Sums of Residues in the Field Fp

Rafael Jakimczuk

División Matemática, Universidad Nacional de Luján
Buenos Aires, Argentina
jakimczu@mail.unlu.edu.ar

Abstract

Let us consider the linear equation in Fp,

\[ A_1 x_1 + \ldots + A_r x_r = A \quad (r \geq 1) \]

It is well known that if some \( A_i \) is nonzero, then the number \( N \) of solutions \((x_1, \ldots, x_r)\) to this linear equation is \( N = p^{r-1} \).

In this article we study the number \( N' \) of solutions \((x_1, \ldots, x_r)\) to this linear equation where these solutions have some restriction. For example, the \( x_i \) are different of zero, the \( x_i \) are different each other, the \( x_i \) are different of zero and different each other.

We also study the number of sums of elements of Fp which have a same result, where the order of the sumands is irrelevant and some restriction of the former type is established.

Mathematics Subject Classification: 11A15, 11D45, 11A41

Keywords: The linear equation in Fp, solutions with restrictions, sums of residues in Fp

1 Introduction

The elements in the field Fp are \( \{0, 1, \ldots, p-1\} \). Let us consider the linear equation in Fp,

\[ A_1 x_1 + \ldots + A_r x_r = A \quad (r \geq 1) \]

It is well known (see [2], page 34) that if some \( A_i \) is nonzero, then the number \( N \) of solutions \((x_1, \ldots, x_r)\) to this linear equation is

\[ N = p^{r-1} \]

Note that (2) does not depend of the \( A_i \) \((i = 1, \ldots, r)\).
In this article we are interested in the number \( N' \) of solutions \((x_1, \ldots, x_r)\) to (1) where these solutions have some restriction. For example, the \( x_i \) are different of zero, the \( x_i \) are different each other, the \( x_i \) are different of zero and different each other.

We also are interested in the number of sums of elements of \( \mathbb{F}_p \) which have a same result, where the order of the sumands is irrelevant and some restriction of the former type is established.

In this class of problems a general combinatorial theorem is frequently used. This theorem is sometimes called the principle of cross-classification (see [2], page 84). We now enunciate the principle.

**Theorem 1.1** Principle of cross-classification. Let \( S \) be a set of \( N \) distinct elements, and let \( S_1, \ldots, S_r \) be arbitrary subsets of \( S \) containing \( N_1, \ldots, N_r \) elements, respectively. For \( 1 \leq i < j < \ldots < l \leq r \), let \( S_{ij \ldots l} \) be the intersection of \( S_i, S_j, \ldots, S_l \) and let \( N_{ij \ldots l} \) be the number of elements of \( S_{ij \ldots l} \). Then the number of elements of \( S \) not in any of \( S_1, \ldots, S_r \) is

\[
K = N - \sum_{1 \leq i \leq r} N_i + \sum_{1 \leq i < j \leq r} N_{ij} - \sum_{1 \leq i < j < k \leq r} N_{ijk} + \ldots + (-1)^r N_{12\ldots r} \tag{3}
\]

Proof. See, for example, [2] (page 84) or [1] (page 233).

We have the following theorem.

**Theorem 1.2** Let us consider the equation \((r \geq 1)\)

\[
A_1 x_1 + \ldots + A_r x_r = R \quad (R \neq 0) \tag{4}
\]

Where \( A_i \neq 0 \) \((i = 1, 2, \ldots, r)\).

The number of solutions \((x_1, \ldots, x_r)\) to this equation where \( x_i \neq 0 \) \((i = 1, \ldots, r)\) is

\[
p^{r-1} - \binom{r}{1} p^{r-2} + \binom{r}{2} p^{r-3} - \ldots + (-1)^{r-1} \binom{r}{r-1} p^0 \tag{5}
\]

Let us consider the equation \((r \geq 1)\)

\[
A_1 x_1 + \ldots + A_r x_r = 0 \tag{6}
\]

Where \( A_i \neq 0 \) \((i = 1, 2, \ldots, r)\).

The number of solutions \((x_1, \ldots, x_r)\) to this equation where \( x_i \neq 0 \) \((i = 1, \ldots, r)\) is

\[
p^{r-1} - \binom{r}{1} p^{r-2} + \binom{r}{2} p^{r-3} - \ldots + (-1)^{r-1} \binom{r}{r-1} p^0 + (-1)^r \tag{7}
\]
Proof. The proof is an application of the principle of cross-classification.
Consider equation (4). In this case:
\[ S \] is the set of all solutions \((x_1, \ldots, x_r)\) to (4). Therefore \(N = p^{r-1}\) (see (2)).

\[ S_i \ (i = 1, \ldots, r) \] is the set of all solutions \((x_1, \ldots, x_r)\) to (4) such that \(x_i = 0\). Therefore \(N_i = p^{r-2}\) (see (2)).

\[ S_{ij} \ (1 \leq i < j \leq r) \] is the set of all solutions \((x_1, \ldots, x_r)\) to (4) such that \(x_i = x_j = 0\). Therefore \(N_{ij} = p^{r-3}\) (see (2)).

\[ \vdots \]

\(S_{12, \ldots, r}\) is the set of all solutions \((x_1, \ldots, x_r)\) to (4) such that \(x_1 = x_2 = \ldots = x_r = 0\). Therefore \(S_{12, \ldots, r}\) is empty and \(N_{12, \ldots, r} = 0\).

