Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 22, 2016, No. 1, 29–32

On the congruence $ax - by \equiv c\,(mod\,p)$ and the finite field Z_p

Anwar Ayyad

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

Received: 14 June 2015 **Revised:** 25 December 2015 **Accepted:** 28 December 2015

Abstract: For prime p and $1 \leq a, b, c < p$ let V be the algebraic set of the congruence $ax - by \equiv c\,(mod\,p)$ in the plane. For an arbitrary box of size B we obtain a necessary and a sufficient conditions on the size B in order for the box to meet V. For arbitrary subsets S, T of Z_p we also obtain a necessary and a sufficient conditions on the cardinalities of S, T so that $S + T = Z_p$.
Keywords: Congruence, Lattices, Solutions.
AMS Classification: 11D79, 11H06.

1 Introduction

Let V be the set of solutions of the congruence

$$ax - by \equiv c\,(mod\,p) \tag{1.1}$$

in the plane defined by $V = \{\,(x, y) \in Z \times Z : ax - by \equiv c\,(mod\,p)\,\}$.

In this paper, we view the set of solutions V of (1.1) in the plane as a set of lattice points on a lines L_k defined by $L_k :\ ax - by = c + k\,p$ where $k \in Z$. We show the existence of a box of size $B = \frac{dp}{a+b}$ contains no element of V, where $d = (a, b)$, and we prove every box of size $B = \frac{dp}{a+b} + 2\left(\frac{b}{d}\right)$ meets V.

We also study the representation of the finite field Z_p as a sum of two subsets S, T. For such two subsets we define $S + T$ as $S + T = \{s + t :\ s \in S,\ t \in T\}$. It follows from the work of [3] that for any sets S, T with $|S|\cdot|T| > 2p$, $(2S)(2T)+(2S)(2T) = Z_p$ and $(2S)(2T)-(2S)(2T) = Z_p$. In this paper we prove the existence of two subsets S, T with $|S| = \frac{p-1}{2} = |T|$ and $S+T \neq Z_p$, and in contrary to that every two subsets S, T of Z_P with $|S| \geq \frac{p+1}{2}$ and $|T| \geq \frac{p+1}{2}$ satisfies $S+T = Z_p$.

2 Theorems and proofs

Theorem 1. There are two subsets S, T of $Z_p$with $|S| = |T| = \frac{p-1}{2}$ and $S+T \neq Z_p$.
Proof. Consider the congruence

$$x - y \equiv \frac{p-1}{2}(mod\, p) \tag{2.1}$$

and the line L_0 defined by $L_0 : x-y = \frac{p-1}{2}$. The $x-$ $intercept$ $\left(\frac{p-1}{2}, 0\right)$ is a solution of (2.1) on L_0. Let L_{-1} be the line defined by $L_{-1} : x-y = \frac{p-1}{2} - p = -\left(\frac{p+1}{2}\right)$. The $y-intercept$ $\left(0, \frac{p+1}{2}\right)$ is a solution of (2.1) on L_{-1}. Now consider the rectangle R determined by the vertices $(0,0)$, $\left(\frac{p-1}{2}, 0\right)$, $\left(0, \frac{p+1}{2}\right)$ and $\left(\frac{p-1}{2}, \frac{p+1}{2}\right)$, then R contains no solution of (2.1). In particular, there is a box of size $B = \frac{p-1}{2}$ cornered at the origin and contains no solution of (2.1). Let $S = \left\{s : 0 \leq s < \frac{p-1}{2}\right\}$ and $T = \left\{-t : 0 \leq t < \frac{p-1}{2}\right\}$ then $c = \frac{p-1}{2} \notin S+T$. □

The result in Theorem 1 is best possible as the next theorem suggests.

