DISTRIBUTION AND ADDITIVE PROPERTIES OF SEQUENCES WITH TERMS INVOLVING SUMSETS IN PRIME FIELDS

Victor Cuauhtemoc García [1]
Departamento de Ciencias Básicas e Ingeniería, Universidad Autónoma Metropolitana–Azcapotzalco, México
vc.garci@gmail.com

Received: 9/22/11, Revised: 4/4/12, Accepted: 7/4/12, Published: 7/13/12

Abstract

Let p be a large prime number, and $\mathcal{U}$, $\mathcal{V}$ be nonempty subsets of the set of residue classes modulo p. In this paper we obtain results on the distribution and the additive properties of sequences involving terms of the form $u+v$, where $u \in \mathcal{U}$ and $v \in \mathcal{V}$. For instance, we prove that $(\mathcal{A}+\mathcal{A})(\mathcal{B}+\mathcal{Y})+(\mathcal{C}+\mathcal{C})(\mathcal{D}+\mathcal{W}) = \mathbb{F}_p$, for any subsets $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D},\mathcal{Y},\mathcal{W}$ of $\mathbb{F}_p^*$ with $|\mathcal{A}||\mathcal{C}|, \sqrt{|\mathcal{B}||\mathcal{D}||\mathcal{Y}||\mathcal{W}|} \geq 10\,p$. This extends a previous result of Garaev and the author.

1. Introduction

In what follows, p denotes a large prime number and $\mathbb{F}_p^*$ is the multiplicative group of $\mathbb{F}_p$. The notation $f \ll g$ is equivalent to $f = \mathcal{O}(g)$ and means that $|f(x)| \leq Cg(x)$, as $x \to \infty$, for some absolute constant $C > 0$. Given $\mathcal{A}$, $\mathcal{B}$ nonempty subsets of $\mathbb{F}_p$ and k a positive integer we shall use the standard notation

$$\begin{aligned}
\mathcal{A}+\mathcal{B} &= \{a+b \pmod p \ : \ a\in\mathcal{A},\ b\in\mathcal{B}\},\\
\mathcal{A}\,\mathcal{B} &= \{ab \pmod p \ : \ a\in\mathcal{A},\ b\in\mathcal{B}\},\\
k\,\mathcal{A} &= \{a_1+\ldots+a_k \pmod p \ : \ a_1,\ldots,a_k\in\mathcal{A}\}.
\end{aligned}$$

Using combinatorial arguments, Glibichuk [2] established that if $\mathcal{A},\mathcal{B}$ are subsets with $|\mathcal{A}||\mathcal{B}| \geq 2p$, then $8\mathcal{A}\mathcal{B} = \mathbb{F}_p$. We note that the proof of [2, Theorem 1] also implies that $(\mathcal{A}+\mathcal{A})(\mathcal{B}+\mathcal{B})+(\mathcal{A}+\mathcal{A})(\mathcal{B}+\mathcal{B}) = \mathbb{F}_p$.

This result can be interpreted as the assertion that for any arbitrary pair of small sets $\mathcal{A},\mathcal{B}$, with $|\mathcal{A}||\mathcal{B}| \geq 2p$, every residue class modulo p can be written as a small number of combinations of sums and products of their elements.

We note that the condition $|\mathcal{A}||\mathcal{B}| \geq 2p$, is sharp apart from the constant 2. Indeed, let $\Delta = \Delta(p)$ be any increasing function with $\Delta \to \infty$, as $p \to \infty$, and

[1]The author was supported by the Project UAM-A 2232508.

set $\mathcal{A} = \mathcal{B} = \{1, 2, 3, \ldots, [\sqrt{p/\Delta}]\}$. We have that $\mathcal{A}\mathcal{B} \subseteq \{1, 2, 3, \ldots, [p/\Delta] + 1\}$ and clearly there is no fixed integer $k \geq 2$ such that for every prime number $p \geq p_0$ the equality $k\mathcal{A}\mathcal{B} = \mathbb{F}_p$ holds: See the discussion given in [3].