Consequently applying (3) we obtain (5).

Equation (7) can be proved in the same way. The theorem is proved.

**Example 1.3** Let us consider the equations

\[
A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4 = R \quad (R \neq 0)
\]  

(8)

\[
A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4 = 0
\]  

(9)

Where \(p\) is a prime such that the following condition holds: \(A_i \neq 0\) (\(i = 1, 2, 3, 4\)), \(A_i + A_j \neq 0\) (\(1 \leq i < j \leq 4\)), \(A_i + A_j + A_k \neq 0\) (\(1 \leq i < j < k \leq 4\)) and \(A_1 + A_2 + A_3 + A_4 \neq 0\).

We wish obtain the number of solutions \((x_1, x_2, x_3, x_4)\) to these equations such that the \(x_i\) (\(i = 1, 2, 3, 4\)) are different of zero and different each other.

We shall apply the principle of cross-classification.

Consider the equation (8). In this case \(S\) is the set of all solutions \((x_1, x_2, x_3, x_4)\) to (8) such that the \(x_i\) (\(i = 1, 2, 3, 4\)) are different of zero. Therefore (see (5)) \(N = p^3 - 4p^2 + 6p - 4\).

\(S_1\) is the set of all solutions \((x_1, x_2, x_3, x_4)\) to (8) such that the \(x_i\) (\(i = 1, 2, 3, 4\)) are different of zero and \(x_1 = x_2\). Consequently \(N_1\) is the number of solutions \((x_1, x_2, x_3)\) such that the \(x_i\) (\(i = 1, 2, 3\)) are different of zero to the equation

\[
(A_1 + A_2)x_1 + A_3 x_2 + A_4 x_3 = R
\]

Therefore (see 5) \(N_1 = p^2 - 3p + 3\).

\(S_2\) is the set of all solutions \((x_1, x_2, x_3, x_4)\) to (8) such that the \(x_i\) (\(i = 1, 2, 3, 4\)) are different of zero and \(x_1 = x_3\). Consequently \(N_2\) is the number of solutions \((x_1, x_2, x_3)\) such that the \(x_i\) (\(i = 1, 2, 3\)) are different of zero to the equation

\[
(A_1 + A_3)x_1 + A_2 x_2 + A_4 x_3 = R
\]

Therefore (see 5) \(N_2 = p^2 - 3p + 3\).
$S_3$ is the set of all solutions $(x_1, x_2, x_3, x_4)$ to (8) such that the $x_i$ $(i = 1, 2, 3, 4)$ are different of zero and $x_1 = x_4$. Consequently $N_3$ is the number of solutions $(x_1, x_2, x_3)$ such that the $x_i$ $(i = 1, 2, 3)$ are different of zero to the equation

$$(A_1 + A_4)x_1 + A_2x_2 + A_3x_3 = R$$

Therefore (see 5) $N_3 = p^2 - 3p + 3$.

$S_4$ is the set of all solutions $(x_1, x_2, x_3, x_4)$ to (8) such that the $x_i$ $(i = 1, 2, 3, 4)$ are different of zero and $x_2 = x_3$. Consequently $N_4$ is the number of solutions $(x_1, x_2, x_3)$ such that the $x_i$ $(i = 1, 2, 3)$ are different of zero to the equation

$$(A_2 + A_3)x_1 + A_1x_2 + A_4x_3 = R$$

Therefore (see 5) $N_4 = p^2 - 3p + 3$.

$S_5$ is the set of all solutions $(x_1, x_2, x_3, x_4)$ to (8) such that the $x_i$ $(i = 1, 2, 3, 4)$ are different of zero and $x_3 = x_4$. Consequently $N_5$ is the number of solutions $(x_1, x_2, x_3)$ such that the $x_i$ $(i = 1, 2, 3)$ are different of zero to the equation

$$(A_3 + A_4)x_1 + A_1x_2 + A_2x_3 = R$$

Therefore (see 5) $N_5 = p^2 - 3p + 3$.

We shall denote the sets $S_1$, $S_2$, $S_3$, $S_4$, $S_5$ and $S_6$ in the form

$$x_1 = x_2 \quad x_1 = x_3 \quad x_1 = x_4 \quad x_2 = x_3 \quad x_2 = x_4 \quad x_3 = x_4$$

respectively. For example, the set $S_{13}$ we shall denote in the form

$$x_1 = x_2 \quad x_1 = x_4$$

etc.

Consequently the \( \binom{n}{2} \) = 15 sets $S_{ij}$ $(1 \leq i < j \leq 6)$ will be

$$x_1 = x_2 \quad x_1 = x_3 \quad x_1 = x_4 \quad x_2 = x_3 \quad x_2 = x_4 \quad x_3 = x_4$$
Let us consider the set $S_{12}$. Consequently $N_{12}$ is the number of solutions $(x_1, x_2)$ where $x_1$ and $x_2$ are different of zero to the equation

$$(A_1 + A_2 + A_3)x_1 + A_4x_4 = R$$

That is (see (5)) $N_{12} = p - 2$.

