Journal of Algebra, Number Theory: Advances and Applications
Volume 13, Number 2, 2015, Pages 53-64

ON THE LATTICE SOLUTIONS OF THE CONGRUENCE $bx \equiv cy \pmod{p}$

ANWAR AYYAD

Department of Mathematics
AL-Azhar University
P. O. Box 1277
Gaza Strip
Palestine
e-mail: anwarayyad@yahoo.com

Abstract

Let $\mathcal{B}$ be arbitrary box of size B subset of $\mathbb{R} \times \mathbb{R}$ and V be the set of lattice solutions of the congruence $bx \equiv cy \pmod{p}$ in $\mathbb{Z} \times \mathbb{Z}$, where p is prime number and $1 \leq b, c < p$. We obtain a condition on the size B, so that $\mathcal{B} \cap V$ is empty intersection, and we also find a condition on B in order for $\mathcal{B}$ to contains a point of V.

1. Introduction

For prime p and $1 \leq b, c < p$, let V be the set of all solutions of the congruence $bx \equiv cy \pmod{p}$ in $\mathbb{Z}^2$, and let $\mathcal{B}$ be arbitrary box of size B in the XY-plane. We obtain an upper bound on the size B so that $\mathcal{B} \cap V$ is empty, and also we find a lower bound on B in order for $\mathcal{B}$ to contain a point of V.

2010 Mathematics Subject Classification: Primary 11D79.
Keywords and phrases: congruences, solutions.
Received April 16, 2015

© 2015 Scientific Advances Publishers

For $1 \leq c < b < p$ and $\frac{b^2 - c^2}{d^2} < p \,(\mathrm{mod}\; p)$, where $d = (b, c)$, we prove any box of size

$$B > \frac{dp}{b+c} + 2\left(\frac{c}{d}\right), \tag{1}$$

contains a point of V. For $c = 1$ and $1 < b < \sqrt{p}$, we prove the bound in (1), $B > \frac{p}{b+1} + 2$ is best possible in the sense that there exist a box of size $B = \frac{p}{b+1}$ does not meet V.

If $1 \leq c < b < p$ with $(b, c) = 1$ and $y_0 < \frac{b}{2}$ any box of size

$$B > \frac{p}{x_0(b+c) - p} + 2x_0, \tag{2}$$

contains a point of V, where (x_0, y_0) is the first positive solution on the line $L := bx - cy = p$. For $c = 1, b$ in the interval $(\frac{p}{2}, \frac{2p}{3})$, we prove the bound in (2) is best possible.

For $1 \leq c < b < p$ with $(b, c) = 1$ and $y_0 > \frac{b}{2}$ any box of size

$$B > \frac{p}{x_0 - y_0 + b - c} + 2(x_0 - c) \tag{3}$$

meets V. For $c = 1$ and b in the interval $(\frac{2p}{3}, p)$, we prove the bound in (3) is best possible.

Theorem 1. *For $1 \leq b, c < p$, the congruence $bx \equiv cy \,(\mathrm{mod}\; p)$ has a non-zero solution $\boldsymbol{x} = (x_0, y_0)$ with $\|\boldsymbol{x}\| = \max(x_0, y_0) < \sqrt{p}$.*

Proof. We look at the set of solutions of $bx \equiv cy \,(\mathrm{mod}\; p)$ as a lattice points on the lines defined by $L_k := bx - cy = k(dp)$, where $d = (b, c)$ the greatest common divisor of b and c, and $k \in \mathbb{Z}$.

