Irish Math. Soc. Bulletin
Number 96, Winter 2025, 63–67
ISSN 0791-5578

Finding Small Solutions of Bivariate Linear Congruences

PETROULA DOSPRA

Abstract. In this note, we propose an algorithm for computing all solutions of small size of a bivariate linear congruence.

1. Introduction

Let $a_1, \ldots, a_k, b, n \in \mathbb{Z}$ with $n \geq 1$. A *linear congruence* in the unknowns $x_1, \ldots, x_k$ is an expression of the form

$$a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}.$$

An ordered k-tuple of integers $(x_1, \ldots, x_k)$ that satisfies this congruence is called a *solution.* These solutions are often considered under additional constraints, such as $\gcd(x_i, n) = t_i$ for $1 \leq i \leq k$, where $t_1, \ldots, t_k$ are given positive divisors of n. The number of solutions subject to such conditions has been studied by several authors (see [1]). Moreover, small solutions of linear homogeneous congruences and systems have been analysed, with many results extended to number fields (see [2]).

In this note, we focus on solutions of small size to non-homogeneous bivariate linear congruences and describe an algorithm for their computation. Notably, the private key and ephemeral key in several digital signature schemes correspond to solutions of such congruences (see [3, Section 11.5]). We prove the following result:

Theorem 1. *Let q be an odd prime number, and let $A, B \in \{2, \ldots, (q-1)/2\}$. Let μ and ν be positive integers such that $\mu \leq A/2$ and $\nu < q/(2A)$. Consider the bivariate linear congruence*

$$y + Ax + B \equiv 0 \pmod{q}. \tag{1}$$

Then, the number of solutions (x, y) satisfying the bounds

$$|x| \leq \mu \left\lfloor \frac{q}{A} \right\rfloor \quad \textit{and} \quad |y| \leq \nu A$$

is at most $(2\mu+1)(2\mu+2\nu+1)$. Moreover, all such solutions can be computed in time $O\big(\mu(\mu+\nu)(\log q)^2\big)$ bit operations.

The idea of the proof is to find a "small" list of pairs and select those that satisfy the given bounds. Note that the smaller the quantities μ and ν are, the more efficiently the solutions of the linear congruence that satisfy the given constraints can be calculated.

Let a, $n \in \mathbb{Z}$ and $n > 1$. We denote the remainder when a is divided by n by '$a \bmod n$'.

The paper is organized as follows. Section 2 presents the proof of Theorem 1. In Section 3, we describe an algorithm, based on Theorem 1, that computes efficiently all "small-size" solutions of the congruence (1). Finally, Section 4 provides two examples illustrating the application of this algorithm.

2020 *Mathematics Subject Classification.* 11Y16, 11A07.
Key words and phrases. Bivariate congruences, small solutions, elementary number theory.
Received on 12 July 2025, revised on 12 October 2025.
DOI: 10.33232/BIMS.0096.63.67.

2. Proof of Theorem 1

Let x_0, $y_0 \in \mathbb{Z}$ satisfy the bounds

$$|x_0| \leq \mu \left\lfloor \frac{q}{A} \right\rfloor \quad \text{and} \quad |y_0| \leq \nu A,$$

and suppose they satisfy the congruence $y_0 + Ax_0 + B \equiv 0 \pmod{q}$. Then, we have the following bound on the absolute value:

$$|y_0 + Ax_0 + B| \leq |y_0| + A|x_0| + B < \frac{q}{2} + \mu q + \frac{q}{2} = (\mu + 1)q.$$

Since q divides $y_0 + Ax_0 + B$, it follows that

$$y_0 + Ax_0 + B = c_1 q, \tag{2}$$

where $c_1 \in \{0, \pm 1, \pm 2, \ldots, \pm \mu\}$.

Next, by Euclidean division, we have $q = Au + v$, where

$$u = \left\lfloor \frac{q}{A} \right\rfloor \quad \text{and} \quad 0 < v < A.$$

This implies the congruence $-Au \equiv v \pmod{q}$.

