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 \( U, V \) 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 \( u \in U \) and \( v \in V \). For instance, we prove that \( (A + A)(B + Y) + (C + C)(D + W) = F_p \), for any subsets \( A, B, C, D, Y, W \) of \( F_p^* \) with \( |A||C|, \sqrt{|B||D||Y||W|} \geq 10p \). This extends a previous result of Garaev and the author.

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

\[
A + B = \{ a + b \pmod p : a \in A, b \in B \}, \\
AB = \{ ab \pmod p : a \in A, b \in B \}, \\
kA = \{ a_1 + \ldots + a_k \pmod p : a_1, \ldots, a_k \in A \}.
\]

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

This result can be interpreted as the assertion that for any arbitrary pair of small sets \( A, B \), with \( |A||B| \geq 2p \), 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 \( |A||B| \geq 2p \), 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

1The author was supported by the Project UAM-A 2232508.
set $A = B = \{1, 2, 3, \ldots, \lfloor p/\Delta \rfloor \}$. We have that $AB \subseteq \{1, 2, 3, \ldots, \lfloor p/\Delta \rfloor + 1 \}$ and clearly there is no fixed integer $k \geq 2$ such that for every prime number $p \geq p_0$, the equality $kAB = \mathbb{F}_p$ 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 $A, B, C, D$ are arbitrary subsets of $\mathbb{F}_p^*$ with

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

then

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

This result directly implies that $4AB + 4CD = \mathbb{F}_p$. Furthermore, from the work by Hart and Iosevich [4], it follows that for any $2k$ subsets $A_i, B_i, 1 \leq i \leq k$, satisfying

$$\prod_{i=1}^{k} |A_i||B_i| \geq Cp^{k+1},$$

we have $\mathbb{F}_p^* \subseteq A_1B_1 + \ldots + A_kB_k$, where $C = C(k)$ is some large constant. In particular

$$\mathbb{F}_p^* \subseteq A_1B_1 + \ldots + A_8B_8,$$

whenever

$$\prod_{i=1}^{8} |A_i||B_i| \gg p^9.$$  

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

With these facts in mind, we expect that for arbitrary subsets $A_i, B_i, C_i, D_i; i = 1, 2$, of $\mathbb{F}_p^*$ with

$$\prod_{i=1}^{2} |A_i||B_i||C_i||D_i| \gg p^4,$$

the following expression holds:

$$(A_1 + A_2)(B_1 + B_2) + (C_1 + C_2)(D_1 + D_2) = \mathbb{F}_p.$$  

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, $A_1 = A_2 = C_1 = C_2 = \mathbb{F}_p, \ B_1 = B_2 = D_1 = D_2 = \{0 \}$ gives

$$\prod_{i=1}^{2} |A_i||B_i||C_i||D_i| = p^4$$

and

$$(A_1 + A_2)(B_1 + B_2) + (C_1 + C_2)(D_1 + D_2) = \{0 \}.$$
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
\[
|\mathcal{A}| |\mathcal{C}| > 10p, \quad |\mathcal{B}| |\mathcal{D}| |\mathcal{Y}| |\mathcal{W}| > 100p^2,
\]
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 \( \mathcal{A}_i, \mathcal{B}_i, 1 \leq i \leq 8 \), are subsets of \( \mathbb{F}_p^* \) with
\[
\prod_{i=1}^{4} |\mathcal{A}_i| \prod_{i=5}^{8} |\mathcal{A}_i| \prod_{i=1}^{4} |\mathcal{B}_i| \prod_{i=5}^{8} |\mathcal{B}_i| \geq 100p^2; \quad (3)
\]
and \( \mathcal{A}_1 = \mathcal{A}_2, \mathcal{A}_3 = \mathcal{A}_4, \mathcal{A}_5 = \mathcal{A}_6, \mathcal{A}_7 = \mathcal{A}_8 \).

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 \( u^* \equiv 1 \pmod{p} \) 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
\[
(u + v)(u' + v')^* \quad (\pmod{p}),
\]
where
\[
\begin{align*}
u & \in \mathcal{U}, \quad u' \in \mathcal{U}', \quad v \in \mathcal{V}, \quad v' \in \mathcal{V}', \\
u + v & \equiv 0 \pmod{p}, \quad u' + v' \not\equiv 0 \pmod{p}.
\end{align*}
\]

**Theorem 1.** Let \( \delta \) be a real number satisfying \( \delta > 1 \) and \( \mathcal{B}, \mathcal{Y}, \mathcal{D}, \mathcal{W} \), subsets of \( \mathbb{F}_p^* \) with \( |\mathcal{B}| |\mathcal{Y}| |\mathcal{D}| |\mathcal{W}| \geq \delta p^2 \). 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 \( \theta \) 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 $A, B, C, D, Y, W$ be subsets of $\mathbb{F}_p^*$ such that
\[
|A||C| \geq 10p, \quad |B||Y||D||W| \geq 100p^2.
\]
Then
\[
(A + A)(B + Y) + (C + C)(D + W) = \mathbb{F}_p. \tag{4}
\]
We immediately derive $2AB + 2AY + 2CD + 2CY = \mathbb{F}_p$. However, we obtain a slight improvement on the number of different sets.