In the same way we obtain that $N_{ij} = p - 2$ $(1 \leq i < j \leq 6)$.

The $\binom{6}{3} = 20$ sets $S_{ijk}$ $(1 \leq i < j < k \leq 6)$ will be

$$x_1 = x_2 \quad x_1 = x_2 \quad x_1 = x_2 \quad x_1 = x_2 \quad x_1 = x_2$$

$$x_1 = x_3 \quad x_1 = x_3 \quad x_1 = x_3 \quad x_1 = x_3 \quad x_1 = x_4$$

$$x_1 = x_4 \quad x_2 = x_3 \quad x_2 = x_4 \quad x_3 = x_4 \quad x_2 = x_3$$

$$x_1 = x_2 \quad x_1 = x_2 \quad x_1 = x_2 \quad x_1 = x_2 \quad x_1 = x_2$$

$$x_1 = x_4 \quad x_1 = x_4 \quad x_2 = x_3 \quad x_2 = x_4 \quad x_2 = x_4$$

$$x_2 = x_4 \quad x_3 = x_4 \quad x_2 = x_4 \quad x_3 = x_4 \quad x_3 = x_4$$

$$x_1 = x_3 \quad x_1 = x_3 \quad x_1 = x_3 \quad x_1 = x_3 \quad x_1 = x_3$$

$$x_1 = x_4 \quad x_1 = x_4 \quad x_1 = x_4 \quad x_2 = x_3 \quad x_2 = x_3$$

$$x_2 = x_3 \quad x_2 = x_4 \quad x_3 = x_4 \quad x_2 = x_4 \quad x_3 = x_4$$

$$x_1 = x_3 \quad x_1 = x_4 \quad x_1 = x_4 \quad x_1 = x_4 \quad x_2 = x_3$$

$$x_2 = x_4 \quad x_2 = x_3 \quad x_2 = x_3 \quad x_2 = x_4 \quad x_2 = x_4$$

$$x_3 = x_4 \quad x_2 = x_4 \quad x_3 = x_4 \quad x_3 = x_4 \quad x_3 = x_4$$

In these 20 sets $S_{ijk}$ there are 16 sets $S_{ijk}$ such that $N_{ijk}$ is the number of solutions $x_1$ where $x_1 \neq 0$ to the equation

$$(A_1 + A_2 + A_3 + A_4)x_1 = R$$

Therefore (see (5)) $N_{ijk} = 1$.

On the other hand, there are 4 sets $S_{ijk}$ $(S_{124}, S_{135}, S_{236}, S_{456})$ such that:

$N_{124}$ is the number of solutions $(x_1, x_2)$ where $x_1$ and $x_2$ are different of zero to the equation

$$(A_1 + A_2 + A_3)x_1 + A_4x_2 = R$$
Therefore (see (5)) \( N_{124} = p - 2 \). Analogously we also obtain that \( N_{135} = N_{236} = N_{456} = p - 2 \)

The \( \binom{6}{4} = 15 \) sets \( S_{ijkl} \) (1 \( \leq i < j < k < l \leq 6 \)) will be

\[
\begin{align*}
    x_1 &= x_2 & x_1 &= x_2 & x_1 &= x_2 & x_1 &= x_2 & x_1 &= x_2 \\
    x_1 &= x_3 & x_1 &= x_3 & x_1 &= x_3 & x_1 &= x_3 & x_1 &= x_3 \\
    x_1 &= x_4 & x_1 &= x_4 & x_1 &= x_4 & x_2 &= x_3 & x_2 &= x_3 \\
    x_2 &= x_3 & x_2 &= x_3 & x_3 &= x_4 & x_2 &= x_4 & x_3 &= x_4
\end{align*}
\]

Consequently \( N_{ijkl} \) is the number of solutions \( x_1 \) where \( x_1 \neq 0 \) to the equation

\[
(A_1 + A_2 + A_3 + A_4)x_1 = R
\]

Therefore (see (5)) \( N_{ijkl} = 1 \)

The \( \binom{6}{5} = 6 \) sets \( S_{ijklm} \) (1 \( \leq i < j < k < l < m \leq 6 \)) will be

\[
\begin{align*}
    x_1 &= x_2 & x_1 &= x_2 & x_1 &= x_2 & x_1 &= x_2 & x_1 &= x_3 \\
    x_1 &= x_3 & x_1 &= x_3 & x_1 &= x_3 & x_1 &= x_3 & x_1 &= x_4 \\
    x_1 &= x_4 & x_1 &= x_4 & x_1 &= x_4 & x_2 &= x_3 & x_2 &= x_3 \\
    x_2 &= x_3 & x_2 &= x_3 & x_2 &= x_3 & x_2 &= x_4 & x_2 &= x_4 \\
    x_2 &= x_4 & x_3 &= x_4 & x_3 &= x_4 & x_3 &= x_4 & x_3 &= x_4
\end{align*}
\]

Consequently \( N_{ijklm} \) is the number of solutions \( x_1 \) where \( x_1 \neq 0 \) to the equation

\[
(A_1 + A_2 + A_3 + A_4)x_1 = R
\]

