\ 23. \end{cases}$$

The program uses the trivial fact that if S is a minimal zerosum subset of size s, and $t \in S$, then $S - \{t\}$ is a zerofree subset of size $s-1$. It proceeds successively by increasing size s and terminates as soon as it doesn't find any zerofree subsets of size s. This relies on the following results (valid also for an arbitrary abelian group M instead of $\mathbb{Z}/m\mathbb{Z}$):

Proposition 3 *Let S be a zerofree multiset in $M = \mathbb{Z}/m\mathbb{Z}$. Then the number $\sigma(S)$ of different elements of S is at most $\mathsf{SD}(m)$.*

Proof. By definition $t := -\Sigma(S) \in M - \{0\}$, hence $T := S \cup \{t\}$ is a zerosum multiset, $\Sigma(T) = \Sigma(S) + t = 0$. There is a minimal zerosum multiset $U \subseteq T$. Since S is zerofree U is not contained in S, hence the multiplicity of t in U is 1+ the multiplicity of t in S, and $U' := U - \{t\}$ (multiplicity of t decreased by 1) is a submultiset of S. Moreover

$$\Sigma(U') = \Sigma(U) - t = -t = \Sigma(S).$$

Therefore $S - U'$ is a zerosum multiset contained in S, hence $= \emptyset$, thus $U' = S$ and $U = U' \cup \{t\} = S \cup \{t\} = T$. Since U is minimal $\sigma(S) \le \sigma(T) = \sigma(U) \le \mathsf{SD}(m)$. $\diamond$

Corollary 1 *If $S \subseteq M$ is a zerofree subset, then $\#S \le \mathsf{SD}(m)$.*

Proof. Since S is a set $\#S = \sigma(S)$. $\diamond$

Corollary 2 *The maximum size of a zerofree subset of M is $\mathsf{SD}(m)$ or $\mathsf{SD}(m) - 1$.*

Proof. The maximum size is $\le \mathsf{SD}(m)$ by Corollary 1. To get a zerofree set of size $\mathsf{SD}(m) - 1$ take a zerosum subset of size $\mathsf{SD}(m)$ and remove an arbitrary element. $\diamond$

Example The smallest module for which all zerofree subsets have size $\le \mathsf{SD}(m) - 1$ is $m = 8$ (with $\mathsf{SD}(8) = 4$). As a consequence for $m = 8$ indecomposable solutions that attain the maximum width $\sigma(x) = \mathsf{SD}(8)$ must be flat.

Problem Assume $m \ge 6$. Let x be an indecomposable solution of $(\mathbf{C}_m)$ of maximal width $\sigma(x) = \mathsf{SD}(m)$. Is $\|x\|_1 \le \sigma(x) + 1$? In other words, has x at most one coordinate > 1, and if so is this coordinate necessarily $= 2$?

The answer is yes for $m \le 16$ (and for $m = 3$ or 4).

For $m = 5$ a counterexample is $x = (3, 1, 0, 0)$.

Notes on the Erdős-Heilbronn conjecture (EHC):

1. The EHC claims that a subset S of a finite abelian group M has a nontrivial subsum equal to 0 if $r = \#S \ge c\sqrt{m}$ with $m = \#M$ for an absolute constant c. Erdős and Heilbronn proved this for the cyclic group $M = \mathbb{Z}/p\mathbb{Z}$ of prime order p with $c = 3\sqrt{6}$. Olson [21] dropped the constant to $c = 2$ for prime order p, and [22] to $c = 3$ for arbitrary (even non-abelian) M.
2. Let c be the E-H constant valid for the abelian group M. Let $T \subseteq M$ be a minimal zerosum set. Then $\#T \le \lceil c\sqrt{m}\,\rceil$:
   For if $\#T > \lceil c\sqrt{m}\,\rceil$, then $\#T \ge \lceil c\sqrt{m}\,\rceil + 1$. Dropping an arbitrary element from T results in a proper subset $S \subset T$ of size $\#S \ge \lceil c\sqrt{m}\,\rceil$, hence containing a nontrivial zerosum subset. Therefore T is not minimal.

3. Olson's result, see Note 1 in Section 5, applied to a subset $S \subseteq \mathbb{Z}/m\mathbb{Z}$ of size r with at most $r^2/9$ different subset sums, implies that 0 is a nontrivial subset sum of S. The precondition on r is obviously satisfied if $r^2/9 \geq m$, that is, $r \geq 3\sqrt{m}$. This yields Olson's bound.
4. The strong form of the EHC (by Erdős) drops the constant to $c = \sqrt{2}$. In this strong form the conjecture is open, the best known bound is $\sqrt{2p}+5 \log p$ for $m = p$ prime, and $c = \sqrt{2m} + \varepsilon(m)$ where $\varepsilon(m)$ is $\mathrm{O}(\sqrt[3]{m} \cdot \log(m))$ for M cyclic of order m, proved by Hamidoune and Zémor [15].

   Therefore we have

   - $\mathsf{SD}(m) \leq \lceil 3\sqrt{m} \rceil$ (proved by Olson), and
   - $\mathsf{SD}(m) \leq \lceil \sqrt{2m} \rceil$ (conjectured by Erdős).

   The explicit values above show that the bound $\lceil \sqrt{2m} \rceil$ is sharp for many values of m.

10 An Algorithm for Determining All Indecomposable Solutions

We apply Theorems 2, 3, and 4 to derive an algorithm that constructs all indecomposable solutions of $(\mathbf{C}_m)$ and is faster than the algorithms from Sections 2 and 3.

We may assume $m \geq 7$ (for $m \leq 6$ the algorithm from Section 3 is good enough). We extend the algorithm from Section 9 that determines $\mathsf{SD}(m)$, and by the way all minimal zerosum subsets and all zerofree subsets of $\mathbb{Z}/m\mathbb{Z}$, see Appendix C.3.2, in the following way:

- Whenever we detect a new minimal zerosum subset we register the corresponding flat solution.
- Whenever we detect a new zerofree subset S (of size s) we know that the indecomposable solutions x supported by S—except the extremal ones for $s = 2$—have $\|x\|_1 \leq m - s$ and arise from the following procedure:

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

We include the extremal solutions of width 2 separately during the construction of the indecomposable solutions of width 1.

The algorithm proceeds by increasing width s. Here is the sketch of the algorithm:

1. Initialize the lists

   - `solulist` of indecomposable solutions,
   - `zslist` of minimal zerosum subsets,
   - `zflist` zerofree subsets,

   as empty lists. The list `zflist` is reset to the empty list for each new width s (after keeping a temporary copy).

2. First treat the case $s = 1$ separately (together with the extremal solutions of width 2). Loop over $t = 1, \ldots, m-1$.

   - Append $\{t\}$ to `zflist`.
   - Compute $d = \gcd(t, m)$ and set $x_t = m/d$, $x_i = 0$ otherwise, and append x to `solulist`.
   - If $d = 1$ set $x_t = m-2$, $u = 2t \bmod m$, $x_u = 1$, $x_i = 0$ otherwise, and append x to `solulist`.

