Linear Congruences with Two Unknowns

Klaus Pommerening
Johannes-Gutenberg-Universität
Mainz, Germany

October 1986 – english version August 2016 – Version 2, February 2018
last change: February 25, 2018

Given $m \in \mathbb{N}_2$ and $a, b \in \mathbb{N}$. We want to find all solutions $(x, y) \in \mathbb{N}^2$ of the linear congruence

$$(\mathbf{A_2}) \qquad ax + by \equiv 0 \pmod{m}.$$

Without loss of generality we may assume that $a, b \in \{0, \ldots, m-1\}$.

The semigroup $\mathbb{N}^2$ has the (partial) order

$$(x, y) \le (x', y') \Longleftrightarrow x \le x' \text{ and } y \le y'.$$

The solution set of $(\mathbf{A_2})$ is a sub-semigroup $H \le \mathbb{N}^2$ with the property

$$(x, y), (x', y') \in H,\ (x, y) \le (x', y') \Longrightarrow (x' - x, y' - y) \in H.$$

Consider the set M of minimal elements > 0 of H. From Dickson's lemma [1], see also [2], we get that M is finite, consists of the indecomposable elements of H, and generates H. Thus H has a canonical minimal system of generators that is finite.

> *Caution*: Not every sub-semigroup of $\mathbb{N}^2$ is finitely generated. As an example take $H = \{(p, q) \mid q \ge 1\} \cup \{(0, 0)\}$.

Thus solving the the linear congruence $(\mathbf{A_2})$ boils down to determining the indecomposable solutions. In particular:

(I) *Find an efficient algorithm that yields all indecomposable solutions.*

(II) *Determine the number of indecomposable solutions.*

The analogous problem for the linear congruence with one unknwon is trivial:

> Let $m \in \mathbb{N}_2$ and $a \in \mathbb{N}$. 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, then $x = m$.

The results for two unknowns are considerably more involved, but known, see [7], [5]. Here we give a particularily simple derivation plus some extensions. For more unknowns see [4].

1 Reductions

First we reduce $(\mathbf{A_2})$ to the case $a = 1$:

Lemma 1 *Let $m \in \mathbb{N}_2$ and $a, b \in \mathbb{N}$.*

(i) *Let $d := \gcd(m, a)$ and $d' := \gcd(d, b)$, $d = d'e$. Then for $(x, y) \in \mathbb{N}_2$ the following two statements are equivalent for $(x, y) \in \mathbb{N}^2$:*

1. *(x, y) is an indecomposable solution of $(\mathbf{A_2})$.*
2. *$x < \frac{m}{d}$, $e|y$, and $(x, \frac{y}{e})$ is an indecomposable solution of*

$$\frac{a}{d} \cdot s + \frac{b}{d'} \cdot t \equiv 0 \pmod{\frac{m}{d}}.$$

(ii) *If a and m are coprime, then the indecomposable solutions of $(\mathbf{A_2})$ are exactly the same as for $1 \cdot x + b' \cdot y \equiv 0 \pmod m$ where c is the inverse of a modulo m, and $b' = bc \bmod m$.*

Proof. (i) If $x \geq \frac{m}{d}$,then $(\frac{m}{d}, 0)$ is a solution $\leq x$. If $ax + by = km$, then $d|by$, $e|\frac{b}{d'}\, y$, hence $e|y$. Thus

$$ax + by = km \Leftrightarrow \frac{a}{d}\, x + \frac{b}{d'}\, \frac{y}{e} = k\, \frac{m}{d}.$$

Therefore the mapping $(x, y) \mapsto (x, \frac{y}{e})$ is a bijection between the respective sets of solutions, and obviously it preserves the indecomposability (in both directions).

(ii) We have $ac \equiv 1 \pmod m$, thus $ax + by = km \Leftrightarrow x + bcy = kcm$. $\diamond$

Corollary 1 *Let $m \in \mathbb{N}_2$ and $a, b \in \mathbb{N}$. Let $d = \gcd(a, m)$, $d' := \gcd(d, b)$, $a' = a/d$, $m' = m/d$, c the multiplicative inverse of $a' \bmod m'$, and $b' = c \cdot (b/d' \bmod m')$. Then $x \in \mathbb{N}$ is the first coordinate of an indecomposable solution of $(\mathbf{A_2})$ $ax + by \equiv 0 \pmod m$ if and only if x is the first coordinate of an indecomposable solution of $(\mathbf{A_2'})$ $x + b'y \equiv 0 \pmod{m'}$.*

Note that each $x \in \mathbb{N}$ occurs at most once as the first coordinate of an indecomposable solution of $(\mathbf{A_2})$, and only if $x \leq m$. (In particular the number of indecomposable solutions is at most $m + 1$.) The corresponding second coordinate y is

$$y = \min\{t \in \mathbb{N}_1 \mid ax + bt \equiv 0 \pmod m\},$$

except for the one case $x > 0$ and $ax \equiv 0 \pmod m$, where $y = 0$.