Theorem 2. Let S, T arbitrary subsets of Z_p, if $|S| \geq \frac{p+1}{2}$ and $|T| \geq \frac{p+1}{2}$, then $S+T = Z_p$.
Proof. If $c \in Z_p$, let $W = -T + c = \{-t + c : t \in T\}$, then $|W| = |T| \geq \frac{p+1}{2}$, therefore $S \bigcap W \neq \emptyset$. Then there is $s_0 \in S$ and $w_0 \in W$ such that $-t_0 + c = s_0$ for some $t_0 \in T$. Therefore $c = s_0 + t_0 \in S+T$. □

Theorem 3. Every box of size $B \geq \frac{p+1}{2}$ in the plane contains a solution of (1.1).
Proof. Let I be the projection of the box on the $x-axis$, and J be the projection on the y-axis, let $S = a \cdot I = \{ax : x \in I\}$ and $T = -b \cdot J = \{-by : y \in J\}$, then $|S| \geq \frac{p+1}{2}$ and $T \geq \frac{p+1}{2}$, hence by Theorem 2 for every $c \in Z_p$ there exists $ax \in S$ and $-by \in T$ such that $ax - by = c$. □

Theorem 4. There exist a box of size $B = \sqrt{p} - 1$ contains no solution of (1.1).
Proof. Let S be the square defined by $S : \{x : 0 < x < p\} \times \{y : 0 < y < p\}$.

Since $\left(\sqrt{p}-1\right)\left(\left[\sqrt{p}\right]+1\right) < \left(\sqrt{p}-1\right)\left(\sqrt{p}+1\right) = p-1 < p$, then the interval $(0\ ,\ p)$ contains at least $\left[\sqrt{p}\right] + 1$ subintervals each of length $\sqrt{p}-1$, therefore the square S contains at least $\left(\left[\sqrt{p}\right]+1\right)^2 > p$ subsquares each of size $\sqrt{p}-1$, and since number of solutions of (1.1) in the square is $p-1$, then by pigeon-hole principle there is at least one subsquare contains no solution of (1.1). □

Now we view the solutions of (1.1) in the plane as a set of lattice points on a lines L_k defined by L_k: $ax - by = c + kp$ where $k \in Z$.

If L_k is such a line, then the next line to the right is L_{k+d} defined by $L_{k+d} : ax - by = c + kp + dp$, where $d = (a, b)$.

The horizontal distance H between the lines L_k and L_{k+d} is $H = \frac{dp}{a}$, the horizontal distance between solutions on the line L_k is $h = \frac{b}{d}$, and the vertical distance v is $v = \frac{a}{d}$.

Theorem 5. For every $a,\ b,\ c$ there is a box of size $B = \frac{dp}{a+b}$ contains no solution of (1.1).

Proof. For $k \in Z,\ and\ d$ divides $c + kp$, where $d = (a, b)$, consider the two lines L_k, L_{k+d}. Let S the largest square of size B can be inscribed between these two lines. If $\left(x, \frac{ax-c-kp}{b}\right)$ is the corner of the square on L_k then $\left(x + B, \frac{ax-c-kp}{b} - B\right)$ is the corner on L_{k+d} and satisfies its equation. Therefore

$$a\left(x+B\right) - b\left(\frac{ax-c-kp}{b} - B\right) = c + kp + dp$$
$$\left(a+b\right)B = dp$$
$$B = \frac{dp}{a+b}.$$

□

Theorem 6. Let B be the size of the box obtained in Theorem 5, if $B + \frac{b}{d} > \frac{a}{d}$, then any box of size $B + 2\left(\frac{b}{d}\right)$ contains a solution of (1.1).

Proof. We are to find maximum enlargement of the box in Theorem 5 not containing a solution. Let $(x\ ,\ y)$ the corner of the box on L_{k+d} in Theorem 5. Since $B + \frac{b}{d} > \frac{a}{d}$, then there is a solution $(x_0\ ,\ y_0)$ on L_{k+d} such that $x < x_0 < x + \frac{b}{d}$, and $y < y_0 < y + \frac{a}{d} < y + B + \frac{b}{d}$. Therefore any enlargement of the box not containing a solution can contribute at most $\left(B + \frac{b}{d}\right) \cdot \frac{b}{d}$ square units of area along the right side of the box and similarly along the left side. Thus, the total contribution is $4\left(B + \frac{b}{d}\right) \cdot \frac{b}{d}$ square units of area. Therefore, the largest square area not containing a solution is at most

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

□

3 Remarks on Theorems 5, 6

Remark 1. It is surprising to see the results in Theorems 5, 6 do not depend on c but only on a, b and their greatest common divisor.