We have $(\frac{c}{d}, \frac{b}{d})$ as the first positive solution on L_0. Let (x_1, y_1) be the first positive solution on L_1. Define the two vectors u and v by

$$u = \begin{pmatrix} \frac{c}{d} \\ \frac{b}{d} \end{pmatrix}, \quad v = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix},$$

then the set of solutions V is given by $V = u\mathbb{Z} + v\mathbb{Z}$. That is V is a full lattice generated by u and v, and the volume of the lattice is given by the determinant

$$D = \begin{vmatrix} x_1 & \frac{c}{d} \\ y_1 & \frac{b}{d} \end{vmatrix} = \left(\frac{b}{d}\right)x_1 - \left(\frac{c}{d}\right)y_1$$

$$= \frac{1}{d}(bx_1 - cy_1)$$

$$= \frac{1}{d}(dp) = p.$$

Consider the square S centered at the origin and defined by $S := [-\sqrt{p}, \sqrt{p}] \times [-\sqrt{p}, \sqrt{p}]$, then the volume of the square is $2^2 p$. Therefore, Minkowski's convex body theorem guarantees the existence of a non-zero solution (x_0, y_0) in the square S.

As an immediate result of Theorem 1, we have the following corollary.

Corollary 1. *If $\mathcal{B}$ any box of size $B > 2\sqrt{p}$ in XY-plane centered at a solution point $(x_1, y_1) \in V$, then $\mathcal{B}$ contains another solution point (x_2, y_2).*

Proof. Let (x_0, y_0) be the non-zero solution in the square S that obtained in Theorem 1. Translate the square S to be centered at (x_1, y_1), then the point (x_0, y_0) translated to the point $(x_0 + x_1, y_0 + y_1)$. Let $(x_2, y_2) = (x_0 + x_1, y_0 + y_1)$, then $|x_2 - x_1| = |x_0| < \sqrt{p}$, and $|y_2 - y_1| = |y_0| < \sqrt{p}$. That is $(x_2, y_2) \in \mathcal{B}$, and $bx_2 = b(x_0 + x_1) \equiv c(y_0 + y_1) = cy_2 \pmod{p}$.

Theorem 2. *For* $1 \leq c, b < p$, *there exist a box* $\mathcal{B}$ *of size* $B = \dfrac{dp}{b+c}$ *such that* $V \cap \mathcal{B}$ *is empty intersection, where* $d = (b, c)$.

Proof. Consider the set of lines defined by $L_k := bx - cy = k(dp)$, where $d = (b, c)$ and $k \in \mathbb{Z}$, then V is a lattice points on these lines. Let $\mathcal{B}$ be the largest box of size B between any two consecutive lines L_k and L_{k+1}. For simplicity, we consider the two lines $L_0 := bx - cy = 0$ and $L_1 := bx - cy = dp$. Let (x_0, y_0) be the corner of the box on L_0, then $(x_0 + B, y_0 - B)$ is the corner of the box on L_1. Therefore,

$$b(x_0 + B) - c(y_0 - B) = dp$$

$$bx_0 - cy_0 + bB + cB = dp$$

$$(b + c)B = dp$$

$$B = \frac{dp}{b + c}.$$

In particular if $b = c = 1$, $B = \dfrac{p}{2}$.

In next theorem, we obtain a lower bound on the size B so that $V \cap \mathcal{B}$ is a non-empty intersection.

Theorem 3. *If* $1 \leq c < b < p$ *and* $\dfrac{b^2 - c^2}{d^2} < p$, *where* $d = (b, c)$, *then any box of size* $B > \dfrac{dp}{b+c} + 2\left(\dfrac{c}{d}\right)$ *contains a point of V.*

Proof. We have

$$\frac{b^2 - c^2}{d^2} < p$$

$$(b - c)(b + c) < d^2 p$$

$$b - c < \frac{d^2 p}{b + c}$$

$$\frac{b}{d} < \frac{dp}{b + c} + \frac{c}{d}$$

$$\frac{b}{d} < B + \frac{c}{d},$$

where B is the size of the box obtained in Theorem 2. That is the vertical distance between solutions on the line L_1 defined in Theorem 2 less than B plus the horizontal distance between solutions on L_1.