So we need to study only the simplified congruence

$$(\mathbf{A_2'}) \qquad x + by \equiv 0 \pmod m$$

where $m \in \mathbb{N}_2$ and $b \in \mathbb{N}$ arbitrary. We include the degenerate cases $m = 1$ and $b = 0$.

- The congruence $x + by \equiv 0 \pmod 1$ with arbitrary $b \in \mathbb{N}$ has two indecomposable solutions: $(1,0)$ and $(0,1)$.
- The congruence $x + 0 \cdot y \equiv 0 \pmod m$ with arbitrary $m \in \mathbb{N}_1$ has two indecomposable solutions: $(m,0)$ and $(0,1)$.

Our next goal is to find a reduction to a smaller value of the module m, derive a recursive (or iterative) construction of the indecomposable solutions, and determine their number. (We start by looking in the opposite direction, going from m to $m+b$.)

Lemma 2 *Let $m \in \mathbb{N}_1$, $b \in \mathbb{N}$. Assume $(s,t) \in \mathbb{N}^2$ is an indecomposable solution of $s + bt \equiv 0 \pmod m$. Let $u := \frac{s+bt}{m}$. Then:*

(i) *$u = \lceil \frac{bt}{m} \rceil$, except for $(s,t) = (m,0)$.*

(ii) *$t + u \le m + b$; even $t + u < m + b$, except for $(s,t) = (0,m)$, or for $m = 1$, $b = 0$.*

(iii) *$(s, t+u)$ is an indecomposable solution of*

$$x + by \equiv 0 \pmod{m+b}. \tag{1}$$

Proof. (i) If $(s,t) \ne (m,0)$, then $0 \le s < m$, hence $\frac{bt}{m} \le u < \frac{m+bt}{m} = 1 + \frac{bt}{m}$.

(ii) Assume $(s,t) \ne (0,m)$. Then $0 \le t \le m-1$. By (i) we have $u < 1 + \frac{bt}{m}$, or $t = 0$, $s = m$, $u = 1$. In the first case $t + u < m + \frac{bt}{m} \le m + b \cdot \frac{m-1}{m} < m + b$. In the second case $t + u = 1 < 2 \le m + b$, except in the case $m = 1$, $b = 0$; here $(s,t) = (1,0)$ and $u = 1$.

Now let $(s,t) = (0,m)$. Then $u = b$ and $t + u = m + b$.

(iii) If $(s,t) = (m,0)$, then $(s,t+u) = (m,1)$ is an indecomposable solution of (1).

Now assume $0 \le s < m$, $0 < t \le m$. Then $s + b\cdot(t+u) = u \cdot (m+b)$, hence $(s,t+u)$ a solution of (1). Assume (x,y) is a solution of (1) with $0 < (x,y) \le (s,t+u)$. Then $x + by = v \cdot (m+b)$ with $1 \le v \le u$. Since $x \le s < m \le vm$, we have $by = vm + bv - x > bv$. Hence $y > v$ and $x + b \cdot (y-v) = vm \equiv 0 \pmod m$. The assumption $y - v > t$ leads to $vm > b \cdot (y-v) > bt = um - s > (u-1)\cdot m$, hence $v \ge u$, $y > t+u$, a contradiction. Thus $y - v \le t$, $0 < (x, y-v) \le (s,t)$, $x = s$, $y = t+v$, $vm = um$, $v = u$, $(x,y) = (s,t+u)$. $\diamond$

Proposition 1 *Let $m \in \mathbb{N}_1$, $b \in \mathbb{N}$. The assignment $(s,t) \mapsto (s, t+u)$ with $u = \frac{s+bt}{m}$ defines a bijection between*

(i) *the set of indecomposable solutions of $(\mathbf{A'_2})$ $s + bt \equiv 0 \pmod m$*

(ii) *and the set of indecomposable solutions of (1) $x + by \equiv 0 \pmod{m+b}$ except $(m+b, 0)$.*

Proof. By Lemma 2 the map exists and is injective, for each indecomposable solution of (1) is uniquely characterized by its first coordinate. Clearly $(m+b,0)$ is not in the image of this map. We have yet to show the surjectivity.