3. **[Loop]** Exit if `zflist` is empty. Otherwise increment s, keep a copy `oldlist` of `zflist`, and reset `zflist` to the empy list.

   - Expand each `oldset` in `oldlist` successively by one element $t > \max($`oldset`$)$ to get $S =$ `newset`. Discard the result if S is already in `zflist`, or if S contains a zerosum set from `zslist`.
   - Otherwise (S not discarded) test the zerosum property.
     - If the sum over S is divisible by m, a new zerosum subset is detected. Append it to `zslist`, and append the corresponding flat vector x to `solulist`.
     - Otherwise a new zerofree subset S is detected. Append it to `zflist`. Construct all indecomposable solutions supported by S, see below, and append them to `solulist`.

Indecomposable solutions supported by $S = \{i_1, \ldots, i_s\}$:

- Enumerate all integer vectors $y = (y_1, \ldots, y_{s-1})$ in the simplex

$$\mathcal{D} = \{y \in \mathbb{R}^{s-1} \mid y \geq 0, \|y\|_1 \leq m - 2s\}$$

  that depends only on the size s, not on the set S.

- For each y set $x_{i_\nu} = y_\nu + 1$ for $\nu = 1, \ldots, s-1$, and try $x_{i_s} = 1, \ldots, m-2s-\|y\|_1+1$ until x is a solution. Append x to `solulist`. (If no solution is found skip y.) (Since there is no guarantee that x is minimal, as a last step in the algorithm we reduce `solulist` to its minmal elements.)

We illustrate the procedure by a pencil-and-paper example with $m = 7$, see Appendix B. The result is in perfect harmony with the output of the algorithms from Sections 2 and 3.

A Python program that implements this algorithm is in Appendix C.3.3. Here some processing time measurements:

- For m up to 14 the processing time is less than 1 second.
- For $m = 17$ the processing time is about 10 seconds.
- For $m = 21$ the processing time is slightly more than 6 minutes.

11 A Lower 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 algorithm in Sections 3 and 10 we have the explicit values for small modules m, see Table 1. The On-line Encyclopedia of Integer Sequences [23], sequence `A096337`, has the values up to $m = 38$. The corresponding logarithmic plot (base 2) in Figure 2 lets us hope for a slightly sublinear growth, or a slightly subexponential growth of ℓ itself.

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
$P(m)$	2	3	5	7	11	15	22	30	42	56	77
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
$P(m)$	101	135	176	231	297	385	490	627	792	1002	1255

We consider a large class of indecomposable solutions: The multiplicity function α/m is a homomorphism of the solution monoid $H \subseteq \mathbb{N}^{m-1}$ of $(\mathbf{C}_m)$ onto the monoid $\mathbb{N}$. The preimage of 0 consists of 0 only. Therefore all vectors in the preimage of 1 must be indecomposable in H, and these are exactly the solutions of the (truncated) partition equation

$$(\mathbf{P}_m) \qquad x_1 + 2x_2 + \cdots + (m-1)x_{m-1} = m.$$

This observation attributed to Stanley [19]. It shows:

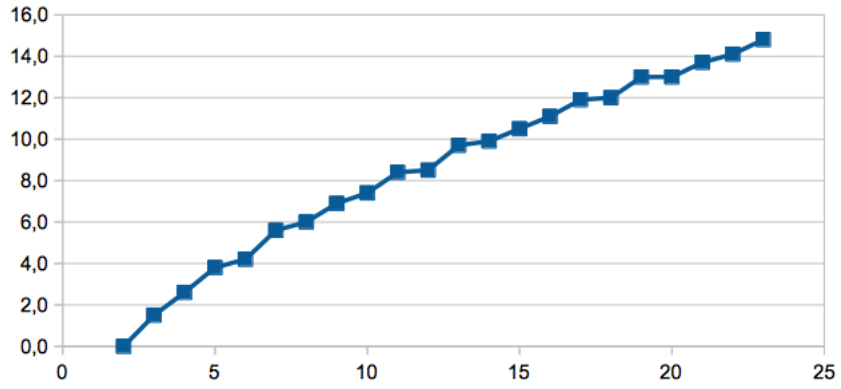

Figure 1: 2-logarithm of the number of indecomposable solutions

Lemma 9 *The indecomposable solutions of* $(\mathbf{C}_m)$ *of weight* m *are exactly the solutions of* $(\mathbf{P}_m)$.

These solutions correspond to the partitions of m except the trivial partition $m = m{\cdot}1$ of m into a single piece of size m that we excluded by omitting the term mx_m from the partition equation. In this way we find $P(m) - 1$ indecomposable solutions where P is the partition function whose values are in the last row of Table 1. These numbers are computed with the SageMath function `Partitions(m).cardinality()`.

Corollary 1 *A solution of* $(\mathbf{C}_m)$ *has index* 1 *if and only if it is conjugated to a solution of* $(\mathbf{P}_m)$.

It's easy to find more indecomposable solutions (except for $m = 2$):

a) The indecomposable solutions with one-element support: Take a $j \in \{1, \ldots, m-1\}$ that is not a divisor of m, and let $t \geq 1$ be minimal with $m | jt$ (maybe $t = m$). Then x with $x_j = t$, $x_i = 0$ otherwise, is an indecomposable solution. This yields $(m-1) - (d(m) - 1) = m - d(m)$ solutions where

$$d(m) := \#\{j \in \{1, \ldots, m\} \mid j | m\}.$$

(Note that the cases where $j | m$ are counted with the partitions of m.)

b) If $x = (x_1, \ldots, x_{m-1})$ is an indecomposable solution of $(\mathbf{C}_m)$, then so is the reverse vector $\overleftarrow{x} = (x_{m-1}, \ldots, x_1)$, a conjugate of x. This yields a new indecomposable solution if x is not symmetric for the reversing operation $x \mapsto \overleftarrow{x}$ and has at least a two-element support. Of the $P(m) - 1$ reverse vectors of the solutions of $(\mathbf{P}_m)$ we know already

1. those with a one-element support $\{j\}$ where $j | m$, a total of $d(m) - 1$,
2. the symmetric ones with at least two entries $\neq 0$; a total of $\lfloor \frac{m-1}{2} \rfloor$. For assume that x is symmetric and $x_j \geq 1$. Then $x_{m-j} = x_j$, and

$$jx_j + (m-j)x_{m-j} = mx_j \equiv 0 \pmod{m}.$$

Since $j + (m - j) = m$ and x is indecomposable we conclude that $x_j = x_{m-j} = 1$, $x_i = 0$ otherwise. Thus $x = e_j + e_{m-j}$ for $1 \leq j \leq \frac{m-1}{2}$.

c) The following lemma gives some additional indecomposable solutions with two-element support. The conditions $\alpha(x) > m$ and $\alpha(\overleftarrow{x}) > m$ ensure that neither x nor $\overleftarrow{x}$ is a solution of $(\mathbf{P}_m)$, so both of them are not contained in our previous sets from a) and b).