We are seeking the maximum enlargement of the box inscribed between L_0 and L_1 in Theorem 2 without containing a solution. Let the box obtained in Theorem 2 cornered on L_1 at the point (x, y), then there is a solution point (x_1, y_1) on L_1, where $x < x_1 < x + \frac{c}{d}$ and $y < y_1 < y + \frac{b}{d} < y + (B + \frac{c}{d})$. Then any enlargement not containing a solution can contribute at most $(\frac{c}{d})(B + \frac{c}{d})$ square units of area along the right side of the box. Thus, the total contribution in any enlargement is at most $4(\frac{c}{d})(B + \frac{c}{d})$ square units of area. Hence the largest square area A not containing a solution is at most

$$A = B^2 + 4\left(\frac{c}{d}\right)\left(B + \frac{c}{d}\right)$$

$$= \left(B + 2\left(\frac{c}{d}\right)\right)^2$$

$$= \left(\frac{dp}{b + c} + 2\left(\frac{c}{d}\right)\right)^2.$$

Remark 1. For $1 < b < \sqrt{p}$, and $c = 1$, the hypothesis of Theorem 3 is satisfied. Theorem 2 guarantees the existence of a box of size $B = \frac{p}{b+1}$ not containing a solution, and Theorem 3 guarantees the existence of a solution in any box of size $B = \frac{p}{b+1} + 2$. Thus, the results obtained in Theorem 2 and Theorem 3 are best possible for these values of b and c.

For $1 \leq c < b < p$, where $(b, c) = 1$, let (x_0, y_0) be the first positive solution on the line $L_1 := bx - cy = p$. x_0 and y_0 plays a central roll in next theorems. In the next theorem, we determine these values of x_0 and y_0.

Theorem 4. *For* $1 \leq c < b < p$, *and* $(b, c) = 1$, *the first positive solution* (x_0, y_0) *of* $bx \equiv cy \pmod{p}$ *on the line* $L_1 := bx - cy = p$ *is given by*

$$(x_0, y_0) = \left(\left[\frac{p}{b}\right] + 1 + \lambda, \ \frac{b\left(\left[\frac{p}{b}\right] + 1\right) - p + \lambda b}{c} \right),$$

where λ *is the minimal non-negative solution of the linear congruence* $bx \equiv p - b\left(\left[\frac{p}{b}\right] + 1\right) \pmod{c}$.

Proof. Here, we look at the solutions on any line L_k as a vector solution rather than a lattice point.

The first positive solution on $L_c : bx - cy = cp$ is given by the vector

$$u = \begin{pmatrix} c\left(\left[\frac{p}{b}\right] + 1\right) \\ b\left(\left[\frac{p}{b}\right] + 1\right) - p \end{pmatrix}.$$

If $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ is the first solution on $L_1 := bx - cy = p$, then the vector $\begin{pmatrix} cx_0 \\ cy_0 \end{pmatrix}$ is a positive solution on L_c. Therefore,

$$\begin{pmatrix} cx_0 \\ cy_0 \end{pmatrix} = \begin{pmatrix} c\left(\left[\frac{p}{b}\right] + 1\right) \\ b\left(\left[\frac{p}{b}\right] + 1\right) - p \end{pmatrix} + \begin{pmatrix} \lambda c \\ \lambda b \end{pmatrix},$$

for some non-negative λ.

$$\begin{pmatrix} cx_0 \\ cy_0 \end{pmatrix} = \begin{pmatrix} c\left(\left[\frac{p}{b}\right] + 1\right) + \lambda c \\ b\left(\left[\frac{p}{b}\right] + 1\right) - p + \lambda b \end{pmatrix}.$$

In particular c divides $b\left(\left[\frac{p}{b}\right] + 1\right) - p + \lambda b$. That is,

$$\lambda b \equiv p - b\left(\left[\frac{p}{b}\right] + 1\right) \pmod{c}.$$

And since $x_0,\ y_0$ is the smallest positive solution, then λ is the minimal solution of the congruence

$$bx \equiv p - b\left(\left[\frac{p}{b}\right] + 1\right) \pmod{c},$$

and

$$(x_0,\ y_0) = \left(\left[\frac{p}{b}\right] + 1 + \lambda,\ \frac{b\left(\left[\frac{p}{b}\right] + 1\right) - p + \lambda b}{c}\right).$$

Note. For the special case where $c = 1$ and $\frac{p}{2} < b < p$, we have $\lambda = 0$ and $\left[\frac{p}{b}\right] = 1$, and hence $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 2 \\ 2b - p \end{pmatrix}$.