Multiplying Equation (2) by $-u$ yields

$$-uy_0 + vx_0 + C \equiv 0 \pmod{q},$$

where

$$-uB = -Kq + C \text{ and } 0 \leq C < q. \tag{3}$$

Furthermore, we can bound the absolute value:

$$|-uy_0 + vx_0 + C| \leq u|y_0| + v|x_0| + C < uA\nu + \mu q + q \leq (\nu + \mu + 1)q.$$

Since q divides $-uy_0 + vx_0 + C$, we deduce that

$$-uy_0 + vx_0 + C = c_2 q, \tag{4}$$

with $c_2 \in \{0, \pm 1, \pm 2, \ldots, \pm(\nu + \mu)\}$.

The Equations (2) and (4) constitute a linear system in the unknowns x_0 and y_0. Solving this system, we obtain

$$x_0 = c_1 u + c_2 - \frac{uB + C}{q} \quad \text{and} \quad y_0 = c_1 v - c_2 A + \frac{CA - vB}{q}.$$

Since, by (3), $-uB = -Kq + C$, we have

$$K = \frac{uB + C}{q} = -\left\lfloor \frac{-uB}{q} \right\rfloor.$$

Using this fact, we rewrite the second fraction as

$$\frac{CA - vB}{q} = AK - B.$$

Hence, the solutions can be expressed in the simpler form

$$x_0 = c_1 u + c_2 - K, \quad y_0 = c_1 v - c_2 A + AK - B, \tag{5}$$

where $c_1 \in \{0, \pm 1, \pm 2, \ldots, \pm \mu\}$, $c_2 \in \{0, \pm 1, \pm 2, \ldots, \pm(\nu + \mu)\}$, u and v are the quotient and the remainder of the division of q by A, and $K = -\lfloor (-uB)/q \rfloor$.

Conversely, one can verify that any pair (x_0, y_0) of this form satisfies the original congruence (1). Since

$$c_1 \in \{-\mu, \ldots, 0, \ldots, \mu\} \quad \text{and} \quad c_2 \in \{-(\nu + \mu), \ldots, 0, \ldots, \nu + \mu\},$$

there are at most $(2\mu + 1)(2\mu + 2\nu + 1)$ such solutions satisfying the prescribed bounds on $|x_0|$ and $|y_0|$.

Finally, by [4, Section 3.3], the computation of u, v, K, and hence of the solutions x_0, y_0, can be performed in $O(\mu(\mu+\nu)(\log q)^2)$ bit operations.

3. The Algorithm

The proof of Theorem 1 leads to the following algorithm for computing solutions to the congruence (1) that satisfy the given bounds.

Algorithm: SOLVE-CONGRUENCE

Input: An odd prime q, A, $B \in \{2, \ldots, (q-1)/2\}$, and positive integers μ, ν with $\mu \leq A/2$ and $\nu < q/(2A)$.

Output: The solutions (x, y) of Congruence (1) with $|x| \leq \mu \lfloor q/A \rfloor$ and $|y| < \nu A$.

(1) Compute integers u and v satisfying $q = Au + v$ and $0 \leq v < A$.

(2) Compute positive integers K and C such that $-uB = -Kq + C$ and $0 < C < q$.

(3) For each $i \in \{0, \pm 1, \ldots, \pm \mu\}$, determine all $j \in \{0, \pm 1, \ldots, \pm(\mu+\nu)\}$ such that the quantities

$$x_{i,j} = iu + j - K \quad \text{and} \quad y_{i,j} = iv - jA + AK - B$$

satisfy the inequalities

$$|x_{i,j}| \leq \mu \left\lfloor \frac{q}{A} \right\rfloor \quad \text{and} \quad |y_{i,j}| < \nu A.$$

(4) Output all pairs $(x_{i,j}, y_{i,j})$ that satisfy the inequalities specified in the previous step.