Lemma 10 *Let $m \geq 4$, and let $2 \leq j \leq \frac{m}{2}$ with $\gcd(j, m) = 1$ and $j \not| (m-1)$. Then $(\mathbf{C}_m)$ has an indecomposable solution of the form $x = e_1 + te_j$ with $\alpha(x) > m$ and $\alpha(\overleftarrow{x}) > m$, thus neither x nor $\overleftarrow{x}$ is a solution of $(\mathbf{P}_m)$.*

Proof. Let $1 = sj + km$ with $s, k \in \mathbb{Z}$. Then $m \,|\, 1 - sj$. Set $t = (-s) \bmod m$. Then $0 < t < m$ and $m \,|\, 1 + tj$, thus $x = e_1 + te_j$ is a solution, and we may assume that t is minimal with this property (or replace t by the minimal value).

Is x indecomposable? A solution $y < x$ would have one of two forms:

- $y = ue_j$ with $0 \leq u \leq t$,
- $y = e_1 + ue_j$ with $0 \leq u < t$.

The second case is excluded by the construction of t, in the first case $m \,|\, uj$, and $u > 0$ would imply that u and m not coprime, contradicting $m \,|\, 1 + tj$. Hence $u = 0$, $y = 0$, and x is indecomposable.

Now $\alpha(x) = m$ would imply $m = 1 + tj$, hence $j \,|\, (m-1)$, and this is excluded. For $\overleftarrow{x} = te_{m-j} + e_{m-1}$ we have $\alpha(\overleftarrow{x}) = t \cdot (m-j) + m - 1 \geq \frac{m}{2} + m - 1 > m$. $\diamond$

This gives a pair of solutions in the following cases:

- Never for $j = 2$ since 2 divides one of m or $m - 1$.
- One pair for each prime $j \geq 3$, $j \leq \frac{m}{2}$ with $m \equiv 2, 3, \ldots, j-1 \pmod{j}$.
- One pair for each $j \geq 3$, $j \leq \frac{m}{2}$ with $m \equiv j - 1 \pmod{j}$.

Counting a) and b) together we get:

$$\ell(m) \geq [P(m) - 1] + [m - d(m)] + \left[P(m) - 1 - d(m) + 1 - \lfloor \frac{m-1}{2} \rfloor \right].$$

This formula simplifies to:

Proposition 4 *The number $\ell(m)$ of indecomposable solutions of $(\mathbf{C}_m)$ satisfies*

$$\ell(m) \geq 2 \cdot P(m) - 2 \cdot d(m) + \lfloor \frac{m}{2} \rfloor.$$

To get a smooth formula we ask for which m we have $2 \cdot d(m) \leq \lfloor \frac{m}{2} \rfloor$.

Lemma 11 *Let $m = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of $m \in \mathbb{N}_1$ with $r \geq 0$, $2 \leq p_1 < \ldots < p_r$, and $e_i > 0$. Then:*

(i) $d(m) = (e_1 + 1) \cdots (e_r + 1)$.

(ii) $(e_1 + 1) \cdots (e_r + 1) \leq m$.

(iii) $2 \cdot d(m) \leq \lfloor \frac{m}{2} \rfloor \Longleftrightarrow 4 \cdot (e_1 + 1) \cdots (e_r + 1) \leq m$.

(iv) *If one of the $p_i^{e_i} \geq 4(e_i + 1)$, or if two of them are $\geq 2(e_i + 1)$, then* $4(e_1 + 1)...(e_r + 1) \leq m$.

(v) $2 \cdot d(m) \leq \lfloor \frac{m}{2} \rfloor$ *except for* $m \leq 10$ *and for* $m = 12, 14, 15, 16, 18, 20, 24, 30$.

Proof. (i) The divisors ≥ 1 of m are exactly the numbers $p_1^{d_1} \cdots p_r^{d_r}$ with $0 \leq d_i \leq e_i$.
(ii) By (i), since $d(m) \leq m$.
(iii) Follows directly from (i), and $2 \cdot d(m) \leq \lfloor \frac{m}{2} \rfloor \Leftrightarrow 2 \cdot d(m) \leq \frac{m}{2}$.
(iv) Since $2^x \geq x+1$ for $x \geq 1$ we have always $p_i^{e_i} \geq e_i + 1$. The assumptions provide for the factor 4.
(v) We have

$$2^e \geq 4 \cdot (e+1) \Longleftrightarrow e \geq 5, \quad 2^e \geq 2 \cdot (e+1) \Longleftrightarrow e \geq 3,$$

$$3^e \geq 4 \cdot (e+1) \Longleftrightarrow e \geq 3, \quad 3^e \geq 2 \cdot (e+1) \Longleftrightarrow e \geq 2,$$

$$5^e \geq 4 \cdot (e+1) \Longleftrightarrow e \geq 2, \quad 5^e \geq 2 \cdot (e+1) \Longleftrightarrow e \geq 1,$$

$$7^e \geq 4 \cdot (e+1) \Longleftrightarrow e \geq 2, \quad 7^e \geq 2 \cdot (e+1) \Longleftrightarrow e \geq 1,$$

$$p^e \geq 4 \cdot (e+1) \quad \text{for all primes } p \geq 11 \text{ and all exponents } e \geq 1.$$

Thus the criterion (iv) applies except when m divides one of the numbers

$$2^4 \cdot 3 = 48, \quad 2^2 \cdot 3^2 = 36, \quad 2^2 \cdot 3 \cdot 5 = 60, \quad \text{or} \quad 2^2 \cdot 3 \cdot 7 = 84,$$

that is the exceptions enumerated in (v) as well as $m = 21, 28, 36, 42, 48, 60, 84$. For these latter ones we verify the assertion by direct calculation. For example $d(21) = 4$. $\diamond$

Theorem 5 *The number of indecomposable solutions of $(\mathbf{C}_m)$ has the lower bound*

$$\ell(m) \geq 2 \cdot P(m) \quad \textit{for } m \geq 7.$$

Proof. Except for $m = 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 24, 30$ this follows from Proposition 4 and Lemma 11 (v). For $m = 7, 8, 9, 10, 12, 14$ we consult Table 1. For the remaining 6 values $15, 16, 18, 20, 2430$ of m we have to provide $2d(m) - \lfloor \frac{m}{2} \rfloor$ more indecomposable solutions of $(\mathbf{C}_m)$, that is $1, 2, 3, 2, 4, 1$. We find them among the indecomposable solutions with two-element support using Lemma 10. We have to count the indices j, $2 \leq j \leq \frac{m}{2}$ with $\gcd(j, m) = 1$ and $j \not| (m-1)$, each one providing two additional solutions. These indices are