For better results, we consider two cases according as whether $y_0 < \frac{b}{2}$ or $y_0 > \frac{b}{2}$, where (x_0, y_0) the first positive solution on L_1 obtained in Theorem 4.

If $y_0 < \frac{b}{2}$, let L_1 and L_2 be the two parallel lines determined by the vector $v = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ and the two points $(0, 0)$ and (c, b), respectively. Slop of L_1 is $m = \frac{y_0}{x_0}$, the equation of L_1 is given by $y = \frac{y_0}{x_0}x$, and the equation of L_2 is given by $y = \frac{y_0}{x_0}(x - c) + b$, the horizontal distance between solutions on L_1 is x_0, and the vertical distance is y_0. Here we view V the set of solutions of $bx \equiv cy \pmod{p}$ as a lattices point on a lines parallel to L_1 and L_2.

Theorem 5. *For* $1 \leq c < b < p$, *with* $(b, c) = 1$ *and* $y_0 < \frac{b}{2}$, *there exist a box* $\mathcal{B}$ *of size* $B = \dfrac{p}{x_0 + y_0} = \dfrac{cp}{x_0(b + c) - p}$ *such that* $V \cap \mathcal{B}$ *is empty.*

Proof. Let $\mathcal{B}$ be the largest possible box of size B between L_1 and L_2. If the corner of the box on L_1 at $(x, \frac{y_0}{x_0}x)$, then the corner on L_2 is at $(x - B, \frac{y_0}{x_0}x + B)$. Therefore,

$$\frac{y_0}{x_0}x + B = \frac{y_0}{x_0}(x - B - c) + b$$

$$B\left(1 + \frac{y_0}{x_0}\right) = b - \frac{y_0}{x_0} c$$

$$B = \frac{bx_0 - cy_0}{x_0 + y_0} = \frac{p}{x_0 + y_0}$$

$$B = \frac{p}{x_0 + \frac{bx_0 - p}{c}} = \frac{cp}{x_0(b + c) - p}.$$

Theorem 5 gives a necessary condition on the size of a box $\mathcal{B}$ to meet V. Next theorem gives a sufficient condition on the size of a box in order to meet V.

Theorem 6. *For* $1 \leq c < b < p$ *with* $(b, c) = 1$, *and* $y_0 < \frac{b}{2}$, *let* B *be the size of the box obtained in Theorem* 5. *If* $B + x_0 > y_0$, *then any box of size* $B + 2x_0 = \frac{cp}{x_0(b + c) - p} + 2x_0$ *contains a point of* V.

Proof. We try to enlarge the size of the box between L_1 and L_2 as much as possible without meeting V. If the corner of the box on L_1 at (x, y), then there exist a solution (x_1, y_1) on L_1 such that $x < x_1 < x + x_0$ and $y < y_1 < y + y_0 < y + B + x_0$. Thus any enlargement not meeting V contributes at most $x_0(B + x_0)$ square units of area along the right side of the box. Therefore, the maximum square area A not meeting V is at most

$$A = B^2 + 4x_0(B + x_0)$$

$$= (B + 2x_0)^2.$$

Remark 2. For the values where $c = 1$ and $\frac{p}{2} < b < p$, we have $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 2 \\ 2b - p \end{pmatrix}$, and $y_0 < \frac{b}{2} \Leftrightarrow 2b - p < \frac{b}{2} \Leftrightarrow b < \frac{2p}{3}$. Theorem 5 guarantees the existence of a box $\mathcal{B}$ of size $B = \dfrac{p}{2(b+1)-p}$ does not meet V, and Theorem 6 guarantees any box of size $B + 4 = \dfrac{p}{2(b+1)-p} + 4$ does meet V. Hence for the values where $c = 1$ and b belongs to the interval $(\frac{p}{2}, \frac{2p}{3})$, the results of Theorem 5 and Theorem 6 are best possible.