Remark 2. Let$(a\ ,\ b) = 1,$ then

$$B + \frac{b}{d} > \frac{a}{d}$$
$$\Leftrightarrow \frac{p}{a+b} + b > a$$
$$\Leftrightarrow \frac{p}{a+b} > a - b$$
$$\Leftrightarrow \quad p > a^2 - b^2.$$

And this is satisfied for $0 < b < a < \sqrt{p}$.

Thus if $0 < b < a < \sqrt{b}$, $(a,\ b)$ =1, there exist a box of size $B = \frac{p}{a+b}$ contains no solution of $ax - by\ \equiv c\,(mod\,p)$, and every box of size $B = \frac{p}{a+b} + 2b$ contains a solution.

In particular if $b = 1$ and $a = \left[\sqrt{p}\right]$ there is box of size $B = \frac{p}{\left[\sqrt{p}\right]+1}$ contains no solution of $ax - by \equiv c\,(mod\,p)$, and every box of size $B = \frac{p}{\left[\sqrt{p}\right]+1} + 2$ contains a solution and this is the best possible.

We use the above remark to prove the next theorem.

Theorem 7. There are sets S, T with $|S| = |T| = \left[\sqrt{p}\right] + 3$ and $S + T = Z_p$.

Proof. Since $\left[\sqrt{p}\right] + 3 > \sqrt{p}$ +2 $> \frac{p}{\left[\sqrt{p}\right]+1} + 2$, then by the above remark, for any $c \in Z_p, \exists\, x_0, y_0$ such that

$$[\sqrt{p}]\,x_0 - y_0 \equiv c\,(mod\ \ p)\ \ and\ \ 0 < x_0, y_0 \leq [\sqrt{p}] + 3.$$

Let $S = \left[\sqrt{p}\right] \cdot I$ and $T = -J$ where $I = J = \left\{x : 0 < x \leq \left[\sqrt{p}\right] + 3\right\}$, then $c \in S + T$. □

It is clear that the result in Theorem 7 is best possible in the sense that any two subsets S, T with cardinalities $\left[\sqrt{p}\,\right]$ does not satisfy $S + T = Z_p$.

Corollary 1. For every c there is a solution of $\left[\sqrt{p}\right] x + y \equiv c\,(mod\,p)$ with $0 < x, y \leq \left[\sqrt{p}\right] + 3$.

Proof. Consider the square of size $\left[\sqrt{p}\right] + 3$ cornered at the origin in the 4^{th} quadrant, then it contains a solution $(x_0\ ,\ y_0)$ of $\left[\sqrt{p}\right] x - y \equiv c\,(mod\,p)\ ,\ y_0 < 0$.

Thus $(x_0, -y_0)$ is a solution of $\left[\sqrt{p}\right] x + y \equiv c\,(mod\,p)$ with $0 < x_0\ ,\ -y_0 \leq \left[\sqrt{p}\right]$ +3. □

Corollary 2. The congruence $x_1x_2x_3 \cdots x_n + y_1y_2y_3 \cdots y_n \equiv c\,(mod\,p)$ has a solution with

$$0 < x_i, y_i\ \ \leq [\sqrt{p}] + 3.$$

Proof. Let (x_0, y_0) be a solution of $\left[\sqrt{p}\right] x + y \equiv c\,(mod\,p)\ ,\ 0 < x_0\ ,\ y_0 \leq \left[\sqrt{p}\right] + 3$.
For $n = 2$, let $x_1 = \left[\sqrt{p}\right]$, $x_2 = x_0$ and $y_1 = y_0\ ,\ y_2 = 1$.
For $n \geq 3$, let x_1=$\left[\sqrt{p}\right]$, $x_2 = x_0, x_3 = \cdots = x_n = 1$.

$$y_1 = y_0, y_2 = y_3 = \cdots = y_n = 1.$$

□

References

[1] Ayyad, A., Cochrane, T. & Zheng, Z. (1996) The congruence $x_1x_2 \equiv x_3x_4(modp)$, the equation and mean values of character sums. *J. Number Theory*, 59, 398–413.

[2] Bourgain, J., Katz N. & Tao, T. (2004) A sum-product estimate in finite fields and their applications, *Geom. Funct. Anal.* 14, 27–57.

[3] Glibichuk, A. A. (2006) Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem, *Mat. Zametki*, 79, 384-395 (in Russian), English transl.: *Math. Notes* 79, 2006, 556–365.