- 4 for $m = 15$,
- 7 for $m = 16$,
- $5, 7$ for $m = 18$,
- $3, 7, 9$ for $m = 20$,
- $5, 7, 11$ for $m = 24$,
- and $7, 11, 13$ for $m = 30$,

enough in any case. $\diamond$

The asymptotic behaviour of the partition function P is well known [16], for example for arbitrary $a \in \mathbb{R}$ with $0 \leq a < \frac{1}{4 \cdot \sqrt{3}}$ we have the lower bound

$$P(m) \geq \frac{a}{m} \cdot e^{\pi \sqrt{\frac{2m}{3}}} \quad \text{for almost all } m \in \mathbb{N}_2.$$

We conclude:

Corollary 2 *Let $a \in \mathbb{R}$ arbitrary with $0 \leq a < \frac{1}{2 \cdot \sqrt{3}}$. Then*

$$\ell(m) \geq \frac{a}{m} \cdot e^{\pi \sqrt{\frac{2m}{3}}} \quad \textit{for almost all } m \in \mathbb{N}_2.$$

Note that Table 1 suggests that the number ℓ of indecomposable solutions grows significantly faster that the partition function P. The asymptotic lower bound given in [5] is somewhat larger, but also far below the empirical values.

Heuristic remark: Let x be a "partition solution", and assume that its stabilizer is the trivial group. Then the orbit of x contributes $\varphi(m)$ indecomposable solutions. Assuming that "most" stabilizers are trivial (or more adequately, that "most" orbits meet the set of partition solutions only in one point), and using that $\varphi(m)$ is about m, we get about $m \cdot P(m)$ different indecomposable solutions. Thus $m \cdot P(m)$ is a heuristic lower bound for the number of indecomposable solutions.

If this idea could be fleshed out appropriately, it would result in lower bounds

$$\ell(m) \stackrel{?}{\geq} m\, P(m) \geq a \cdot e^{\pi \sqrt{\frac{2m}{3}}} \quad \text{for almost all } m \in \mathbb{N}_2.$$

12 An Upper Bound for the Number of Indecomposable Solutions

By the corollary of Theorem 1 we have $\ell(m) \leq \binom{2m-2}{m}$. By Theorem 2 we even have $x_1 + \cdots + x_{m-1} \leq m - 1$ 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 $\ell(m) \le \binom{2m-3}{m-1}$—the e_j are not solutions but satisfy the stronger bound $\|x\|_1 \le m-1$.

By standard methods we easily derive an upper bound for the growth of $\ell(m)$: We use a corollary of STIRLING's formula, see [27]:

Lemma 12

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

where the error term E_n is bounded by

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

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

Proposition 5 *For $m \ge 2$ 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 an exponential 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 $m \ge 4$. Then the support of an indecomposable solution has at most $\mathsf{SD}(m) \le \lfloor \frac{m}{2} \rfloor$ elements. For each $s \in \{1, \dots, \mathsf{SD}(m)\}$ 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.

Proposition 1 says that the number of indecomposable solutions of width $s = 1$ is

$$m-1 = \frac{(m-1)!}{1! \cdot 0! \cdot (m-2)!} = \binom{m-1}{1, 0, m-2}.$$

For $s = 2$ we have $\binom{m-1}{2} = (m-1)(m-2)/2$ choices for S. Let $S = \{i, j\}$ with $1 \le i < j \le m-1$. The number of indecomposable solutions with support in $\{i, j\}$ is $\le m-1$, see [**?**, 29]. This number includes the two solutions with one-element support $\{i\}$ or $\{j\}$. Thus the number of indecomposable solutions with support $\{i, j\}$ is $\le m-3$. Therefore the number of indecomposable solutions of width $s = 2$ is

$$\le \frac{(m-3)(m-1)(m-2)}{2} = \frac{(m-1)!}{2! \cdot 1! \cdot (m-4)!} = \binom{m-1}{2, 1, m-4}.$$

For $s \ge 3$ every indecomposable solution x with support S has $\|x\|_1 \le m-s$ by Corollary 3 of Theorem 3, except when x is one of the two exceptional solutions with $\sigma(x) = 3$ for $m = 6$. We catch all the other ones by choosing arbitrary $y_1, \dots, y_{s-1} \ge 0$ with $y_1 + \cdots + y_{s-1} \le m - 2s$, defining $x_{i_\nu} = y_\nu + 1$, and choosing x_{i_s} appropriately, that is, minimal such that $m \mid \alpha(x)$. The number of such choices is $\binom{m-2s+s-1}{s-1} = \binom{m-s-1}{s-1}$. This proves (for $m \ge 7$):

Lemma 13 *Let $m \geq 6$ and $s \geq 3$. Let $S \subseteq \{1, \ldots, m-1\}$ be an s-element subset. Then S supports at most $\binom{m-s-1}{s-1}$ indecomposable solutions of $(\mathbf{C}_m)$.*

For $m = 6$ and $s = 3$ we have the two exceptional solutions $x = (0, 2, 1, 0, 1)$ and $(1, 0, 1, 2, 0)$ with supports $S = \{2, 3, 5\}$ and $\{1, 3, 4\}$. These two sets don't support any other indecomposable solutions. Since $\binom{m-s-1}{s-1} = \binom{2}{2} = 1$, Lemma 13 is true also for $m = 6$.

Now we look at the result for fixed s:

$$\binom{m-1}{s} \cdot \binom{m-s-1}{s-1} = \frac{(m-1)!}{s!\,(m-1-s)!} \cdot \frac{(m-s-1)!}{(s-1)!\,(m-2s)!} = \binom{m-1}{s, s-1, m-2s},$$

a trinomial coefficient (valid also for $s = 1$ or 2). We resume:

Theorem 6 *For $m \geq 4$ the number $\ell(m)$ of indecomposable solutions of $(\mathbf{C}_m)$ satisfies*

$$\ell(m) \leq \sum_{s=1}^{\mathsf{SD}(m)} \binom{m-1}{s, s-1, m-2s},$$

a sum of trinomial coefficients, in particular $\ell(m) < 3^{m-1}$ for $m \geq 2$.

The last inequality ist stronger then Proposition 5. It follows from the standard result on multinomial coefficients:

$$\sum_{k_1+\cdots+k_r=n} \binom{n}{k_1, \ldots, k_r} = r^n.$$

Table 2 shows some explicit values (extending Table 1) where $q(m)$ is the bound from Theorem 6, using the known values of $\mathsf{SD}(m)$. Figure 2 provides an illustration of these values (extended to $m = 39$). The yellow line represents the lower bound from [5] where the unspecified proportionality factor is set to 1.

Discussion The bound $q(m)$ grows much too fast. Although significantly smaller than 3^{m-1} it seems to grow strictly exponentially. This phenomen has a simple heuristic explanation: In the proof of Theorem 6 we essentially counted all solutions in the respective simplices, not only the indecomposable ones. Since the solutions form the kernel of a homomorphism onto $\mathbb{Z}/m\mathbb{Z}$ we expect a fraction of $1/m$ of all vectors in this domain to yield solutions. Hence the exponential upper bound: volume of simplex $\times 1/m$.