Therefore (see (5)) \( N_{ijklm} = 1 \)
The set \( S_{123456} \) will be
\[
\begin{align*}
x_1 &= x_2 \\
x_1 &= x_3 \\
x_1 &= x_4 \\
x_2 &= x_3 \\
x_2 &= x_4 \\
x_3 &= x_4 
\end{align*}
\]
Consequently \( N_{123456} \) is the number of solutions \( x_1 \) where \( x_1 \neq 0 \) to the equation
\[
(A_1 + A_2 + A_3 + A_4)x_1 = R
\]
Therefore (see (5)) \( N_{123456} = 1 \)
Finally, using (3) we obtain that the number of solutions \((x_1, x_2, x_3, x_4)\) to (8) such that the \( x_i \) (\( i = 1, 2, 3, 4 \)) are different of zero and different each other will be
\[
\begin{align*}
&= (p^3 - 4p^2 + 6p - 4) - 6(p^2 - 3p + 3) + 15(p - 2) - (4(p - 2) + 16) \\
&+ 15 - 6 + 1 = p^3 - 10p^2 + 35p - 50 \tag{10}
\end{align*}
\]
In the same way, we obtain that the number of solutions \((x_1, x_2, x_3, x_4)\) to (9) such that the \( x_i \) (\( i = 1, 2, 3, 4 \)) are different of zero and different each other will be
\[
\begin{align*}
&= (p^3 - 4p^2 + 6p - 4 + 1) - 6(p^2 - 3p + 3 - 1) + 15(p - 2 + 1) \\
&- (4(p - 2 + 1) + 0) + 0 - 0 + 0 = p^3 - 10p^2 + 35p - 26 \tag{11}
\end{align*}
\]
In this example (where only \( r = 4 \)) we see that the application of this principle is very troublesome. It does not give us general formulas as (5) and (7), or if it gives one is difficult to obtain. In the next section, we shall obtain using other approach a simple general formula.
However we can obtain an important consequence of the application of this principle.
Note that (10) and (11) do not depend of \( A_1, A_2, A_3, A_4 \). Clearly this is general. Therefore we have the following theorem.

**Theorem 1.4** Let us consider the equation
\[
A_1 x_1 + \ldots + A_r x_r = R \quad (R \neq 0)
\]
Where \( p \) is a prime such that the following condition holds: \( A_i \neq 0 \) (\( i = 1, \ldots, r \)), \( A_i + A_j \neq 0 \) (\( 1 \leq i < j \leq r \)), \( A_i + A_j + A_k \neq 0 \) (\( 1 \leq i < j < k \leq r \)), \ldots, \( A_1 + \ldots + A_r \neq 0 \).
The number of solutions \((x_1, \ldots, x_r)\) to this equation where the \(x_i\) are different of zero and different each other does not depend of the \(A_i\) \((i = 1, \ldots, r)\).

Let us consider the equation

\[ A_1 x_1 + \ldots + A_r x_r = 0 \]

Where \(p\) is a prime such that the following condition holds: \(A_i \neq 0\) \((i = 1, \ldots, r)\), \(A_i + A_j \neq 0\) \((1 \leq i < j \leq r)\), \(A_i + A_j + A_k \neq 0\) \((1 \leq i < j < k \leq r)\), \ldots, \(A_1 + \ldots + A_r \neq 0\).

The number of solutions \((x_1, \ldots, x_r)\) to this equation where the \(x_i\) are different of zero and different each other does not depend of the \(A_i\) \((i = 1, \ldots, r)\).

**Remark.** Note that the condition: \(A_i \neq 0\) \((i = 1, \ldots, r)\), \(A_i + A_j \neq 0\) \((1 \leq i < j \leq r)\), \(A_i + A_j + A_k \neq 0\) \((1 \leq i < j < k \leq r)\), \ldots, \(A_1 + \ldots + A_r \neq 0\), holds for every prime \(p > A_1 + \ldots + A_r\). However also the condition can be satisfied by a prime \(p\) such that \(p < A_1 + \ldots + A_r\). For example, consider the equations:

\[ 6x_1 + 5x_2 + 5x_3 = A \]
\[ 6x_1 + 5x_2 + 5x_3 = 0 \]

Si \(p = 7\) we have \(7 < 16\) and the condition is clearly satisfied. This condition will be used in theorems 2.2 and 2.4.

## 2 The other approach

If \(A \neq 0\), let \(N(r, 1)\) be the number of solutions \((x_1, \ldots, x_r)\) to (1) where the \(x_i\) are different each other. Clearly \(N(r, 1)\) does not depend of \(A\) since if we wish change \(A\) we can multiply both sides of (1) by a certain nonzero element of \(F_p\).

If \(A = 0\), let \(N(r, 0)\) be the number of solutions \((x_1, \ldots, x_r)\) to (1) where the \(x_i\) are different each other.

We have the following theorem.