It is natural to ask if it is possible to obtain similar results combining more than a pair of different sets. In [1, Theorem 4] it was proved that if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are arbitrary subsets of $\mathbb{F}_p^*$ with

$$|\mathcal{A}||\mathcal{C}|,\ |\mathcal{B}||\mathcal{D}| > (2 + \sqrt{2})p,$$

then

$$(\mathcal{A} + \mathcal{A})(\mathcal{B} + \mathcal{B}) + (\mathcal{C} + \mathcal{C})(\mathcal{D} + \mathcal{D}) = \mathbb{F}_p.$$

This result directly implies that $4\mathcal{A}\mathcal{B} + 4\mathcal{C}\mathcal{D} = \mathbb{F}_p$. Furthermore, from the work by Hart and Iosevich [4], it follows that for any $2k$ subsets $\mathcal{A}_i, \mathcal{B}_i$, $1 \leq i \leq k$, satisfying

$$\prod_{i=1}^{k} |\mathcal{A}_i||\mathcal{B}_i| \geq Cp^{k+1},$$

we have $\mathbb{F}_p^* \subseteq \mathcal{A}_1\mathcal{B}_1 + \ldots + \mathcal{A}_k\mathcal{B}_k$, where $C = C(k)$ is some large constant. In particular

$$\mathbb{F}_p^* \subseteq \mathcal{A}_1\mathcal{B}_1 + \ldots + \mathcal{A}_8\mathcal{B}_8,$$

whenever

$$\prod_{i=1}^{8} |\mathcal{A}_i||\mathcal{B}_i| \gg p^9. \tag{1}$$

This result involves 16 different sets at the cost of an optimal order.

With these facts in mind, we expect that for arbitrary subsets $\mathcal{A}_i, \mathcal{B}_i, \mathcal{C}_i, \mathcal{D}_i;\ i = 1, 2$, of $\mathbb{F}_p^*$ with

$$\prod_{i=1}^{2} |\mathcal{A}_i||\mathcal{B}_i||\mathcal{C}_i||\mathcal{D}_i| \gg p^4,$$

the following expresion holds:

$$(\mathcal{A}_1 + \mathcal{A}_2)(\mathcal{B}_1 + \mathcal{B}_2) + (\mathcal{C}_1 + \mathcal{C}_2)(\mathcal{D}_1 + \mathcal{D}_2) = \mathbb{F}_p. \tag{2}$$

We also notice that the most interesting case takes place if the zero class is removed for each set. Otherwise, it is possible to construct exceptional examples; for instance, $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{C}_1 = \mathcal{C}_2 = \mathbb{F}_p, \quad \mathcal{B}_1 = \mathcal{B}_2 = \mathcal{D}_1 = \mathcal{D}_2 = \{0\}$ gives

$$\prod_{i=1}^{2} |\mathcal{A}_i||\mathcal{B}_i||\mathcal{C}_i||\mathcal{D}_i| = p^4$$

and

$$(\mathcal{A}_1 + \mathcal{A}_2)(\mathcal{B}_1 + \mathcal{B}_2) + (\mathcal{C}_1 + \mathcal{C}_2)(\mathcal{D}_1 + \mathcal{D}_2) = \{0\}.$$

Using the combinatorial point of view, and methods of estimation of trigonometric sums we establish (2) for some important cases. We obtain that for any subsets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{Y}, \mathcal{W}$ of $\mathbb{F}_p^*$ satisfying

$$|\mathcal{A}||\mathcal{C}| > 10p, \qquad |\mathcal{B}||\mathcal{D}||\mathcal{Y}||\mathcal{W}| > 100p^2,$$

the following equality holds: $(\mathcal{A}+\mathcal{A})(\mathcal{B}+\mathcal{Y}) + (\mathcal{C}+\mathcal{C})(\mathcal{D}+\mathcal{Z}) = \mathbb{F}_p$. This extends the already mentioned result of [1]. As a direct consequence we have

$$2\mathcal{A}\mathcal{B} + 2\mathcal{A}\mathcal{Y} + 2\mathcal{C}\mathcal{D} + 2\mathcal{C}\mathcal{Y} = \mathbb{F}_p.$$