**Theorem 3.** Let $A_i, B_i$, $1 \leq i \leq 8$, be subsets of $\mathbb{F}_p^*$ with
\[
\prod_{i=1}^{4} |A_i|, \prod_{i=5}^{8} |A_i| \geq 100p^2; \quad \prod_{i=1}^{4} |B_i|, \prod_{i=5}^{8} |B_i| \geq 100p^2;
\]
\[A_1 = A_2, \quad A_3 = A_4, \quad A_5 = A_6, \quad A_7 = A_8.\]
Then $A_1B_1 + \ldots + A_8B_8 = \mathbb{F}_p$.

We note that from Theorem 1 it follows that if $|U||U'|||Y'|||V'| \geq \Delta p^2$, with $\Delta$ an arbitrary strictly increasing function such that $\Delta = \Delta(p) \to \infty$ as $p \to \infty$, then
\[
|(U + Y)(U' + V')^*| = p \left(1 + O(1/\sqrt{\Delta})\right).
\]
In particular, almost all residue classes modulo $p$ can be written as
\[(u + v)(u' + v')^* \pmod{p},\]
for some $u \in U, u' \in U', v \in V, v' \in V'$.

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

### 3. Proof of Theorem 1

First, we establish the following lemma.

**Lemma 4.** Let $B, Y, D, W \subseteq \mathbb{F}_p$ be nonempty. If $\max\{|B|, |Y|\} \max\{|D|, |W|\} > p$, then, for the set $\mathcal{H} = (B + Y)^*(D + W)$, the following asymptotic formula holds:
\[
|\mathcal{H}| = (p - 1) + \frac{\theta p^2}{\left(\max\{|B|, |Y|\} \max\{|D|, |W|\}\right) \sqrt{|B||Y||D||W|}}, \tag{5}
\]
where $\theta$ 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

\[
|\mathcal{R}| \leq \frac{p^2}{\sqrt{|\mathcal{B}||\mathcal{V}||\mathcal{D}||\mathcal{W}|}} \left( 1 - \frac{p}{\max(|\mathcal{B}|,|\mathcal{V}|) \max(|\mathcal{D}|,|\mathcal{W}|)} \right).
\]

For any \( r \in \mathcal{R} \) the congruence

\[
d + w \equiv r(b + y) \pmod{p}
\]

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 \( \min\{|\mathcal{B}|,|\mathcal{V}|\} \min\{|\mathcal{D}|,|\mathcal{W}|\} \) solutions subject to

\[
b \in \mathcal{B}, \quad y \in \mathcal{V}, \quad d \in \mathcal{D}, \quad w \in \mathcal{W}.
\]

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

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

Picking up the term corresponding to \( t = 0 \), we obtain

\[
|\mathcal{R}||\mathcal{B}||\mathcal{V}||\mathcal{D}||\mathcal{W}| \leq p|\mathcal{R}| \min\{|\mathcal{B}|,|\mathcal{V}|\} \min\{|\mathcal{D}|,|\mathcal{W}|\} + S,
\]

where

\[
S = S(\mathcal{R}, \mathcal{B}, \mathcal{V}, \mathcal{D}, \mathcal{W}) := \sum_{t=1}^{p-1} \left| \sum_{d \in \mathcal{D}} \sum_{w \in \mathcal{W}} e^{2\pi i \frac{t}{p}(d+w)} \sum_{r \in \mathcal{R}} \sum_{b \in \mathcal{B}} \sum_{y \in \mathcal{V}} e^{2\pi i \frac{r}{p}((b+y))} \right|.
\]

Extending the range of the summation over \( r \) to \( 1 \leq r \leq p - 1 \), we obtain

\[
S \leq \sum_{t=1}^{p-1} \left| \sum_{d \in \mathcal{D}} \sum_{w \in \mathcal{W}} e^{2\pi i \frac{t}{p}(d+w)} \sum_{r=1}^{p-1} \left| \sum_{b \in \mathcal{B}} \sum_{y \in \mathcal{V}} e^{2\pi i \frac{r}{p}((b+y))} \right| \right| \leq \left( \sum_{t=1}^{p-1} \left| \sum_{d \in \mathcal{D}} \sum_{w \in \mathcal{W}} e^{2\pi i \frac{t}{p}(d+w)} \right| \right) \left( \sum_{r=1}^{p-1} \left| \sum_{b \in \mathcal{B}} \sum_{y \in \mathcal{V}} e^{2\pi i \frac{r}{p}((b+y))} \right| \right).
\]
Applying the Cauchy-Schwarz-Bunyakovskii inequality,