**Theorem 2.1** If \(p\) is a prime such that \(A_1 + \ldots + A_r \neq 0\) (see (1)), then the following formula holds

\[ N(r, 1) = N(r, 0) = (p - 1)(p - 2) \ldots (p - (r - 1)) \quad (r \geq 2) \quad (12) \]
\[ N(1, 1) = N(1, 0) = 1 \quad (13) \]

Proof. Let \((x_1, \ldots, x_r)\) be a solution where the \(x_i\) are different each other to the equation

\[ A_1 x_1 + \ldots + A_r x_r = 0 \quad (14) \]
Then \((x_1 + 1, \ldots, x_r + 1)\) is a solution where the \(x_i + 1\) are different each other to the equation

\[
A_1 x_1 + \ldots + A_r x_r = A_1 + \ldots + A_r = A \neq 0
\] (15)

Conversely, let \((x_1, \ldots, x_r)\) be a solution where the \(x_i\) are different each other to the equation

\[
A_1 x_1 + \ldots + A_r x_r = A_1 + \ldots + A_r = A \neq 0
\]

Then \((x_1 + (p - 1), \ldots, x_r + (p - 1))\) is a solution where the \(x_i + (p - 1)\) are different each other to the equation

\[
A_1 x_1 + \ldots + A_r x_r = 0
\]

Consequently \(N(r, 1) = N(r, 0)\). The number of all possibles \(r\)-tuples \((x_1, \ldots, x_r)\) where the \(x_i\) are different each other is equal to the number of \(r\)-permutations of the set of \(p\) elements \(\{0, 1, \ldots, p - 1\}\). That is,

\[
p(p - 1)(p - 2) \ldots (p - (r - 1))
\]

This number is also equal to

\[
(p - 1)N(r, 1) + N(r, 0) = (p - 1)N(r, 0) + N(r, 0) = pN(r, 0)
\]

Therefore

\[
N(r, 0) = (p - 1)(p - 2) \ldots (p - (r - 1))
\]

The theorem is proved.

**Remark.** Note that if \(p \leq r - 1\) then \(N(r, 1) = N(r, 0) = 0\).

**Remark.** The equality \(N(r, 1) = N(r, 0)\) also can be proved easily using the cross-classification principle and equation (2).

If \(A \neq 0\), let \(P(r, 1)\) be the number of solutions \((x_1, \ldots, x_r)\) to (1) where the \(x_i\) are different of zero and different each other. Clearly \(P(r, 1)\) does not depend of \(A\) since if we wish change \(A\) we can multiply both sides of (1) by a certain nonzero element of \(F_p\).

If \(A = 0\), let \(P(r, 0)\) be the number of solutions \((x_1, \ldots, x_r)\) to (1) where the \(x_i\) are different of zero and different each other.

**Remark.** Note that if \(p \leq r\) then \(P(r, 1) = P(r, 0) = 0\).

We have the following theorem.
Theorem 2.2 Let $p > r$ a prime such that the following condition holds (see (1)): $A_i \neq 0$ ($i = 1, \ldots, r$), $A_i + A_j \neq 0$ ($1 \leq i < j \leq r$), $A_i + A_j + A_k \neq 0$ ($1 \leq i < j < k \leq r$), $\ldots$, $A_1 + \ldots + A_r \neq 0$.

Then if $r$ is even,

$$P(r, 1) - P(r, 0) = -r!$$

(16)

On the other hand, if $r$ is odd,

$$P(r, 1) - P(r, 0) = r!$$

(17)

Proof. If $r = 1$ we have

$$P(1, 1) = 1 = 0 + 1! = P(1, 0) + 1!$$

That is

$$P(1, 1) - P(1, 0) = 1!$$

Since $P(1, 1) = 1$ is the number of solutions different of zero to the equation $A_1x_1 = A \neq 0$ and $P(1, 0) = 0$ is the number of solutions different of zero to the equation $A_1x_1 = 0$.

Suppose the theorem holds for $n$ odd. That is

$$P(n, 1) - P(n, 0) = n!$$

(18)

We shall prove the theorem also holds for $n + 1$ (even).

Let us consider the equations

$$A_1x_1 + \ldots + A_{n+1}x_{n+1} = A \neq 0$$

$$A_1x_1 + \ldots + A_{n+1}x_{n+1} = 0$$

We have

$$N(n + 1, 1) = P(n + 1, 1) + (n + 1)P(n, 1)$$

(19)

$$N(n + 1, 0) = P(n + 1, 0) + (n + 1)P(n, 0)$$

(20)

Where $P(n, 1)$ is the number of solutions $(x_1, \ldots, x_n)$ to the $n + 1$ equations (see theorem 1.4)

$$A_2x_1 + A_3x_2 + \ldots + A_{n+1}x_{n+1} = A \neq 0$$

$$A_1x_1 + A_3x_2 + \ldots + A_{n+1}x_{n+1} = A \neq 0$$

$$\vdots$$

$$A_1x_1 + A_2x_2 + \ldots + A_nx_n = A \neq 0$$

and $P(n, 0)$ is the number of solutions $(x_1, \ldots, x_n)$ to the $n + 1$ equations (see theorem 1.4)

$$A_2x_1 + A_3x_2 + \ldots + A_{n+1}x_{n+1} = 0$$
\[ A_1 x_1 + A_3 x_2 + \ldots + A_{n+1} x_{n+1} = 0 \]
\[ \vdots \]
\[ A_1 x_1 + A_2 x_2 + \ldots + A_n x_n = 0 \]

(19) and (20) give (see theorem 2.1)

\[ N(n+1,1) - N(n+1,0) = 0 = P(n+1,1) - P(n+1,0) + (n+1)(P(n,1) - P(n,0)) \]

That is (see (18))

\[ P(n+1,1) - P(n+1,0) = -(n+1)! \]

Now, suppose the theorem holds for \( n \) even. That is

\[ P(n,1) - P(n,0) = -n! \]

In the same way we can prove the theorem also holds for \( n+1 \) (odd).