Thus for improvements we should not bother with the sum in Theorem 6 but rather analyze the number $\binom{m-s-1}{s-1}$ in Lemma 13 that overestimates the number of *indecomposable* solutions.

On the other hand the value $m\,P(m)$ seems to provide a rather narrow lower bound for $m > 30$. See the heuristic remark in Section 11.

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

m	4	5	6	7	8	9	10	11
$2 \cdot P(m)$	10	14	22	30	44	60	84	112
$\ell(m)$	6	14	19	47	64	118	165	347
$m \cdot P(m)$	20	35	66	105	176	270	420	616
$q(m)$	6	16	45	126	357	1016	2781	8350
m	12	13	14	15	16	17	18	19
$2 \cdot P(m)$	154	202	270	352	462	594	770	980
$\ell(m)$	366	826	973	1493	2134	3912	4037	7935
$m \cdot P(m)$	924	1313	1890	2640	3696	5049	6930	9310
$q(m)$	23606	64032	163891	393498	1517895	[...]		
m	20	21	22	23	24	25	26	27
$2 \cdot P(m)$	1254	1584	2004	2510	3150	3916	4872	6020
$\ell(m)$	8246	12966	17475	29161	28064	49608	59357	83419
$m \cdot P(m)$	12540	16632	22044	28865	37800	48950	63336	81270

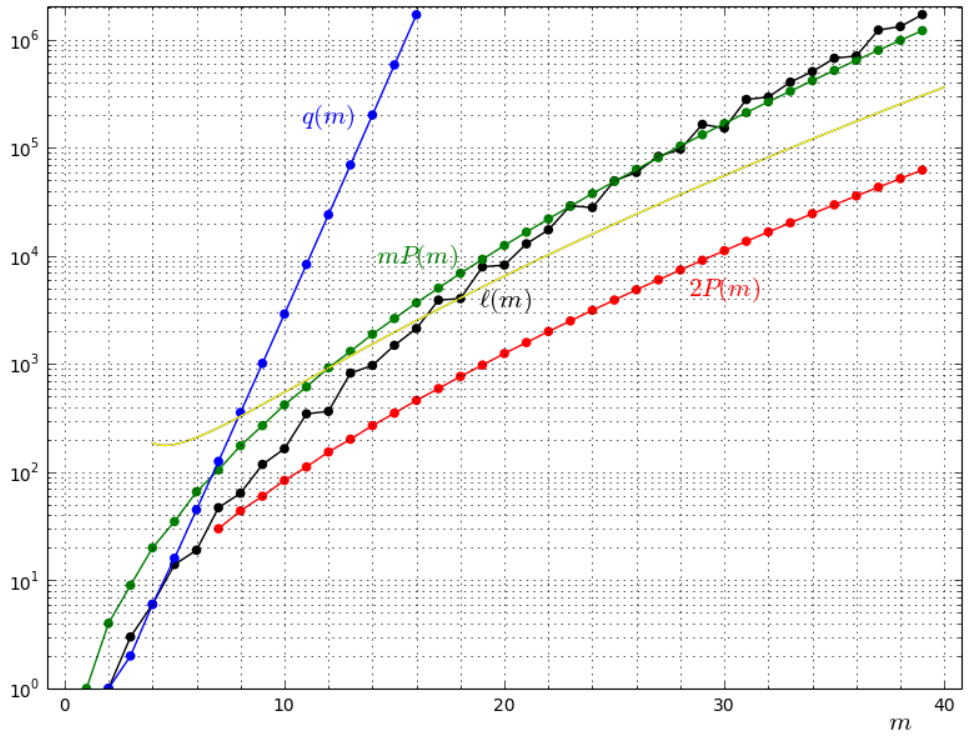

Figure 2: The number of indecomposable solutions (semi-logarithmic scale)

Some questions:

1. Is $\ell(m) \geq m\,P(m)$ for $m > 30$?
2. Is $\ell(m) \leq a \cdot e^{b\sqrt{m}}$ for certain constants a und b?
3. Is $\ell(m) \leq cm \cdot P(m)$ for $m \geq 2$ for some constant c? Note that this would imply a positive answer to question 2. Necessarily $c > 1$ if it exists at all since $\ell(23) > 23 \cdot P(23)$.
4. Or is at least $\ell(m) \leq f(m) \cdot P(m)$ for some polynomial f?

A Some Auxiliary Algorithms

Remove Non-Minimal Entries from a List

Suppose we have a (partially) ordered set M, and are given a list $(m_0, \ldots, m_{l-1})$ of elements of M. We want to reduce this list to its minimal elements. That is we want to remove the entry m_i from the list if there is an index $j \neq i$ such that $m_j < m_i$.

A naive algorithm would loop through all indices $i = 0, \ldots, l-1$, and for each loop would compare m_i with all m_j for $j \neq i$ until a smaller entry is found. Obviously in the worst case this algorithm performs about l^2 comparisions.

For better performance we go through all elements of the list and remove all entries that are larger than the current element. Then after each loop the list has shrunk a bit, and the loops become shorter and shorter.

A moment's thought convinces us that in each loop we better run through the list from right to left. For otherwise we had to update the index j after each successful comparision. So we use the following algorithm:

Let the index i point to the current entry $t = m_i$, initialize it with $i = 0$.
Loop over i:
  For $j = l - 1$ down to $i + 1$: [Comment: right-hand part of the list]
    If $m_j > t$: remove m_j.
  For $j = i - 1$ down to 0: [Comment: left-hand part of the list]
    If $m_j > t$: remove m_j and decrement i.
    [Comment: The current entry moves one position to the left.]
  Increment i. Update l. If $i < l$ rerun the loop.
  [Comment: Otherwise we reached the end of the (remaining) list.]

The update of the list for a removal on the right-hand or left-hand part is illustrated by Figures 3 and 4. The function `minelts()` in Appendix C gives a Python implementation of this algorithm for the ordered monoid $\mathbb{N}^n$.

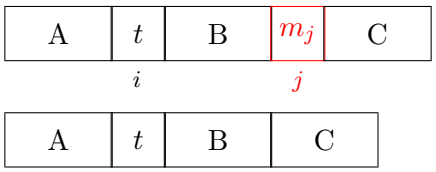

Figure 3: Remove an entry from the right-hand side

List All Integer Elements of a Hypercube

We enumerate the $(m+1)^n$ elements of $\mathcal{D}_0 = \{0, \ldots, m\}^n$ by the following pseudocode procedure:

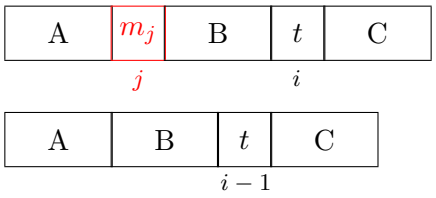

Figure 4: Remove an entry from the left-hand side

Use two lists L_0 and L_1 of vectors in $\mathbb{N}^r$.
    [The dimension r increases from 1 to n.]
Initialize L_0 as the empty list.
For $r = 1$ to n:
    Start by setting L_1 as empty list.
    For each element y of L_0: [a vector of dimension $r-1$]
        For $t = 0, \ldots, m$:
            Append the coordinate t to y, yielding a vector x of dimension r.
            Append x to L_1.
    Replace L_0 by L_1.