Now we consider the case where $y_0 > \frac{b}{2}$.

If $y_0 > \frac{b}{2}$, let L_1 and L_2 be the two parallel lines determined by the vector $v = \begin{pmatrix} x_0 - c \\ \\ y_0 - b \end{pmatrix}$ and the two points $(0, 0)$ and (b, c), respectively. The slop of L_1 is $m = \dfrac{y_0 - b}{x_0 - c}$ is negative, the equation of L_1 is given by $y = \dfrac{y_0 - b}{x_0 - c}x$, the equation of L_2 is given by $y = \dfrac{y_0 - b}{x_0 - c}(x - c) + b$. The horizontal distance between solutions on L_1 is $x_0 - c$ and the vertical distance is $b - y_0$.

Theorem 7. *For* $1 \le c < b < p$ *with* $(b, c) = 1$, *and* $y_0 > \frac{b}{2}$, *there exists a box of size* $B = \dfrac{p}{x_0 - y_0 + b - c}$ *such that B does not meet V.*

Proof. Let $\mathcal{B}$ be the largest box of size B between L_1 and L_2. If corner of the box on L_1 at $(x, \frac{y_0 - b}{x_0 - c}x)$, then the corner on L_2 at $(x + B, \frac{y_0 - b}{x_0 - c}x + B)$, hence

$$\frac{y_0 - b}{x_0 - c}x + B = \left(\frac{y_0 - b}{x_0 - c}\right)(x + B - c) + b$$

$$B\left(1-\frac{y_0-b}{x_0-c}\right) = b - c\left(\frac{y_0-b}{x_0-c}\right)$$

$$B = \frac{b - c\left(\frac{y_0-b}{x_0-c}\right)}{1-\frac{y_0-b}{x_0-c}}$$

$$B = \frac{bx_0 - cy_0}{x_0 - c - y_0 + b} = \frac{p}{x_0 - y_0 + b - c}.$$

Theorem 8. *Let* $1 \le c < b < p$ *with* $(b, c) = 1$ *and* $y_0 > \frac{b}{2}$. *If* $B + (x_0 - c) > b - y_0$, *where B is the size of the box obtained in Theorem 7, then any box of size* $B + 2(x_0 - c)$ *meets V.*

Proof. If the corner of the box in Theorem 7 on L_1 at (x, y), then there is a solution (x_1, y_1) on L_1 such that $x - (x_0 - c) < x_1 < x$ and $y < y_1 < y + (b - y_0) < y + B + (x_0 - c)$. Thus any enlargement of the box not meeting V contributes at most $(x_0 - c)(B + (x_0 - c))$ square units of area along the left side of the box. Therefore, the maximum square area A not meeting V is at most

$$\begin{aligned} A &= B^2 + 4(x_0 - c)(B + (x_0 - c)) \\ &= (B + 2(x_0 - c))^2. \end{aligned}$$

Remark 3. The results in Theorem 7 and Theorem 8 are the best when $x_0 - c$ is minimal and $y_0 > \frac{b}{2}$. For $c = 1$ and $\frac{p}{2} < b < p$, $x_0 - c = 1$, and $y_0 > \frac{b}{2} \Leftrightarrow 2b - p > \frac{b}{2} \Leftrightarrow b > \frac{2p}{3}$. Therefore, for these values where $c = 1$ and b belongs to the interval $\left(\frac{2p}{3}, p\right)$, the results of Theorem 7 and Theorem 8 are best possible.

References

[1] A. Ayyad, The distribution of solutions of the equation $ax - y \equiv 0 \pmod{m}$, JP Jour. Algebra, Number Theory and Appl. 6(2) (2006), 313-324.

[2] R. C. Baker, Small solution of congruences, Mathematica 30 (1983), 164-188.

[3] T. Cochrane and Z. Zheng, Small solutions of the congruence $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv c \pmod{p}$, Acta Math. Sinica 14 (1998), 113-120.

■