Let $(x, y) \in \mathbb{N}^2$ be an indecomposable solution $\neq (m + b, 0)$ of (1), say $x + by = u \cdot (m + b)$ with $u \in \mathbb{N}_1$. By Lemma 2 (i) we have

$$u = \lceil \frac{by}{m+b} \rceil < \frac{by}{m+b} + 1 < y + 1,$$

hence $u \leq y$. From $x + b \cdot (y - u) = um$ we get that $(x, y - u)$ is a solution mod m. Is it indecomposable? It is $\neq 0$, for otherwise $x = 0$, $y = u$, $bu = um + ub$, contradiction. Now assume $0 \leq (s, t) \leq (x, y - u)$ with $s + bt \equiv 0 \pmod{m}$, say $s + bt = vm$ with $0 \leq v \leq u$. Then $s + b \cdot (t + v) = v \cdot (m + b)$ and $s \leq x$, $t + v \leq y - u + v \leq y$. We conclude

$$s = x, \quad t + v = y, \quad v = u, \quad t = y - u$$

or otherwise

$$s = 0, \quad t + v = 0, \quad t = 0.$$

Thus (x, y) has $(x, y - u)$ as pre-image. $\diamond$

2 Counting the Indecomposable Solutions

For $b \in \mathbb{N}$ and $m \in \mathbb{N}_1$ let $A(m, b)$ be the number of indecomposable solutions of the congruence $(\mathbf{A_2'})$ $x + by \equiv 0 \pmod{m}$.

Note that by the corollary of Lemma 1 the number of indecomposable solutions of $(\mathbf{A_2})$ $ax + by \equiv 0 \pmod{m}$ is $A(m', b')$.

Lemma 3 (i) *$A(m, 0) = 2$ for all $m \in \mathbb{N}_1$.*

(ii) *$A(m, 1) = m + 1$ for all $m \in \mathbb{N}_1$.*

(iii) *A is periodic in its second variable: $A(m, m + b) = A(m, b)$ for all $m \in \mathbb{N}_1$ and $b \in \mathbb{N}$.*

(iv) *A is quasiperiodic in its first variable: $A(m + b, b) = 1 + A(m, b)$ for all $m \in \mathbb{N}_1$ and $b \in \mathbb{N}_1$.*

(v) *If $ab \equiv 1 \pmod{m}$, then $A(m, a) = A(m, b)$.*

Proof. (i) The indecomposable solutions are $(m, 0)$ and $(0, 1)$.

(ii) The indecomposable solutions are $(k, m - k)$ for $k = 0, \ldots, m$.

(iii) $x + by \equiv 0 \pmod{m} \Leftrightarrow x + (b + m)y \equiv 0 \pmod{m}$.

(iv) follows directly from Proposition 1.

(v) $x + ay \equiv 0 \pmod{m} \Leftrightarrow bx + bay \equiv 0 \pmod{m} \Leftrightarrow y + bx \equiv 0 \pmod{m}$. $\diamond$

The recursive formulas (iii) and (iv) allow a very efficient calculation of the table of all $A(m, b)$ from the initial conditions $A(m, 0) = 2$, see Table 1. This is the algorithm: In row r

Table 1: Numbers $A(m, b)$ of indecomposable solutions

	$b =$ 0	1	2	3	4	5	6	7	8	9	10
$m = 1$	2	2	2	2	2	2	2	2	2	2	2
2	2	3	2	3	2	3	2	3	2	3	2
3	2	4	3	2	4	3	2	4	3	2	4
4	2	5	3	3	2	5	3	3	2	5	3
5	2	6	4	4	3	2	6	4	4	3	2
6	2	7	4	3	3	3	2	7	4	3	3
7	2	8	5	4	5	4	3	2	8	5	4
8	2	9	5	5	3	4	3	3	2	9	5
9	2	10	6	4	4	6	3	4	3	2	10
10	2	11	6	5	4	3	4	5	3	3	2

- set the first entry $A(m, 0) = 2$,
- calculate the entries $A(m, 1), \ldots, A(m, m-1)$ by quasi-peridocity from the formula $A(m, b) = A(m - b, b)$,
- calculate the entries from $A(m, m)$ to the right by peridocity from the formula $A(m, b) = A(m, b - m)$,

The corresponding Python program is in Appendix A.3.

Examples We calculate some values for small parameters by paper and pencil.

- $A(3, 2) = 1 + A(1, 2) = 1 + A(1, 0) = 3$.
- $A(4, 2) = 1 + A(2, 2) = 1 + A(2, 0) = 3$.

Remark Here are some obvious general rules:

1. For $m = 2r - 1$ odd: $A(m, 2) = 1 + A(m-2, 2) = \ldots = r - 1 + A(1, 2) = r + 1$.
2. Likewise for $m = 2r$ even: $A(m, 2) = r - 1 + A(2, 2) = r + 1$.
3. $A(m, m - 1) = 1 + A(1, m - 1) = 3$ for $m \geq 2$.
4. $A(m, m - 2) = 1 + A(2, m - 2) = 4$ for odd $m \geq 3$, and $= 3$ for even $m \geq 4$.