The theorem is proved.

**Corollary 2.3** Consider a prime \( p \). If \( A_1, A_2, \ldots, A_p \) is a sequence of \( p \) nonzero residues in \( F_p \), then there exists a subsequence \( A_{i_1}, A_{i_2}, \ldots, A_{i_k} \) such that

\[ A_{i_1} + A_{i_2} + \ldots + A_{i_k} = 0 \quad (k \geq 2) \]  \hfill (21)

Proof. Suppose in theorem 2.2 that \( r = p \). Equations (19) and (20) are

\[ N(p,1) = P(p,1) + (n+1)P(p-1,1) \]
\[ N(p,0) = P(p,0) + (n+1)P(p-1,0) \]

Now, \( P(p,1) = P(p,0) = 0 \). Consequently \( P(p-1,1) - P(p-1,0) = 0 \). That is, an evident contradiction (see (16) and (17)).

Consequently the hypothesis in theorem 2.2: \( A_i \neq 0 \ (i = 1, \ldots, p) \), \( A_i + A_j \neq 0 \ (1 \leq i < j \leq p) \), \( A_i + A_j + A_k \neq 0 \ (1 \leq i < j < k \leq p) \), ..., \( A_1 + \ldots + A_p \neq 0 \) is not satisfied.

Therefore there exists \( A_{i_1}, A_{i_2}, \ldots, A_{i_k} \) (\( k \geq 2 \)) such that (21) holds. The proof is complete.

**Remark.** This corollary is also an immediate consequence of the Erdös-Ginzburg-Ziv theorem, see [3] (page 48).

We now can establish the theorem where we obtain the general formulas mentioned in the former section.
Theorem 2.4 If the hypothesis of theorem 2.2 is fulfilled then the following formulas hold.

If \( r \) is even

\[
P(r, 0) = \frac{(p - 1)(p - 2) \ldots (p - r) + (p - 1)r!}{p}
\]  \hspace{1cm} (22)

\[
P(r, 1) = \frac{(p - 1)(p - 2) \ldots (p - r) - r!}{p}
\]  \hspace{1cm} (23)

If \( r \) is odd

\[
P(r, 0) = \frac{(p - 1)(p - 2) \ldots (p - r) - (p - 1)r!}{p}
\]  \hspace{1cm} (24)

\[
P(r, 1) = \frac{(p - 1)(p - 2) \ldots (p - r) + r!}{p}
\]  \hspace{1cm} (25)

Proof. The number of all possible \( r \)-tuples \( (x_1, \ldots, x_r) \) where the \( x_i \) are different of zero and different each other is equal to the number of \( r \)-permutations of the set of \( p - 1 \) elements \( \{1, \ldots, p - 1\} \). That is,

\[(p - 1)(p - 2) \ldots (p - r)\]

This number is also equal to

\[(p - 1)P(r, 1) + P(r, 0)\]

Therefore

\[(p - 1)(p - 2) \ldots (p - r) = (p - 1)P(r, 1) + P(r, 0)\]  \hspace{1cm} (26)

Consequently, if \( r \) is even we have (see (16))

\[(p - 1)(p - 2) \ldots (p - r) = (p - 1)(P(r, 0) - r!) + P(r, 0)\]

That is

\[P(r, 0) = \frac{(p - 1)(p - 2) \ldots (p - r) + (p - 1)r!}{p}\]

From (16) we obtain

\[P(r, 1) = \frac{(p - 1)(p - 2) \ldots (p - r) + (p - 1)r!}{p} - r!\]

\[= \frac{(p - 1)(p - 2) \ldots (p - r) - r!}{p}\]

The other two formulas can be proved in the same way using (17). The theorem is thus proved.
Remark. Note that these formulas are polynomials in \( p \) since the constant coefficient in the polynomial numerator is clearly zero. Furthermore, these polynomials have degree \( r - 1 \), integral coefficientes alternating in sign and leading coefficient 1 (that is, they are monics).