Moreover, we prove that $\mathcal{A}_1\mathcal{B}_1 + \ldots + \mathcal{A}_8\mathcal{B}_8 = \mathbb{F}_p$, assuming that $\mathcal{A}_i, \mathcal{B}_i$, $1 \le i \le 8$, are subsets of $\mathbb{F}_p^*$ with

$$\begin{gathered} \prod_{i=1}^{4} |\mathcal{A}_i|, \prod_{i=5}^{8} |\mathcal{A}_i|, \prod_{i=1}^{4} |\mathcal{B}_i|, \prod_{i=5}^{8} |\mathcal{B}_i| \ge 100\, p^2; \\ \text{and} \;\; \mathcal{A}_1 = \mathcal{A}_2, \quad \mathcal{A}_3 = \mathcal{A}_4, \quad \mathcal{A}_5 = \mathcal{A}_6, \quad \mathcal{A}_7 = \mathcal{A}_8. \end{gathered} \tag{3}$$

This result sharpen the one of Hart and Iosevich for some cases. We remove one factor p in the right side of (1) using 12 different sets subject to (3).

2. Formulation of the Results

Throughout the paper, given u in $\mathbb{F}_p^*$, by $u^* \pmod p$ we denote the residue class such that $uu^* \equiv 1 \pmod p$. Also, for $\mathcal{U}, \mathcal{U}', \mathcal{V}, \mathcal{V}'$, nonempty subsets of $\mathbb{F}_p^*$, we denote by $(\mathcal{U}+\mathcal{U}')(\mathcal{V}+\mathcal{V}')^*$ the subset of $\mathbb{F}_p^*$ with elements of the form

$$(u+v)(u'+v')^* \pmod p,$$

where

$$\begin{gathered} u \in \mathcal{U}, \quad u' \in \mathcal{U}', \quad v \in \mathcal{V}, \quad v' \in \mathcal{V}', \\ u+v \not\equiv 0 \pmod p, \quad u'+v' \not\equiv 0 \pmod p. \end{gathered}$$

Theorem 1. *Let δ be a real number satisfying $\delta > 1$ and $\mathcal{B}, \mathcal{Y}, \mathcal{D}, \mathcal{W}$, subsets of $\mathbb{F}_p^*$ with $|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}| \ge \delta p^2$. Then*

$$|(\mathcal{B}+\mathcal{Y})(\mathcal{D}+\mathcal{W})^*| = (p-1) + \frac{\theta p^2}{\left(1 - \frac{1}{\sqrt{\delta}}\right)\sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|}},$$

where θ is a real number satisfying $|\theta| < 1$.

Combining Theorem 1 with some arguments used in [1] one can obtain the following result.

Theorem 2. *Let* $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{Y}, \mathcal{W}$ *be subsets of* $\mathbb{F}_p^*$ *such that*

$$|\mathcal{A}||\mathcal{C}| \geq 10p, \qquad |\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}| \geq 100p^2.$$

Then

$$(\mathcal{A}+\mathcal{A})(\mathcal{B}+\mathcal{Y}) + (\mathcal{C}+\mathcal{C})(\mathcal{D}+\mathcal{W}) = \mathbb{F}_p. \tag{4}$$

We immediately derive $2\mathcal{A}\mathcal{B} + 2\mathcal{A}\mathcal{Y} + 2\mathcal{C}\mathcal{D} + 2\mathcal{C}\mathcal{Y} = \mathbb{F}_p$. However, we obtain a slight improvement on the number of different sets.