As an easy application of these rules we improve the trivial bound $m + 1$ on the number of indecomposable solutions:

Proposition 2 *Assume that $m \geq 4$ and $b \not\equiv 1 \pmod{m}$. Then $A(m, b) \leq m - 1$.*

Proof. We may assume that $2 \le b \le m-1$, and the case $b = 2$ is settled by the rules 1 and 2. For $b \ge 3$ we get

$$A(m,b) = 1 + A(m-b,b) \le 1 + (m-b) + 1 = m + 2 - b \le m - 1.$$

$\diamond$

Corollary 1 *Assume that $m \ge 4$ and $b \not\equiv a \pmod{m}$. Then the congruence ($\mathbf{A_2}$) has at most $m-1$ indecomposable solutions.*

Proof. The corollary of Lemma 1 reduces the assertion to Proposition 2. (Note that m' might be 2 or 3, but then the weaker statement $A(m', b') \le m' + 1$ suffices.) $\diamond$

The stepwise reduction by quasi-periodicity in the examples reminds us of the Euclidean algorithm [3], and indeed:

Proposition 3 *Let $m \in \mathbb{N}_1$, $b \in \mathbb{N}$, and consider the Euclidean division chain*

$$r_0 = m,\ r_1 = b,\ ...,\ r_{i-1} = q_i r_i + r_{i+1},\ \ldots,\ r_{n-1} = q_n r_n$$

with $0 < r_n < ... < r_1$, $r_n = \gcd(m,b)$, $r_{n+1} = 0$. Furthermore let

$$\tilde{A}(m,b) = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} q_{2k+1}$$

be the sum of the quotients with odd index. Then

$$A(m,b) = \begin{cases} \tilde{A}(m,b) + 1, & \text{if } n \text{ is odd,} \\ \tilde{A}(m,b) + 2, & \text{if } n \text{ is even.} \end{cases}$$

In other words we can explicitly calculate $A(m,b)$ by the Euclidean algorithm, or, in yet other words, from the continued fraction expansion of $\frac{m}{b}$, cf. [5].

Proof. Since $m = q_1 b + r_2$ or $m = q_1 b$, Lemma 3 (iv) immediately yields

$$A(m,b) = \begin{cases} q_1 + A(r_2, b), & \text{if } n \ge 2, \\ q_1 - 1 + A(b,b) = q_1 - 1 + A(b,0) = q_1 + 1, & \text{if } n = 1. \end{cases}$$

From this the assertion follows inductively step by step: For $n \ge 3$ we have $r_1 = q_2 r_2 + r_3$, hence $A(r_2, b) = A(r_2, r_1) = A(r_2, r_3)$.

Now if $n = 2t+1$ is odd: $r_{n-2} = q_{n-1} r_{n-1} + r_n$, $r_{n-1} = q_n r_n$, hence

$$A(m,b) = q_1 + \cdots + q_{n-2} + \underbrace{A(r_{n-1}, r_n)}_{q_n + 1}.$$

And if $n = 2t$ is even

$$A(m,b) = q_1 + \cdots + q_{n-1} + \underbrace{A(r_n, 0)}_{2}.$$

$\diamond$

This algorithm is implemented by the Python program in Appendix A.4. Using it we easily compute

- $A(7,3) = 4$
- $A(20,5) = 5$
- $A(25000,753) = 37$

3 Computing the Indecomposable Solutions

Proposition 1 yields more than just the numbers of indecomposable solutions: It leads to the solutions themselves:

Theorem 1 (TINSLEY, RIEMENSCHNEIDER) *Let $m \in \mathbb{M}_2$, $b \in \mathbb{N}_1$, and let $r_0 = m$, $r_1 = b$, $\ldots$, r_n be the Euclidean division chain, $r_{i-1} = q_i r_i + r_{i+1}$ for $1 \le i \le n$. Then the first coordinates of the indecomposable solutions of $(\mathbf{A_2'})$ $x + by \equiv 0 \pmod m$ are exactly the numbers r_0 $(= m)$ and*

$$r_{2i} - j \cdot r_{2i+1} \quad \textit{for } 0 \le i \le \lfloor \frac{n-1}{2} \rfloor, \quad 1 \le j \le q_{2i+1},$$

and additionally 0 if n is even. The corresponding second coordinates y derive from the first coordinates x as the minimum values ≥ 0 such that $m | x + by$ (except for $x = 0$).

Proof. The indecomposable solutions of $(\mathbf{A_2'})$ are of two different types:

1. $(m, 0)$,
2. $(s, t+u)$ where (s,t) is an indecomposable solution of $s + bt \equiv 0 \pmod{m-b}$ and $u = (s+bt)/(m-b)$.

After q_1 steps of this kind we may state: The indecomposable solutions of $x + r_1 y \equiv 0 \pmod{r_0}$ are of two different types:

1. $(x, *)$ with $x = r_0, r_0 - r_1, \ldots, r_0 - q_1 r_1 = r_2$,
2. $(s, *)$ where (s,t) is an indecomposable solution of $s + r_1 t \equiv 0 \pmod{r_2}$, or equivalently, of $s + r_3 t \equiv 0 \pmod{r_2}$.

Note that we neglect the values of the y-coordinates—they are calculated at the end of the algorithm, see the last sentence of the theorem.