Remark 1. If the integers μ and ν are sufficiently small – if, for instance, μ, ν are both less than $(\log q)^2$ – then the above algorithm runs in polynomial time and is therefore practical for computation.

4. Examples

In this section, we work through two examples illustrating the use of the algorithm SOLVE-CONGRUENCE. We remark that, in these examples, the number of solutions satisfying the given bounds is significantly smaller than the upper bound mentioned in Theorem 1.

Example 1. Consider the prime $q = 1073741827$. We shall compute the solutions of the congruence

$$y + 131073x + 25277021 \equiv 0 \pmod{q} \tag{6}$$

with

$$|x| \leq 8100 \quad \text{and} \quad |y| \leq 12000.$$

We have $A = 131073$, $B = 25277021$, and $\lfloor q/A \rfloor = 8191$. We choose parameters $\mu = \nu = 1$. Thus, we find integers $u = 8191$ and $v = 122884$ such that $q = Au + v$ and $0 < v < A$. Next, we compute $K = 193$ and $C = 188093600$ such that $-uB = -Kq + C$. Finally, we compute $AK - B = 20068$.

We now consider solutions to the Congruence (6) of the form $(x_{i,j}, y_{i,j})$ $(i = 0, \pm 1,\ j = 0, \pm 1, \pm 2)$, where

$$x_{i,j} = i8191 + j - 193, \quad \text{and} \quad y_{i,j} = i122884 - j131073 + 20068.$$

We check which of these pairs satisfy the required bounds. For $i = -1, 0$, the values $y_{i,j}$ $(j = -2, -1, 0, 1, 2)$ do not meet the given bound. For $i = 1$, only the pair $(x_1, y_1) = (7999, 11879)$ satisfies the bounds. Therefore, the only solution to the congruence (6) within the specified bounds is $(7999, 11879)$.

Example 2. Consider the linear bivariate congruence

$$y + 149x + 475 \equiv 0 \pmod{1013}. \tag{7}$$

We shall compute the solutions of the above congruences $(x, y) \in \mathbb{Z}^2$ with $|x| \leq 90$ and $|y| \leq 149$.

The integer $q = 1013$ is a prime number. We are given $A = 149$, $B = 475$, and observe that $\lfloor q/A \rfloor = 6$. We choose parameters $\mu = 15$ and $\nu = 1$. According to the algorithm, we first determine integers $u = 6$ and $v = 119$ such that $q = Au + v$, with $0 \leq v < A$. Next, we compute integers $K = 3$ and $C = 189$ satisfying $-uB = -Kq + C$, with $0 \leq C < q$. Then, we obtain the solutions

$$(x_{i,j}, y_{i,j}) \quad (i = 0, \pm 1, \ldots, \pm 15,\ j = 0, \pm 1, \ldots, \pm 16)$$

of Congruence (7), where

$$x_{i,j} = i6 + j - 3 \quad \text{and} \quad y_{i,j} = i119 - j149 - 28.$$

For $i = 0$, we find that only $j = 0$ and $j = -1$ yield values of $|y_{0,j}| \leq 149$. Specifically, the corresponding solutions are:

$$(x_{0,0}, y_{0,0}) = (-3, -28), \quad (x_{0,-1}, y_{0,-1}) = (-4, 121),$$

both of which satisfy the imposed upper bounds.

For $j = 0$, we find that only $i = 1$ and $i = -1$, other than $i = 0$, yield values of $|y_{i,0}| \leq 149$. Specifically, the corresponding solutions are:

$$(x_{1,0}, y_{1,0}) = (3, 91), \quad (x_{-1,0}, y_{-1,0}) = (-9, -147).$$

If $i > 0$ and $j < 0$, then

$$y_{i,j} = 119i - 149j - 28 > 149,$$

violating the bound on $y_{i,j}$. Similarly, if $i < 0$ and $j > 0$, then

$$y_{i,j} = 119i - 149j - 28 < -149,$$

which also violates the bound. Therefore, for any $i \neq 0$ and $j \neq 0$, i and j must be of the same sign. Accordingly, for each $i = \pm 1, \ldots, \pm 15$, we examine values of $j = \pm 1, \ldots, \pm 16$ with the same sign to determine whether the corresponding pairs $(x_{i,j}, y_{i,j})$ satisfy the given bounds and solve Congruence (7). We have 59 such solutions that are listed in the table overleaf. Note that this number is considerably smaller than the bound 1023 that is provided by Theorem 1.