\[
S \leq \left\{ \sum_{t=0}^{p-1} \left| \sum_{d \in \mathcal{D}} e^{2\pi i \frac{td}{p}} \right|^2 \sum_{\pi=0}^{p-1} \left| \sum_{\nu \in \mathcal{W}} e^{2\pi i \frac{\nu}{p}} \right|^2 \right\}^{\frac{1}{2}} \left\{ \sum_{\nu=0}^{p-1} \left| \sum_{h \in \mathcal{B}} e^{2\pi i \frac{\nu h}{p}} \right|^2 \sum_{y \in \mathcal{Y}} \left| \sum_{h=0}^{p-1} e^{2\pi i \frac{h y}{p}} \right|^2 \right\}^{\frac{1}{2}} \leq p^2 \sqrt{|\mathcal{B}\mathcal{Y}||\mathcal{D}\mathcal{W}|}.
\]

Therefore, combining this with estimation (7),

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

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 \(J\) the number of solutions of the congruence

\[a_1 + h c_1 \equiv a_2 + h c_2 \pmod p,
\]

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, \(J \leq |\mathcal{H}| |\mathcal{A}| |\mathcal{C}| + |\mathcal{A}|^2 |\mathcal{C}|^2\). Thus, there exists an element \(h_0 \in \mathcal{H}\) such that \(J_0\), the number of solutions of the congruence

\[a_1 + h_0 c_1 \equiv a_2 + h_0 c_2 \pmod p; \quad a_1, a_2 \in \mathcal{A}, \ c_1, c_2 \in \mathcal{C},
\]

satisfies

\[J_0 \leq |\mathcal{A}| |\mathcal{C}| + \frac{|\mathcal{A}|^2 |\mathcal{C}|^2}{|\mathcal{H}|}.
\]
By the Cauchy-Schwarz-Bunyakovskii inequality it follows that
\[
\#\{A + h_0 C\} \geq \frac{|A|^2|C|^2}{|H|^2}.
\] (9)

Since \(h_0\) is a fixed element of \(H\), there exist fixed elements \(b_0 \in B, y_0 \in Y, d_0 \in D, w_0 \in W\) such that
\[
h_0 \equiv (b_0 + y_0)(d_0 + w_0) \pmod{p}.
\]

Multiplying the set \(\{A + h_0 C\}\) by \((b_0 + y_0)\), it is clear that
\[
\#\{(b_0 + y_0)A + (d_0 + w_0)C\} = \#\{A + h_0 C\}. 
\] (10)

We claim that
\[
\#\{(b_0 + y_0)A + (d_0 + w_0)C\} > p/2.
\] (11)

Indeed, by combining the relation (10) with the equations (8) and (9) we have
\[
\#\{(b_0 + y_0)A + (d_0 + w_0)C\} \geq \frac{|A||C|}{1 + |A||C|/|H|}.
\]

Thus, it will suffice to show that
\[
\frac{|A||C|}{1 + |A||C|/|H|} > p/2,
\]
or equivalently
\[
|A||C| \left(2 - \frac{p}{|H|}\right) > p.
\]

Next, applying Theorem 1: \(|A||C|, \sqrt{\|B\||Y||D||W|} \geq 10p\), and the value set
\[
|H| = (p - 1) + \frac{\theta p^2}{10 \sqrt{|B||Y||D||W|}} \geq \frac{3}{5} p.
\]

we get
\[
|A||C| \left(2 - \frac{p}{|H|}\right) > 10p \left(2 - \frac{p}{3p/5}\right) \geq \frac{10}{3} p.
\]

Therefore Eq. (11) holds.

Finally, let \(\lambda\) be any integer. It is clear that
\[
\#\{\lambda - (b_0 + y_0)A - (d_0 + w_0)C\} > p/2.
\]

By the pigeonhole principle there exist fixed elements \(a', a'' \in A, c', c'' \in C\), 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

\[ b_i' \in B_i, \quad 1 \leq i \leq 8, \]

such that

\[ \#\{ (b_1' + b_2'A_1) + (b_3' + b_4')A_3 \} > p/2, \quad \#\{ (b_5' + b_6')A_5 + (b_7' + b_8')A_7 \} > p/2. \]

Let \( \lambda \) be any integer. It is clear that

\[ \#\{ \lambda - (b_5' + b_6')A_5 - (b_7' + b_8')A_7 \} > p/2. \]

Hence, by the pigeon-hole principle there exist elements

\[ a_1' \in A_1, \quad a_3' \in A_3, \quad a_5' \in A_5, \quad a_7' \in A_7, \]

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.