Theorem 3. *Let* $\mathcal{A}_i, \mathcal{B}_i$, $1 \leq i \leq 8$, *be subsets of* $\mathbb{F}_p^*$ *with*

$$\prod_{i=1}^{4}|\mathcal{A}_i|, \prod_{i=5}^{8}|\mathcal{A}_i| \geq 100\,p^2; \quad \prod_{i=1}^{4}|\mathcal{B}_i|, \prod_{i=5}^{8}|\mathcal{B}_i| \geq 100\,p^2;$$
$$\mathcal{A}_1 = \mathcal{A}_2, \quad \mathcal{A}_3 = \mathcal{A}_4, \quad \mathcal{A}_5 = \mathcal{A}_6, \quad \mathcal{A}_7 = \mathcal{A}_8.$$

Then $\mathcal{A}_1\mathcal{B}_1 + \ldots + \mathcal{A}_8\mathcal{B}_8 = \mathbb{F}_p$.

We note that from Theorem 1 it follows that if $|\mathcal{U}||\mathcal{U}'||\mathcal{V}||\mathcal{V}'| \geq \Delta p^2$, with Δ an arbitrary strictly increasing function such that $\Delta = \Delta(p) \to \infty$ as $p \to \infty$, then

$$|(\mathcal{U}+\mathcal{V})(\mathcal{U}'+\mathcal{V}')^*| = p\left(1 + \mathcal{O}(1/\sqrt{\Delta})\right).$$

In particular, almost all residue classes modulo p can be written as

$$(u+v)(u'+v')^* \pmod{p},$$

for some $u \in \mathcal{U}, u' \in \mathcal{U}', v \in \mathcal{V}, v' \in \mathcal{V}'$.

Within this spirit, combining Theorem 1 with the pigeon–hole principle we have that $(\mathcal{A}+\mathcal{X})(\mathcal{B}+\mathcal{Y})^* + (\mathcal{C}+\mathcal{Z})(\mathcal{D}+\mathcal{W})^* = \mathbb{F}_p$, if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{W}$ are subsets of $\mathbb{F}_p^*$ satisfying $|\mathcal{A}||\mathcal{X}||\mathcal{C}||\mathcal{Z}| \geq 100p^2$ and $|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}| \geq 100p^2$.

3. Proof of Theorem 1

First, we establish the following lemma.

Lemma 4. *Let* $\mathcal{B}, \mathcal{Y}, \mathcal{D}, \mathcal{W} \subseteq \mathbb{F}_p$ *be nonempty. If* $\max\{|\mathcal{B}|, |\mathcal{Y}|\}\max\{|\mathcal{D}|, |\mathcal{W}|\} > p$, *then, for the set* $\mathcal{H} = (\mathcal{B}+\mathcal{Y})^*(\mathcal{D}+\mathcal{W})$, *the following asymptotic formula holds:*

$$|\mathcal{H}| = (p-1) + \frac{\theta p^2}{\left(1 - \frac{p}{\max\{|\mathcal{B}|,|\mathcal{Y}|\}\max\{|\mathcal{D}|,|\mathcal{W}|\}}\right)\sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|}}, \tag{5}$$

where θ *is some real number with* $|\theta| \leq 1$.

Proof. We define $\mathcal{R} := \mathbb{F}_p^* \setminus \mathcal{H}$. In view of the equality $|\mathcal{R}| = (p-1) - |\mathcal{H}|$, it is sufficient to establish the inequality

$$|\mathcal{R}| \le \frac{p^2}{\sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|}\left(1 - \frac{p}{\max\{|\mathcal{B}|,|\mathcal{Y}|\}\max\{|\mathcal{D}|,|\mathcal{W}|\}}\right)}.$$