References

[1] K. Bibak, B. M. Kapron, V. Srinivasan, R. Tauraso, L. Tóth, Restricted linear congruences. *J. Number Theory* 171, (2017) 128–144.

[2] E. B. Burger, Small solutions to systems of linear congruences over number fields. *Rocky Mt. J. Math.* 26, No. 3, (1996) 875–888.

[3] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of applied cryptography.* CRC Press Series on Discrete Mathematics and its Applications. Boca Raton, FL: CRC Press 1997.

[4] V. Shoup, *A Computational Introduction to Number Theory and Algebra,* Second Edition, Cambridge University Press 2008.

i	j	$(x_{i,j}, y_{i,j})$
-15	-12	$(-105, -25)$
-15	-13	$(-106, 124)$
-14	-11	$(-98, -55)$
-14	-12	$(-99, 94)$
-13	-10	$(-91, -85)$
-13	-11	$(-92, 64)$
-12	-9	$(-84, -115)$
-12	-10	$(-85, 34)$
-11	-8	$(-77, -145)$
-11	-9	$(-78, 4)$
-10	-8	$(-71, -26)$
-10	-9	$(-72, 123)$
-9	-7	$(-64, 56)$
-9	-8	$(-65, 93)$
-8	-6	$(-57, -86)$
-8	-7	$(-58, 63)$
-7	-5	$(-50, -116)$
-7	-6	$(-51, 33)$
-6	-4	$(-43, -146)$
-6	-5	$(-44, 3)$
-5	-4	$(-37, -27)$
-5	-5	$(-38, 122)$
-4	-3	$(-30, 57)$
-4	-4	$(-31, 92)$
-3	-2	$(-23, -87)$
-3	-3	$(-24, 62)$
-2	-1	$(-16, -117)$
-2	-2	$(-17, 32)$
-1	0	$(-9, -147)$
-1	-1	$(-10, 2)$
0	-1	$(-4, 121)$
0	0	$(-3, -28)$
1	0	$(3, 91)$
1	1	$(4, -58)$
2	1	$(10, 61)$
2	2	$(11, -88)$
3	2	$(17, 31)$
3	3	$(18, -118)$
4	3	$(24, 1)$
4	4	$(25, -148)$
5	3	$(30, 120)$
5	4	$(31, -29)$
6	4	$(37, 90)$
6	5	$(38, -59)$
7	5	$(44, 60)$
7	6	$(45, -89)$
8	6	$(51, 30)$
8	7	$(52, -119)$
9	6	$(57, 149)$
9	7	$(58, 0)$
9	8	$(59, -149)$
10	7	$(64, 119)$
10	8	$(65, -30)$
11	8	$(71, 89)$
11	9	$(72, -60)$
12	9	$(78, 59)$
12	10	$(79, -90)$
13	10	$(85, 29)$
13	11	$(86, -120)$

Petroula Dospra is a graduate of the Department of Mathematics of the Aristotle University of Thessaloniki. In 2008 she received her Master's Degree in Theoretical Mathematics from the Department of Mathematics of the Aristotle University of Thessaloniki and in 2015 she was awarded a Ph.D. in Mathematics from the Agricultural University of Athens. Her research interests focus mainly on Computational Mathematics and especially on Geometry and Algebra of Quaternions.

School of Science and Technology, Hellenic Open University, 11 Sahtouri Street, 26 222 Patras, Greece.
E-mail address: petroula.dospra@gmail.com