The resulting Python function in Appendix C is `dlist0()`.

List All Integer Elements of a Simplex

We enumerate the elements of $\mathcal{D}_1 = \{x \in \mathbb{N}^n \mid \|x\|_1 \leq m\}$ in a similar way as for $\mathcal{D}_0$, however appending only coordinates t that don't make the 1-norm larger then m. This is the pseudocode:

Use two lists L_0 and L_1 of vectors in $\mathbb{N}^r$.
    [The dimension r increases from 1 to n.]
Initialize L_0 as the empty list.
For $r = 1$ to n:
    Start by setting L_1 as empty list.
    For each element y of L_0: [a vector of dimension $r-1$]
        Calculate the 1-norm s of y, the sum of its coordinates.
        For $t = 0, \ldots, m-s$:
            Append the coordinate t to y, yielding a vector x of dimension r.
            Append x to L_1.
    Replace L_0 by L_1.

The resulting Python function in Appendix C is `dlist1()`.

B Indecomposable Solutions of (C_7)

We have $m = 7$ (and expect indecomposable solutions of widths 1, 2, and 3).

Initialization Set `solulist = []`, `zslist = []`, `zflist = []`.

The step $s = 1$

We loop over $t = 1, \ldots, 6$.

- We construct `zflist` $= [\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}]$.
- For all t we have $d = \gcd(t, 7) = 1$, hence append $x = 7e_t$ ...
- ... and $5e_t + e_{2t}$ to `solulist`.

Now `solulist = [700000, 070000, 007000, 000700, 000070, 000007, 510000, 050100, 005001, 100500, 001050, 000015]` (in a simplified but self-explanatory notation).

`zslist` remains empty.

The step $s = 2$

We start with `oldlist` $= [\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}]$ and reset `zflist` to empty. Then we successively treat the 15 two-element sets

$$\begin{aligned} S \;=\; &\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{1,6\}, \{2,3\}, \{2,4\}, \{2,5\}, \{2,6\}, \\ &\{3,4\}, \{3,5\}, \{3,6\}, \{4,5\}, \{4,6\}, \{5,6\}. \end{aligned}$$

After testing the zerosum property we append $\{1,6\}, \{2,5\}, \{3,4\}$ to `zslist` and `100001, 010010, 001100` to `solulist`. The remaining 12 two-element sets form the new `zflist`, and we have, for each of them, to construct the indecomposable solutions it supports. This construction involves the one-dimensional simplex

$$\mathcal{D} = \{y \in \mathbb{Z} \mid y \geq 0,\ y \leq m - 2s = 3\} = \{0, 1, 2, 3\},$$

giving raise to the values $1, 2, 3, 4$ for the solution coordinate x_{i_1}, and the search interval for x_{i_2} is $1, \ldots, 5 - x_{i_1}$ (that is $\|x\|_1 = x_{i_1} + x_{i_2} \leq m - s = 5$).

- For $S = \{1, 2\}$ we find suitable x_2-coordinates for $x_1 = 1$ and 3, yielding the indecomposable solutions `130000, 320000`.

Instead of treating all 12 sets separately we simplify the pencil-and-paper procedure by considering only one two-element subset from each orbit under the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$. These orbits are given by the following table:

	$\times 2$	$\times 3$	$\times 4$	$\times 5$	$\times 6$
$\{1,2\}$	$\{2,4\}$	$\{3,6\}$	$\{4,1\}$	$\{5,3\}$	$\{6,5\}$
$\{1,3\}$	$\{2,6\}$	$\{3,2\}$	$\{4,5\}$	$\{5,1\}$	$\{6,4\}$
$\{1,6\}$	$\{2,5\}$	$\{3,4\}$	$\{4,3\}$	$\{5,2\}$	$\{6,1\}$

(Remember that the group operation consist in multiplying the indices.) Thereby for the sets $\{2,4\},\{3,6\},\{1,4\},\{3,5\},\{5,6\}$ we get the additional ten indecomposable solutions `030200, 003002, 200300, 002030, 000023, 010300, 001003, 300100, 003010, 000031`.

- For $S = \{1,3\}$ we find suitable x_3-coordinates for $x_1 = 1$ and 4, yielding the indecomposable solutions `102000, 401000`. Again application of the multiplicative group catches the sets $\{2,6\},\{2,3\},\{4,5\},\{1,5\},\{4,6\}$ and generates the additional ten indecomposable solutions `010002, 021000, 000120, 200010, 000201, 040001, 014000, 000410, 100040, 000104`.

Since the orbits of $\{1,2\}$ and $\{1,3\}$ cover all zerofree sets of size 2 we are done with the step $s = 2$. The current `zslist` is

$$\{1,6\},\ \{2,5\},\ \{3,4\},$$

and the current `solulist`,

```
700000, 000007, 070000, 000070, 007000, 000700,
510000, 050100, 005001, 100500, 001050, 000015,
100001, 010010, 001100,
320000, 030200, 003002, 200300, 002030, 000023,
130000, 010300, 001003, 300100, 003010, 000031,
102000, 010002, 021000, 000120, 200010, 000201,
401000, 040001, 014000, 000410, 100040, 000104
```

The step $s = 3$

We start with `oldlist` consisting of

$$\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,6\},\{3,5\},\{3,6\},\{4,5\},\{4,6\},\{5,6\},$$

that form two orbits, and reset `zflist` to empty. Expanding the two representatives by one element we get

$$\{1,2\} \mapsto \{1,2,3\}, \underbrace{\{1,2,4\}}_{\text{zerosum}}, \underbrace{\{1,2,5\}}_{\supseteq\{2,5\}}, \underbrace{\{1,2,6\}}_{\supseteq\{2,6\}},$$
$$\{1,3\} \mapsto \underbrace{\{1,2,3\}}_{\text{redundant}}, \underbrace{\{1,3,4\}}_{\supseteq\{3,4\}}, \{1,3,5\}, \underbrace{\{1,3,6\}}_{\supseteq\{1,6\}},$$

and the conjugates of these sets. We find the minimal zerosum set

$$\{1,2,4\} \quad \text{and its conjugate} \quad \{3,5,6\},$$

and the zerofree set

$$\{1,2,3\} \quad \text{with conjugates} \quad \{2,4,6\},\{2,3,6\},\{1,4,5\},\{1,3,5\},\{4,5,6\}.$$

We append `110100` and `001011` to `solulist`, and are left with only one zerofree set up to conjugates:

- $S = \{1,2,3\}$. The auxiliary vectors y are 2-dimensional. Since $m - 2s = 1$ the simplex to consider consists of $(y_1, y_2) = (0,0), (0,1), (1,0)$.
  - For $y = (0,0)$ we have $x_1 = x_2 = 1$, and x_3 is restricted by $1 \le x_3 \le m - s - x_1 - x_2 = 2$. Neither $x_3 = 1$ nor $x_3 = 2$ yield a solution.
  - For $y = (0,1)$ we have $x_1 = 1$, $x_2 = 2$, and x_3 is restricted by $1 \le x_3 \le 1$. We get a non-solution.
  - For $y = (1,0)$ we have $x_1 = 2\, x_2 = 1$, and $x_3 = 1$, an indecomposable solution. We append `211000` and its conjugates `020101, 012001, 100210, 101020, 000112` to `solulist`.