For any $r \in \mathcal{R}$ the congruence

$$d + w \equiv r(b+y) \pmod p \tag{6}$$

does not have solutions with b, y, d, w subject to

$$b + y \not\equiv 0 \pmod p, \quad d + w \not\equiv 0 \pmod p.$$

Therefore, since $b+y \equiv 0 \pmod p$ implies that $d+w \equiv 0 \pmod p$, for any r in $\mathcal{R}$, the congruence (6) has at most $\min\{|\mathcal{B}|, |\mathcal{Y}|\}\min\{|\mathcal{D}|, |\mathcal{W}|\}$ solutions subject to

$$b \in \mathcal{B}, \quad y \in \mathcal{Y}, \quad d \in \mathcal{D}, \quad w \in \mathcal{W}.$$

Expressing the number of solutions of (6), with $r \in \mathcal{R}$, via trigonometric sums we have

$$\frac{1}{p}\sum_{t=0}^{p-1}\sum_{r\in\mathcal{R}}\sum_{\substack{b\in\mathcal{B}\\ y\in\mathcal{Y}}}\sum_{\substack{d\in\mathcal{D}\\ w\in\mathcal{W}}} e^{2\pi i\frac{t}{p}((d+w)-r(b+y))} \le |\mathcal{R}|\min\{|\mathcal{B}|,|\mathcal{Y}|\}\min\{|\mathcal{D}|,|\mathcal{W}|\}.$$

Picking up the term corresponding to $t = 0$, we obtain

$$|\mathcal{R}||\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}| \le p|\mathcal{R}|\min\{|\mathcal{B}|,|\mathcal{Y}|\}\min\{|\mathcal{D}|,|\mathcal{W}|\} + S, \tag{7}$$

where

$$S = S(\mathcal{R},\mathcal{B},\mathcal{Y},\mathcal{D},\mathcal{W}) := \sum_{t=1}^{p-1}\Bigg|\sum_{\substack{d\in\mathcal{D}\\ w\in\mathcal{W}}} e^{2\pi i\frac{t}{p}(d+w)}\Bigg|\sum_{r\in\mathcal{R}}\Bigg|\sum_{\substack{b\in\mathcal{B}\\ y\in\mathcal{Y}}} e^{2\pi i\frac{tr}{p}((b+y)}\Bigg|.$$

Extending the range of the summation over r to $1 \le r \le p-1$, we obtain

$$\begin{aligned} S &\le \sum_{t=1}^{p-1}\Bigg|\sum_{\substack{d\in\mathcal{D}\\ w\in\mathcal{W}}} e^{2\pi i\frac{t}{p}(d+w)}\Bigg|\sum_{r=1}^{p-1}\Bigg|\sum_{\substack{b\in\mathcal{B}\\ y\in\mathcal{Y}}} e^{2\pi i\frac{tr}{p}((b+y)}\Bigg| \\ &\le \left(\sum_{t=1}^{p-1}\Bigg|\sum_{\substack{d\in\mathcal{D}\\ w\in\mathcal{W}}} e^{2\pi i\frac{t}{p}(d+w)}\Bigg|\right)\left(\sum_{r=1}^{p-1}\Bigg|\sum_{\substack{b\in\mathcal{B}\\ y\in\mathcal{Y}}} e^{2\pi i\frac{r}{p}((b+y)}\Bigg|\right). \end{aligned}$$

Applying the Cauchy-Schwarz-Bunyakovskii inequality,

$$S \leq \left\{ \sum_{t=0}^{p-1} \left| \sum_{d \in \mathcal{D}} e^{2\pi i \frac{td}{p}} \right|^2 \sum_{t=0}^{p-1} \left| \sum_{w \in \mathcal{W}} e^{2\pi i \frac{tw}{p}} \right|^2 \right\}^{\frac{1}{2}} \left\{ \sum_{h=0}^{p-1} \left| \sum_{b \in \mathcal{B}} e^{2\pi i \frac{hb}{p}} \right|^2 \sum_{h=0}^{p-1} \left| \sum_{y \in \mathcal{Y}} e^{2\pi i \frac{hy}{p}} \right|^2 \right\}^{\frac{1}{2}}$$
$$\leq p^2 \sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|}.$$