**Example 2.5** If \( r = 1 \) then

\[
P(1, 0) = 0 \\
P(1, 1) = 1
\]

If \( r = 2 \) then

\[
P(2, 0) = p - 1 \\
P(2, 1) = p - 3
\]

If \( r = 3 \) then

\[
P(3, 0) = p^2 - 6p + 5 \\
P(3, 1) = p^2 - 6p + 11
\]

If \( r = 4 \) (see (10) and (11) in example 1.3) then

\[
P(4, 0) = p^3 - 10p^2 + 35p - 26 \\
P(4, 1) = p^3 - 10p^2 + 35p - 50
\]

If \( r = 5 \) then

\[
P(5, 0) = p^4 - 15p^3 + 85p^2 - 225p + 154 \\
P(5, 1) = p^4 - 15p^3 + 85p^2 - 225p + 274
\]

**Theorem 2.6** The following recursive formula holds

\[
P(r + 1, 0) = (p - 1)P(r, 1) - rP(r, 0) \tag{27}
\]

Proof. If \( r \) is even we have

\[
(p - 1)P(r, 1) - rP(r, 0) = (p - 1) \frac{(p - 1)(p - 2) \ldots (p - r) - r!}{p}
\]
\[
= \frac{(p - 1)(p - 2) \ldots (p - (r + 1)) - (p - 1)(r + 1)!}{p} = P(r + 1, 0)
\]

On the other hand, if \( r \) is odd we have

\[
(p - 1)P(r, 1) - rP(r, 0) = (p - 1) \frac{(p - 1)(p - 2) \ldots (p - r) + r!}{p}
\]
\[
= \frac{(p - 1)(p - 2) \ldots (p - (r + 1)) + (p - 1)(r + 1)!}{p} = P(r + 1, 0)
\]

The proof of (27) is complete.
3 Sums of elements in $\mathbb{F}_p$

**Definition 3.1** Let $A$ be an element of $\mathbb{F}_p$. Let us consider the set (possibly empty) of all sums (the order of the nonzero summands is irrelevant) whose result is $A$ and such that they have $L$ ($L \geq 1$) different summands, $t$ ($t \geq 1$) summands, and furthermore $L_1$ different summands appear $K_1$ times each, $L_2$ different summands appear $K_2$ times each, ..., $L_m$ different summands appear $K_m$ times each ($K_1 > K_2 > \ldots > K_m$). The set of these sums we shall call structure.

We shall denote the number of sums in a structure where $A \neq 0$ in the form:

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m; A)$$

Clearly this number does not depend of $A$, since if we wish change $A$ we can multiply both sides of each sum in the structure by a certain nonzero element of $\mathbb{F}_p$. On the other hand, we shall denote the number of sums in a structure where $A = 0$ in the form:

$$(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m; 0)$$

Note that

$$L_1 + L_2 + \ldots + L_m = L$$

$$L_1 K_1 + L_2 K_2 + \ldots + L_m K_m = t$$

**Example 3.2** Suppose $p = 11$. The sum $5 + 5 + 5 + 4 + 4 + 4 + 7 + 7 + 1 = 9$ belongs to the structure $(2, 3 : 1, 2 : 1, 1; 9)$

Note that if $t$ is fixed the number of different structures corresponding to $t$ is equal to 2 times the number of partitions of $t$ ($p(t)$).

**Example 3.3** All structures corresponding to $t = 4$ are:

<table>
<thead>
<tr>
<th>Structure</th>
<th>Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(4, 1; A)$</td>
<td>$1 + 1 + 1 + 1 = 4$</td>
</tr>
<tr>
<td>$(4, 1; 0)$</td>
<td>$1 + 1 + 1 + 1 = 4$</td>
</tr>
<tr>
<td>$(1, 2 : 2, 1; A)$</td>
<td>$2 + 1 + 1 = 4$</td>
</tr>
<tr>
<td>$(1, 2 : 2, 1; 0)$</td>
<td>$2 + 1 + 1 = 4$</td>
</tr>
<tr>
<td>$(1, 3 : 1, 1; A)$</td>
<td>$3 + 1 = 4$</td>
</tr>
<tr>
<td>$(1, 3 : 1, 1; 0)$</td>
<td>$3 + 1 = 4$</td>
</tr>
</tbody>
</table>
Theorem 3.4 If \( p > t \) then the following formulas hold,

\[
(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m; A) = \frac{P(L, 1)}{L_1!L_2!\ldots L_m!} \tag{28}
\]

\[
(L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m; 0) = \frac{P(L, 0)}{L_1!L_2!\ldots L_m!} \tag{29}
\]

Proof. Let us consider the equation

\[
K_1 x_1 + \ldots + K_1 x_{L_1} + K_2 x_{L_1+1} + \ldots + K_2 x_{L_1+L_2} + \ldots + K_m x_{L_1+\ldots+L_{m-1}+1} + \ldots + K_m x_{L_1+\ldots+L_m} = A \tag{30}
\]

The number of solutions \((x_1, \ldots, x_{L_1+\ldots+L_m} = x_L)\) to this equation where the \(x_i\) are nonzero and different each other is \(P(L, 1)\). Now, \(K_1\) repeat \(L_1\) times, \(K_2\) repeat \(L_2\) times, \ldots, \(K_m\) repeat \(L_m\) times. Consequently (28) holds.

Equation (29) can be proved in the same way. The theorem is proved.

We shall need the following well known combinatorial result.

Lemma 3.5 Let \( S \) be a set of \( n \) objects. The number of combinations of \( m \) objects \((1 \leq m < n, m = n, m > n)\) where repetition of objects is permitted is

\[
\binom{m+n-1}{m} \tag{31}
\]

If \( A \neq 0 \), let \( S(t, 1) \) be the number of sums (the order of the summands is irrelevant) of \( t \) residues whose result is \( A \). Clearly \( S(t, 1) \) does not depend of \( A \). If \( A = 0 \), let \( S(t, 0) \) be the number of sums (the order of the summands is irrelevant) of \( t \) residues whose result is 0.