In the i-th step of the procedure we have the analogous alternative: The indecomposable solutions of $x + r_{2i-1}y \equiv 0 \pmod{r_{2i-2}}$ are of two different types:

1. $(x, *)$ with $x = r_{2i-2}, r_{2i-2} - r_{2i-1}, \ldots, r_{2i-2} - q_{2i-1}r_{2i-1} = r_{2i}$,
2. $(s, *)$ where (s, t) is an indecomposable solution of $s + r_{2i+1}t \equiv 0 \pmod{r_{2i}}$,

as long as $2i + 1 \leq n$. If $2i = n$, then this alternative has to be replaced by

- $(x, *)$ with $x = r_n, 0$.

If $2i + 1 = n$ then for the second type of the alternative we have to determine the indecomposable solutions of $s + r_n t \equiv 0 \pmod{r_{n-1}}$, and since $r_n | r_{n-1}$ the x-coordinates of the indecomposable solutions are

- $x = r_{n-1}, r_{n-1} - r_n, \ldots, r_{n-1} - q_n r_n = 0$.

This completes the proof. $\diamond$

Note that the x-coordinates of the indecomposable solutions form the strictly decreasing sequence

$$r_0,\ r_0 - r_1,\ \ldots,\ r_0 - q_1 r_1 = r_2,\ r_2 - r_3,\ \ldots,\ r_2 - q_3 r_3 = r_4,\ \ldots,\ 0.$$

4 Algorithmic Solution

The following algorithm finds all indecomposable solutions of $(\mathbf{A_2'})$:

Initialization Start with the list `xlist` $= [m]$ of x-values, and set $r = m$, $s = b \bmod m$.

While $s > 0$: $q = \lfloor \frac{r}{s} \rfloor$.

- For $i = 1, \ldots, q$: set $r = r - s$, append r to `xlist`.
- If $r > 0$ set $s = s \bmod r$, else set $s = 0$.

Finalization If $r > 0$ append 0 to `xlist`.

Complete result For each $x \in$ `xlist`:

- If $x > 0$: compute $y = \min\{t \in \mathbb{N} \mid m | x + bt\}$.
- If $x = 0$: compute $y = \min\{t \in \mathbb{N}_1 \mid m | bt\}$.

The Python program in Appendix A.5 gives all the indecomposable solutions of $(\mathbf{A_2'})$. Here are some sample results

- For $m = 7$, $b = 3$: `[[7,0], [4,1], [1,2], [0,7]]`

- For $m = 20$, $b = 5$: `[[20,0], [15,1], [10,2], [5,3], [0,4]]`
- For $m = 25000$, $b = 753$: `[[25000,0],[24247,1],[23494,2],[22741,3],[21988,4],[21235,5],[20482,6],[19729,7],[18976,8],[18223,9],[17470,10],[16717,11],[15964,12],[15211,13],[14458,14],[13705,15],[12952,16],[12199,17],[11446,18],[10693,19],[9940,20],[9187,21],[8434,22],[7681,23],[6928,24],[6175,25],[5422,26],[4669,27],[3916,28],[3163,29],[2410,30],[1657,31],[904,32],[151,33],[2,166],[1,12583],[0,25000]]`

Taking all the pieces together we get an algorithm that finds all indecomposable solutions of $(\mathbf{A_2})$ $ax + by \equiv 0 \pmod m$:

Reduction phase Compute $d = \gcd(a, m)$ as well as the coefficients of the linear combination $d = ca + km$ by the extended Euclidean algorithm (Appendix A.1).

- Set $m' = m/d$ and $a' = a/d$.
- Set $b' = bc \bmod m'$.

x-values Compute the list `xlist` of the x-coordinates of all indecomposable solutions of $(\mathbf{A_2'})$ $x + b'y \equiv 0 \pmod m$ (Appendix A.2).

y-values For each $x \in$ `xlist` compute the corresponding y-coordinate by the formula

- If $x > 0$: compute $y = \min\{t \in \mathbb{N} \mid m|ax + bt\}$.
- If $x = 0$: compute $y = \min\{t \in \mathbb{N}_1 \mid m|bt\}$.

The Python code is in Appendix A.6. Here is a sample result:

- $2x + 3y \equiv 0 \pmod 7$: `[[7,0], [2,1], [1,4], [0,7]]`

5 Extremal Solutions

Theorem 2 *Assume $m \in \mathbb{N}_3$, $a, b \in \mathbb{N}$, and $a \not\equiv b \pmod m$. Let $(x, y) \in \mathbb{N}^2$ be an indecomposable solution of $(\mathbf{A_2})$ with $x \neq 0$ and $y \neq 0$. Then:*

(i) $x + y \leq m - 1$.