Therefore, combining this with estimation (7),

$$|\mathcal{R}| \sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|} \left(1 - \frac{p}{\max\{|\mathcal{B}|, |\mathcal{Y}|\} \max\{|\mathcal{D}|, |\mathcal{W}|\}} \right) \leq p^2;$$

Lemma 4 follows. □

Now we turn directly to the proof of Theorem 1. From the hypothesis we obtain

$$(\max\{|\mathcal{B}|, |\mathcal{Y}|\} \max\{|\mathcal{D}|, |\mathcal{W}|\})^2 \geq |\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}| \geq \delta\, p^2,$$

which implies

$$\frac{1}{\left(1 - \frac{p}{\max\{|\mathcal{B}|,|\mathcal{Y}|\} \max\{|\mathcal{D}|,|\mathcal{W}|\}}\right)} \leq \frac{1}{\left(1 - \frac{1}{\sqrt{\delta}}\right)}.$$

Theorem 1 follows from this relation applied to (5).

4. Proof of Theorem 2

To prove Theorem 2, denote by $\mathcal{J}$ the number of solutions of the congruence

$$a_1 + hc_1 \equiv a_2 + hc_2 \pmod p,$$

with

$$a_1, a_2 \in \mathcal{A}, \quad c_1, c_2 \in \mathcal{C}, \quad h \in \mathcal{H}.$$

If $a_1 \equiv a_2 \pmod p$, then $c_1 \equiv c_2 \pmod p$ and h can be an arbitrary element of $\mathcal{H}$. Otherwise, for given a_1, a_2, c_1, c_2 with $a_1 \not\equiv a_2 \pmod p$ we have at most one possible value for h. Therefore, $\mathcal{J} \leq |\mathcal{H}||\mathcal{A}||\mathcal{C}| + |\mathcal{A}|^2|\mathcal{C}|^2$. Thus, there exists an element $h_0 \in \mathcal{H}$ such that $\mathcal{J}_0$, the number of solutions of the congruence

$$a_1 + h_0c_1 \equiv a_2 + h_0c_2 \pmod p; \quad a_1, a_2 \in \mathcal{A},\ c_1, c_2 \in \mathcal{C},$$

satisfies

$$\mathcal{J}_0 \leq |\mathcal{A}||\mathcal{C}| + \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{|\mathcal{H}|}. \tag{8}$$

By the Cauchy-Schwarz-Bunyakovskii inequality it follows that

$$\#\{\mathcal{A} + h_0\mathcal{C}\ \} \geq \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{\mathcal{J}_0}. \tag{9}$$

Since h_0 is a fixed element of $\mathcal{H}$, there exist fixed elements $b_0 \in \mathcal{B}$, $y_0 \in \mathcal{Y}$, $d_0 \in \mathcal{D}$, $w_0 \in \mathcal{W}$ such that

$$h_0 \equiv (b_0 + y_0)^*(d_0 + w_0) \pmod p.$$

Multiplying the set $\{\mathcal{A} + h_0\mathcal{C}\}$ by $(b_0 + y_0)$, it is clear that

$$\#\{(b_0 + y_0)\mathcal{A} + (d_0 + w_0)\mathcal{C}\} = \#\{\mathcal{A} + h_0\mathcal{C}\}. \tag{10}$$

We claim that

$$\#\{(b_0 + y_0)\mathcal{A} + (d_0 + w_0)\mathcal{C}\} > p/2. \tag{11}$$

Indeed, by combining the relation (10) with the equations (8) and (9) we have

$$\#\{(b_0 + y_0)\mathcal{A} + (d_0 + w_0)\mathcal{C}\} \geq \frac{|\mathcal{A}||\mathcal{C}|}{1 + |\mathcal{A}||\mathcal{C}|/|\mathcal{H}|}.$$