Now `solulist` contains 47 indecomposable solutions

```
700000, 000007, 070000, 000070, 007000, 000700,
510000, 050100, 005001, 100500, 001050, 000015,
100001, 010010, 001100,
320000, 030200, 003002, 200300, 002030, 000023,
130000, 010300, 001003, 300100, 003010, 000031,
102000, 010002, 021000, 000120, 200010, 000201,
401000, 040001, 014000, 000410, 100040, 000104,
110100, 001011,
211000, 020101, 012001, 100210, 101020, 000112
```

The step $s = 4$

Since $4 > 7/2$ no extension of the zerofree sets of size 3 will yield a zerofree or minimal zerosum set. Hence the new `zflist` is empty, all sets of size 4 are discarded, and the exit condition is met at the next restart of the loop. The last `solulist` is the final one.

C Python Code

C.1 Auxiliary Routines

Compare Two Integer Vectors

```
def smaller(lista,listb):
  """Compare two integer lists in componentwise (partial) order of N^n."""
  ll = len(lista)
  unequal = False
  if ll != len(listb):
    return False
  for i in range(ll):
    if lista[i] > listb[i]:
      return False
    elif (not(unequal) and (lista[i] < listb[i])):
      unequal = True
  if unequal:
    return True
  else:
    return False
```

Remove Non-Minimal Entries from a List

```
def minelts(vlist):
  """Delete all entries from vlist that are properly larger than
  another entry."""
  i = 0
# Loop over i
  ll = len(vlist)
  while i < ll:
    t = vlist[i]
    for j in range(ll-1,i,-1):
      if smaller(t,vlist[j]):
        del vlist[j]
    for j in range(i-1,-1,-1):
      if smaller(t,vlist[j]):
        del vlist[j]
        i = i-1
    i = i+1
    ll = len(vlist)
  return vlist
```

List the Integer Elements of a Hypercube

```
def dlist0(n,m):
  """generate list of integer vectors of dim n
     in the hypercube [0,...,m]^n"""
  auxlist = [[]]
  for r in range(n):
    outlist = []
    for y in auxlist:
      for t in range(m+1):
        x = y + [t]
        outlist.append(x)
    auxlist = [] + outlist
  return outlist
```

List the Integer Elements of a Simplex

```
def dlist1(n,m):
  """generate list of integer vectors of dim n
     in the simplex ||x||_1 <= m"""
  auxlist = [[]]
  for r in range(n):
    outlist = []
    for y in auxlist:
      s = sum(y)
      for t in range(m+1-s):
        x = y + [t]
        outlist.append(x)
    auxlist = [] + outlist
  return outlist
```

C.2 Subroutines for Linear Congruences

Check the General Congruence

```
def chkcong(m, alist, xlist):
  """Check if alist[0]*xlist[0] + ... + alist[ll-1]*ilist[ll-1]
  congruent to 0 mod m."""
  l = len(alist)
  if len(xlist) != l:
    return False
  sum = 0
  for i in range(l):
    sum = sum + alist[i]*xlist[i]
  modsum = sum % m
  if modsum == 0:
    return True
  else:
    return False
```

C.3 Programs

For all the following programs assume the first lines

```
#!/usr/bin/env python3
import sys
import auxLC
```

`sys` provides access to the command line parameters, `auxLC` contains all the necessary functions from Appendices C.1 and C.2.

C.3.1 Solve a Linear Congruence

```
mm = int(sys.argv[1])
coeff = sys.argv[2:]
ll = len(coeff)
for i in range(ll):
  coeff[i] = int(coeff[i])
sollist = []   # list of solutions
dlist = dlist0(ll,mm)
nullvec = [0]*ll
dlist.remove(nullvec)
for xlist in dlist:
  if chkcong(mm,coeff,xlist):
    sollist.append(xlist)
redlist = minelts(sollist) # list of indecomposable solutions
print(redlist)
```

Sample call: `solve_A.py 10 1 2 4 1 3 5`
For a somewhat better performance replace `dlist0()` by `dlist1()`.

C.3.2 Construct Zerofree and Zerosum Sets

```
mm = int(sys.argv[1])
zslist = []  # list of zerosum subsets, to be built successively
zflist = []  # list of zerofree subsets of actual size,
             #   to be replaced in each step
for t in range(1,mm):
  zflist.append({t})
print("Size 1", "| zerofree subsets:", zflist)
s = 1                          # actual size
while len(zflist) > 0:         # stop condition not yet reached
  s += 1                       # next size
  oldlist = zflist.copy()      # zerofree sets of previous size
  zflist = []                  # zerofree sets of actual size
  for oldset in oldlist:       # expand each zerofree set
    for t in range(1,mm):      #   by one element t
      discard = False
      newset = oldset.copy()
      newset.add(t)
      if len(newset) < s or newset in zflist:
        discard = True         # discard if t already in oldset
                               #   or newset not really new
      else:
        for zsset in zslist: # or if newset contains a zerosum set
          if zsset <= newset:
            discard = True
      if not(discard):
        if sum(newset) % mm == 0: # test zerosum property
          zslist.append(newset)
          SD = s     # update value for strong Davenport constant
        else:
          zflist.append(newset)
  print("Size", s, "| zerofree subsets:", zflist)
print("Zerosum subsets:", zslist)
print("Number of zerosum subsets:", len(zslist))
print("Strong Davenport constant for module", mm, "is", SD)
```