(ii) *If $x + y = m - 1$, then one of the following statements is true:*

- *$x = m - 2$, $y = 1$, $\gcd(m, a) = 1$, and if c is the $\bmod\, m$-inverse of a (i. e. $ca \equiv 1 \pmod m$), then $cb \equiv 2 \pmod m$.*
- *$x = 1$, $y = m - 2$, $\gcd(m, b) = 1$, and if c is the $\bmod\, m$-inverse of b, then $ca \equiv 2 \pmod m$.*

Remarks For $m = 2$, $a = b = 1$, the solution $(1, 1)$ is a counterexample for (i).

The two items in (ii) describe the same set of cases, only with the denotations of a and b interchanged. The second statements for both cases of (ii) follow directly, since (for instance) $0 \equiv c\,(ax + by) \equiv m - 2 + cb \pmod m$.

Definition (For $m \in \mathbb{N}_3$) A solution (x, y) of $(\mathbf{A_2})$ (with $a \not\equiv b \pmod{m}$) is called **extremal** if it is indecomposable, $x \neq 0$, $y \neq 0$, and $x + y = m - 1$.

Example If $a = 1$, $b = 2$, then $(m-2, 1)$ is an extremal solution. This is essentially the only example: Theorem 2 tells us that by the action of the mutliplicative group mod m we get all extremal solutions for a fixed module m and varying coefficients a and b.

Remark If $a \equiv b \pmod{m}$ the situation is different: In the case where $\gcd(m, a) = 1$ the indecomposable solutions are all the pairs (x, y) with $x + y = m$.

Corollary 1 *The congruence* $(\mathbf{A_2})$ *admits an extremal solution if and only if a is coprime with m and* $b \equiv 2a \pmod{m}$, *or b is coprime with m and* $a \equiv 2b \pmod{m}$. *This extremal solution,* $(m-2, 1)$ *or* $(1, m-2)$, *is unique.*

Let us consider the more general linear congruence for integer vectors $x \in \mathbb{N}^m$

$$(\mathbf{C}'_m) \qquad 0 \cdot x_0 + 1 \cdot x_1 + \cdots + (m-1) \cdot x_{m-1} \equiv 0 \pmod{m}.$$

The support of a solution x is the set of indices i with $x_i \neq 0$. Clearly the indecomposable solutions with one-element support are given by the remark in the introduction:

> For each i let x_i be the minimal integer > 0 with $m|ix_i$. Then $(0, \ldots, x_i, \ldots, 0)$ is an indecomposable solution. If m and i are coprime, then $x_i = m$.

Thus there are exactly $\varphi(m)$ indecomposable solutions with one-element support and $\|x\|_1 = x_0 + \cdots + x_{m-1} = m$ (where φ is the Euler function). Theorem 2 provides a nontrivial analogue:

Corollary 2 *The number of solutions x of* $(\mathbf{C}'_m)$ *with two-element support and* $\|x\|_1 = m - 1$ *is* $\varphi(m)$.

We prove Theorem 2 by induction on m and assume without loss of generality that $a, b \in \{0, \ldots, m-1\}$. Let $d = \gcd(m, a)$, $d' = \gcd(d, b)$, $d = d'e$.

If $m = 3$, then the case $d \neq 1$ occurs only for $a = 0$. Then $(1, 0)$ is an indecomposable solution, and any other one has the form $(0, y)$. Therefore the assumption $x \neq 0$ and $y \neq 0$ enforces $d = 1$, $a = 1$ or 2. By symmetry also $b = 1$ or 2, hence $a = 1$, $b = 2$ or $a = 2$, $b = 1$. In both cases the indecomposable solutions are $(3, 0)$, $(1, 1)$, $(0, 3)$. Hence (i) and (ii) are obviously true.

Now we assume that $m \geq 4$.

Case I, $d \neq 1$. Then by Lemma 1 (i) we have $e|y$, and (x, y') is an indecomposable solution of $a's + b't \equiv 0 \pmod{m'}$ where $y' = y/e$, $a' = a/d$, $b' = b/d'$, and $m' = m/d$.

Case Ia, $m' \geq 3$. Since $m' < m$ the induction hypothesis yields

$$x + \frac{y}{e} \leq \frac{m}{d} - 1, \quad x + y \leq dx + d'y \leq m - d < m - 1.$$

Thus (i) is true, and (ii) is void.

Case Ib, $m' = 2$, $m = 2d$. Then depending on a' mod 2 and b' mod 2, the solution vector (s, t) is one of $(1, 0)$, $(2, 0)$, $(1, 1)$, $(0, 1)$, $(0, 2)$. The condition $x \neq 0$, $y \neq 0$ is met only for $(s, t) = (1, 1)$. Then $x = 1$, $y = e$,

$$x + y = 1 + e \leq d - 1 + d = m - 1,$$

hence (i) is proved, and $x + y = m - 1$ implies that $d - 1 = 1$ and $e = d$, that is $d = 2$, $m = 4$, and $y = 2$, as required for (ii).

Case Ic, $m' = 1$. Then $d = m$, $d|a$, hence $a = 0$. Then the indecomposable solutions have the form $(1, 0)$ or $(0, y)$ and violate the conditions of the theorem.