Thus, it will suffice to show that

$$\frac{|\mathcal{A}||\mathcal{C}|}{1 + |\mathcal{A}||\mathcal{C}|/|\mathcal{H}|} > p/2,$$

or equivalently

$$|\mathcal{A}||\mathcal{C}|\left(2 - \frac{p}{|\mathcal{H}|}\right) > p.$$

Next, applying Theorem 1; $|\mathcal{A}||\mathcal{C}|$, $\sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|} \geq 10p$, and the value set

$$|\mathcal{H}| = (p-1) + \frac{\theta\, p^2}{\frac{9}{10}\sqrt{|\mathcal{B}||\mathcal{Y}||\mathcal{D}||\mathcal{W}|}} > \frac{3}{5}p,$$

we get

$$|\mathcal{A}||\mathcal{C}|\left(2 - \frac{p}{|\mathcal{H}|}\right) > 10p\left(2 - \frac{p}{3p/5}\right) \geq \frac{10}{3}p.$$

Therefore Eq. (11) holds.

Finally, let λ be any integer. It is clear that

$$\#\{\lambda - (b_0 + y_0)\mathcal{A} - (d_0 + w_0)\mathcal{C}\} > p/2.$$

By the pigeonhole principle there exist fixed elements $a', a'' \in \mathcal{A}, c', c'' \in \mathcal{C}$, such that

$$(a' + a'')(b_0 + y_0) + (c' + c'')(d_0 + w_0) \equiv \lambda \pmod p.$$

5. Proof of Theorem 3

Following the same arguments as Theorem 2, it follows that there exist fixed elements

$$b'_i \in \mathcal{B}_i, \qquad 1 \le i \le 8,$$

such that

$$\#\{(b'_1 + b'_2)\mathcal{A}_1 + (b'_3 + b'_4)\mathcal{A}_3\} > p/2, \quad \#\{(b'_5 + b'_6)\mathcal{A}_5 + (b'_7 + b'_8)\mathcal{A}_7\} > p/2.$$

Let λ be any integer. It is clear that

$$\#\{\lambda - (b'_5 + b'_6)\mathcal{A}_5 - (b'_7 + b'_8)\mathcal{A}_7\} > p/2.$$

Hence, by the pigeon-hole principle there exist elements

$$a'_1 \in \mathcal{A}_1, \quad a'_3 \in \mathcal{A}_3, \quad a'_5 \in \mathcal{A}_5, \quad a'_7 \in \mathcal{A}_7,$$

such that

$$a'_1(b'_1 + b'_2) + a'_3(b'_3 + b'_4) \equiv \lambda - a'_5(b'_5 + b'_6) - a'_7(b'_7 + b'_8) \pmod{p},$$

thus

$$\sum_{i=1}^{8} a'_i b'_i \equiv \lambda \pmod{p},$$

with

$$a'_1 = a'_2, \quad a'_3 = a'_4, \quad a'_5 = a'_6, \quad a'_7 = a'_8.$$

References

[1] M. Z. Garaev and V. C. Garcia, 'The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications,' *J. Number Theory,* **128** (2008), no.9, 2520–2537.

[2] A. A. Glibichuk, 'Combinatorial properties of sets of residues modulo a prime and the Erdös–Graham problem', *Mat. Zametki* **79**, no.3, 384–395 (2006); English transl., *Math. Notes* **79**, no.3–4, 356–365 (2006).

[3] A. A. Glibichuk and S. V. Konyagin, 'Additive properties of product sets in fields of prime order' *Additive Combinatorics,* CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 279–286.

[4] H. Hart and A. Iosevich, 'Sums and products in finite fields: An integral geometric viewpoint,' *Radon transforms, geometry, and wavelets,* Contemp. Math., vol. 464, Amer. Math. Soc., Providence, RI, 2008, pp. 129–135.