Sample call: `zerosets.py 9`

C.3.3 Solve $(\mathbf{C}_m)$

```
m = int(sys.argv[1])
solulist = [] # list of indecomposable solutions
zslist = []   # list of zerosum subsets, to be built successively
zflist = []   # list of zerofree subsets of actual size,
              #   to be replaced in each step
nullvec = [0]*(m-1)
s = 1                         # actual size

### Treat the case s = 1 separately (and btw construct the extremal solutions
###   of width 2)
for t in range(1,m):
  zflist.append({t})
  x = nullvec.copy()
  dab = eEuclid(m,t)
  d = dab[0]
  x[t-1] = m//d
  solulist.append(x)    # indecomposable solution of width 1
  if d == 1:
    x = nullvec.copy()
    x[t-1] = m-2
    u = 2*t % m
    x[u-1] = 1
    solulist.append(x)  # extremal solution of width 2

### Loop over increasing size s
while len(zflist) > 0:       # stop condition not yet reached
  s += 1                     # next size
  auxvecs = dlist1(s-1,m-2*s) # y-vectors in simplex
  oldlist = zflist.copy()    # zerofree sets of previous size
  zflist = []                # zerofree sets of actual size
  for oldset in oldlist:     # expand each zerofree set
    for t in range(max(oldset)+1,m):  #   by one element t
      discard = False
      newset = oldset.copy()
      newset.add(t)
      if newset in zflist:
        discard = True       # discard if newset not really new
      else:
        for zsset in zslist: # or if newset contains a zerosum set
          if zsset <= newset:
            discard = True
      if not(discard):
```

```
        if sum(newset) % m == 0:  # test zerosum property
          zslist.append(newset)   # new minimal zerosum subset detected
          x = nullvec.copy()
          for i in newset:
            x[i-1] = 1
          solulist.append(x)      # corresponding flat solution
        else:
          zflist.append(newset)   # new zerofree subset detected
# Now construct indecomposable solutions supported by newset
          for y in auxvecs:
            norm1y = sum(y)
            j = 0
            x = nullvec.copy()
            pwt = 0          # partial sum of 1*x[0] + ... + (m-1)*x[m-2]
            for i in range(m-1):
              if (i+1) in newset:
                if j < (s-1):
                  x[i] = y[j] + 1
                  j += 1
                  pwt += (i+1)*x[i]
                else:   # j = s-1
                  go_on = True
                  k = 1
                  while (k <= m + 1 - 2*s - norm1y) and go_on:
                    x[i] = k
                    pwttotal = pwt + (i+1)*k
                    if (pwttotal % m) == 0:
                      z = x[:]
                      solulist.append(z) # solution found, not necessarily minimal
                      go_on = False
                    k += 1
redlist = minelts(solulist)
print(len(redlist), "indecomposable solutions:")
print(redlist)
```

Sample call: `solve_Cm.py 7`

References

[1] P. Bachmann: *Niedere Zahlentheorie*, Zweiter Teil, Additive Zahlentheorie. Teubner Leipzig 1910.

[2] S. T. Chapman, M. Freeze, W. W. Smith: Minimal zero sequences and the strong Davenport constant. Discr. Math. 203 (1999), 271–277.

[3] S. T. Chapman, W. W. Smith: A characterization of minimal zero sequences of index one in finite cyclic groups. Integers 5 (2005), #A27.

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

[5] 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.

[6] R. B. Eggleton, P. Erdős: Two combinatorial problems in group theory. Acta Arithmetica 21 (1972), 111–116.

[7] E. Ehrhardt: Sur un problème de géométrie diophantienne. J. reine angew. Math. 226 (1967), 1–29; 227 (1967), 25–49; 231 (1968), 220.

[8] E. Ehrhardt: Sur les équations diophantiennes linéaires. C. R. Acad. Sc. Paris 288 (1979), Série A, 785–787.

[9] A. Elashvili, M. Jibladze: Hermite reciprocity for the regular representations of cyclic groups. Indag. Math. 9 (1998), 233–238.

[10] P. Erdős, H. Heilbronn: On the addition of residue classes mod p. Acta Arithmetica 9 (1964), 149–159.

[11] 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.

[12] B. M. Finklea, T. Moore, V. Ponomarenko, Z. J. Turner: Invariant polynomials and minimal zero sequences. Involve 1 (2008), 159–165.

[13] W. D. Gao: Zero sums in finite cyclic groups. Integers 0 (2000), #A12.

[14] Y. O. Hamidoune: Subsequence sums. Combinatorics, Probability and Computing 12 (2003), 413–425.

[15] Y. O. Hamidoune, G. Zémor: On zero-free subset sums. Acta Arithm. 78 (1996), 143–152.

[16] G. H. Hardy, E. M. Wright: *Zahlentheorie.* Oldenbourg, M¸nchen 1958. = *Introduction to the Theory of Numbers.* Oxford Univ. Press 1938, 1954.

[17] J. C. Harris, D. L. Wehlau: Non-negative integer linear congruences. Indag. Math. 17 (2006), 37–44.

[18] M. Hochster: Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes. Annals of Math. 96 (1972), 318–337.

[19] V. G. Kac: Root systems, representations of quivers and invariant theory. *Invariant Theory*, Montecatini 1982, ed. by F. Gherardelli. Springer Lect. Notes 996 (1983).

[20] D. Knuth: *The Art of Computer Programming*, Volume 1, Fundamental Algorithms. Addison-Wesley, Reading Mass. 1968, 1973.

[21] J. E. Olson: An addition theorem modulo p. J. Comb. Theory 5 (1968), 45–52.

[22] J. E. Olson: Sums of sets of group elements. Acta Aritm. 28 (1975), 147–156.

[23] The On-line Encyclopedia of Integer Sequences, A096337. Online: `http://oeis.org/A096337`

[24] H. Ostmann: *Additive Zahlentheorie.* Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, Berlin usw. 1956.

[25] K. Pommerening: A remark on subsemigroups (Dickson's lemma). Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/Dickson.pdf`

[26] K. Pommerening: A remark on subset sums. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/SubSum.pdf`

[27] K. Pommerening: Stirling's formula. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/Stirling.pdf`

[28] K. Pommerening: Orbits of the multiplicative group mod m. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/OMGr.pdf`

[29] K. Pommerening: Linear congruences with two unknowns. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/LinCong2.pdf`

[30] K. Pommerening: The indecomposable solutions of linear Diophantine equations. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/LinDio.pdf`

[31] K. Pommerening: Some remarks on the complexity of invariant algebras. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/ComplInv.pdf`

[32] V. Ponomarenko: MZS. Online: `http://vadim.sdsu.edu/mzs.zip`

[33] L. Rédei: *Theorie der endlich erzeugbaren kommutativen Halbgruppen.* Akadémiai Kiadó, Budapest 1963.

[34] S. Savchev, F. Chen: Long zero-free sequences in finite cyclic groups. Discr. Math. 307 (2007), 2671–2679.

[35] C. W. Strom: On complete systems under certain finite groups. Bull. Amer. Math. Soc. 37 (1931), 570–574.

[36] M. F. Tinsley: A combinatorial theorem in number theory. Duke Math. J. 33 (1966), 75–79.

[37] Yuan P.: On the index of minimal zero-sum sequences over finite cyclic groups. J. Comb. Theory A 114 (2007), 1545–1551.

[38] Yuan P., Li Y.: Long unsplittable zero-sum sequences over a finite cyclic group. Int. J. Number Theory 12 (2016), 979–993.

[39] Zeng X., Yuan P., Li Y.: On the structure of long unsplittable minimal zero-sum sequences. Acta Arith. 176 (2016), 131–159.