Case II, $d = 1$. By Lemma 1 (ii) we may assume that $a = 1$ (and $b \neq 1$). We may also assume that $b \neq 0$, hence $2 \leq b \leq m - 1$:

> If $b = 0$, then $(0, 1)$ is an indecomposable solution, and any other one has the form $(x, 0)$. Thus there is nothing to prove.

We look at the proof of Theorem 1: Since (x, y) is not the solution $(m, 0)$, it has the form $(s, t + u)$ where (s, t) is an indecomposable solution of $s + bt \equiv 0 \pmod{m - b}$ with $s = x \neq 0$, and

$$u = \frac{s + bt}{m - b} \leq 1 + \frac{bt}{m - b}.$$

Case IIa. If $(s, t) = (m - b, 0)$, then $u = 1$ and $(x, y) = (m - b, 1)$,

$$x + y = m - b + 1 \leq m - 1,$$

with equality if and only if $b = 2$. We have detected the solution $(m - 2, 1)$ and are done.

> Otherwise $t \geq 1$ and $s < m - b$, hence
>
> $$u = \frac{s + bt}{m - b} < \frac{(m - b) + b(m - b)}{m - b} = 1 + b, \quad \text{thus } u \leq b.$$
>
> Moreover $t < m - b$, in particular $u < b + s/(m - b)$. We consider four more subcases:

Case IIb. If $m - b \geq 3$ and $b \not\equiv 1 \pmod{m - b}$, then the induction hypothesis applies and yields $s + t \leq m - b - 1$. Hence

$$x + y = s + t + u \leq m - b - 1 + b = m - 1,$$

and (i) is proved. Equality implies $u = b$ and $s + t = m - b - 1$. By induction we have one of the following two situations:

1. $s = 1$, $t = m - b - 2$, hence $x = 1$, $y = t + u = m - 2$, as required for (ii).
2. $s = m - b - 2$, $t = 1$, hence $x = m - b - 2$, $y = t + u = b + 1$. Then

$$b = u < 1 + \frac{bt}{m - b} = 1 + \frac{b}{m - b} \leq 1 + \frac{b}{3},$$

This implies $3b < 3 + b$, $2b < 3$, $b \leq 1$, contradiction.

Case IIc. If $m-b \geq 3$ and $b \equiv 1 \pmod{m-b}$, then (s,t) is an indecomposable solution of $s+t \equiv 0 \pmod{m-b}$ with $s \neq 0$. Hence $t = m-b-s$ and

$$u = \frac{s+bt}{m-b} = \frac{s+b\,(m-b-s)}{m-b} = b + \frac{(1-b)\,s}{m-b} \leq b.$$

From $u = b$ the contradiction $(1-b)\,s/(m-b) = 0$, hence $b = 1$, would result. Therefore $u \leq b-1$, and

$$x+y = s+t+u \leq m-b+b-1 = m-1,$$

and (i) is proved.

Equality enforces $u = b-1$,

$$\frac{(1-b)\,s}{m-b} = -1, \quad s = \frac{m-b}{b-1},$$

hence $m-b \geq b-1$, $m+1 \geq 2b$,

$$b \leq \frac{m+1}{2}, \quad m-b \geq \frac{m-1}{2}.$$

This is compatible with $b \equiv 1 \pmod{m-b}$ if and only if $b = (m+1)/2$ (and m odd). Then $s = (m-b)/(b-1) = 1$, $t = m-b-1$,

$$x = 1, \quad y = m-2,$$

as required for (ii).

Case IId. Assume $m-b = 2$. Since Case IIa is done, $(x,y) = (s,t+u)$ where (s,t) an indecomposable solution of $s+bt \equiv 0 \pmod 2$, with $t \geq 1$ and $u = (s+bt)/2$.

> Assume that b is even. Then (s,t) is one of $(2,0)$ or $(0,1)$, contradicting $t \geq 1$ or $s = x \neq 0$.

Therefore b is odd, and also m is odd and (s,t) is one of $(2,0)$ or $(1,1)$ or $(0,2)$, hence $(s,t) = (1,1)$,

$$u = \frac{b+1}{2} = \frac{m-1}{2}, \quad x = 1, \quad y = t+u = \frac{m+1}{2},$$

$$x+y = \frac{m+3}{2} \leq m-1,$$

the letter inequality since $m \geq 5$ ($m \geq 4$ and odd). This proves (i).

Assertion (ii) is void for $m \geq 7$. For $m = 5$ the equality $x+y = m-1 = 4$ enforces

$$x = 1, \quad y = 3 = m-2,$$

as required for (ii).

Case IIe. If $m-b = 1$, then $b = m-1$, and

$$x+by \equiv 0 \pmod b \quad \Longleftrightarrow \quad x \equiv y \pmod b.$$

The indecomposable solutions are $(m,0)$, $(1,1)$, $(0,m)$. Therefore (i) is obvious, and (ii) is void except for $m = 3$, where it is true.

The proof of Theorem 2 is complete.

A Python Code

A.1 Extended Euclidean Algorithm

```
def eEuclid(a,b):
  """Compute the gcd d of two integers a and b together with
  integer coefficients x and y such that d = ax + by.
  Ouput the triple [d,x,y]."""
# Initialization
  if a < 0:
    r0 = -a
    v = -1    # keep sign
  else:
    r0 = a
    v = 1
  if b < 0:
    r1 = -b
    w = -1    # keep sign
  else:
    r1 = b
    w = 1
  x0 = 1
  x1 = 0
  y0 = 0
  y1 = 1
# Extended division chain
  while r1 > 0:
    q = r0//r1
    r = r0 - q * r1
    x = x0 - q* x1
    y = y0 - q * y1
# Here we have r0 = |a|*x0+|b|*y0, r1 = |a|*x1+|b|*y1, r = |a|*x+|b|*y.
    r0 = r1
    r1 = r
    x0 = x1
    x1 = x
    y0 = y1
    y1 = y
# Finalization
  d = r0
  x = v * x0
  y = w * y0
  return [d,x,y]
```

A.2 Get the List of x-values for $(\mathbf{A_2'})$

```
def a2prime(m,b):
  """Compute the list of all x-values of indecomposable solutions of
  x + by = 0 (mod m)."""
  xlist = [m]
  r = m
  s = b % m
  while s > 0:
    q = r // s
    for i in range(q):
      r = r-s
      xlist.append(r)
    if r > 0:
      s = s % r
    else:
      s = 0
  if r > 0:
    xlist.append(0)
  return xlist
```

A.3 Compute the Table of $A(m, b)$

In this program, as well as in the following ones, we access the command line parameters `sys.argv` by including the line `import sys`.

```
r = int(sys.argv[1])  # number of rows
s = int(sys.argv[2])  # number of columns
actlst = [2]*(s+1)    # worklist for actual row
A = [[], actlst]      # dummy row 0 plus first row
for m in range(2,r+1):
  actlst = actlst[0:] # generate new copy
  actlst[0] = 2
  for b in range (1,m):
    actlst[b] = 1 + A[m-b][b] # quasi-periodicity
  for b in range (m,s+1):
    actlst[b] = actlst[b-m] # periodicity
  A.append(actlst)
del A[0]              # remove dummy row
print(A)
```

A.4 Compute $A(m, b)$ Directly

```
m = int(sys.argv[1])    # module
b = int(sys.argv[2])    # coefficient
r = m
s = b%m
sum = 1
i = 0
while s > 0:   # Euclidean step
  i += 1
  q = r//s
  t = r%s
  if i%2 ==1:  # i is odd
    sum += q
  r = s
  s = t
if i%2 == 0:   # i is even
  sum += 1
print("A(m,b):", sum)
```

A.5 Solve ($\mathbf{A}_2'$)

```
m = int(sys.argv[1]) # module
b = int(sys.argv[2]) # coefficient
xlist = [m]          # list of x-values
r = m
s = b % m
while s > 0:
  q = r // s
  for i in range(q):
    r = r-s
    xlist.append(r)
  if r > 0:
    s = s % r
  else:
    s = 0
if r > 0:
  xlist.append(0)
xylist = []          # list of solution pairs
for x in xlist:
  go_on = True
  if x == 0:
    y = 1
  else:
    y = 0
  while go_on:
    if (x + b*y) % m == 0:
      y = t
      go_on = False
    else:
      y += 1
  xylist.append([x,y])
print(xylist)
```

A.6 Solve $(\mathbf{A_2})$

```
m = int(sys.argv[1])
a = int(sys.argv[2])
b = int(sys.argv[3])
gcd = eEuclid(a,m)
dprime = eEuclid(d,b)[0]
c = gcd[1]
mprime = m//d
aprime = a//d
bprime = c * ((b//dprime) % mprime)

xlist = a2prime(mprime,bprime)
xylist = []
for x in xlist:
  go_on = True
  if x == 0:
    y = 1
  else:
    y = 0
  while go_on:
    if (a*x + b*y) % m == 0:
      go_on = False
    else:
      y += 1
  xylist.append([x,y])
print(xylist)
```

References

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

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

[3] K. Pommerening: The Euclidean algorithm. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/Euclid.pdf`

[4] K. Pommerening: The indecomposable solutions of linear congruences. (in preparation) Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/LinCong.pdf`

[5] O. Riemenschneider: Deformationen von Quotientensingularitäten (nach zyklischen Gruppen). Math. Ann. 209 (1974), 211–248.

[6] O. Riemenschneider: Die Invarianten der endlichen Untergruppen von $GL(2, \mathbb{C})$. Math. Z. 153 (1977), 37–50.

[7] M. F. Tinsley: Permanents of cyclic matrices. Pacific J. Math. 10 (1960), 1067–1082.