Lemma 3.6 If \( p > t \) then

\[
S(t, 1) = S(t, 0) = \binom{p+t-1}{t} \quad (t \geq 1)
\]

Proof. Consider a sum whose result is zero. If we add 1 to each summand then obtain a sum whose result is \( t \). Conversely, consider a sum whose result is \( t \). If we add \( p - 1 \) to each summand then obtain a sum whose result is zero. Consequently \( S(t, 1) = S(t, 0) \). The rest of the proof is a consequence of (31). The lemma is proved.
Example 3.7 Suppose $p = 5$. If $t = 1$ we have

\[ 0 = 0 \quad 1 = 1 \quad 2 = 2 \quad 3 = 3 \quad 4 = 4 \]

Consequently $S(1,1) = S(1,0) = 1$. If $t=2$ we have

\[
\begin{align*}
0 + 0 &= 0 & 0 + 1 &= 1 & 0 + 2 &= 2 & 0 + 3 &= 3 & 0 + 4 &= 4 \\
1 + 4 &= 0 & 2 + 4 &= 1 & 1 + 1 &= 2 & 1 + 2 &= 3 & 1 + 3 &= 4 \\
2 + 3 &= 0 & 3 + 3 &= 1 & 3 + 4 &= 2 & 4 + 4 &= 3 & 2 + 2 &= 4
\end{align*}
\]

Consequently $S(2,1) = S(2,0) = 3$. If $t=3$ we have

\[
\begin{align*}
0 + 0 + 0 &= 0 & 0 + 0 + 1 &= 1 & 0 + 0 + 2 &= 2 & 0 + 0 + 3 &= 3 \\
0 + 1 + 4 &= 0 & 0 + 2 + 4 &= 1 & 0 + 1 + 1 &= 2 & 0 + 1 + 2 &= 3 \\
0 + 2 + 3 &= 0 & 0 + 3 + 3 &= 1 & 0 + 3 + 4 &= 2 & 0 + 4 + 4 &= 3 \\
2 + 2 + 1 &= 0 & 2 + 2 + 2 &= 1 & 4 + 4 + 4 &= 2 & 1 + 1 + 1 &= 3 \\
2 + 4 + 4 &= 0 & 1 + 1 + 4 &= 1 & 1 + 3 + 3 &= 2 & 2 + 3 + 3 &= 3 \\
1 + 1 + 3 &= 0 & 3 + 4 + 4 &= 1 & 2 + 2 + 3 &= 2 & 2 + 2 + 4 &= 3 \\
3 + 3 + 4 &= 0 & 1 + 2 + 3 &= 1 & 1 + 2 + 4 &= 2 & 1 + 3 + 4 &= 3
\end{align*}
\]

Consequently $S(3,1) = S(3,0) = 7$.

We shall write $S(t, 1) = S(t, 0) = S(t)$.

If $A \neq 0$, let $Q(t, 1)$ be the number of sums (the order of the summands is irrelevant) of $t$ nonzero elements whose result is $A$. Clearly $Q(t, 1)$ does not depend of $A$. If $A = 0$, let $Q(t, 0)$ be the number of sums (the order of the summands is irrelevant) of $t$ nonzero elements whose result is 0.

Note that

\[ Q(t, 1) = \sum (L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m; A) \quad (32) \]

Where the sum run on all $p(t)$ structures.

\[ Q(t, 0) = \sum (L_1, K_1 : L_2, K_2 : \ldots : L_m, K_m; 0) \quad (33) \]

Where the sum run on all $p(t)$ structures.
Theorem 3.8 If $p > t \geq 2$ then

$$Q(t, 1) = Q(t, 0) = \binom{(p-1)+t-1}{t} \quad (34)$$

Proof. In the $S(t+1)$ sums $(t \geq 1)$ whose result is a certain residue $r$ (zero or nonzero) we have:
- $S_1(t+1)$ sums such that in these sums some summand is zero.
- $S_2(t+1)$ sums such that all $t$ summands are nonzero.

Therefore

$$S(t + 1) = S_1(t + 1) + S_2(t + 1) \quad (35)$$

For example if $p = 5$, $t = 3$ and $r = 3$ we have (see example 3.7) $S(3) = 7 = S_1(3) + S_2(3) = 3 + 4 = 7$

The $S_1(t+1)$ sums are obtained from the $S(t)$ sums whose result is $r$ adding to these sums the summand zero.

For example (see example 3.7) if $p = 5$, $t = 3$ and $r = 3$ we have that the $S_1(3)$ sums, namely

- $0 + 0 + 3 = 3$
- $0 + 1 + 2 = 3$
- $0 + 4 + 4 = 3$

are obtained from the $S(2)$ sums whose result is $r = 3$, namely

- $0 + 3 = 3$
- $1 + 2 = 3$
- $4 + 4 = 3$

adding to these sums the summand zero.

Consequently

$$S_1(t + 1) = S(t) \quad (36)$$

(35) and (36) give

$$S_2(t + 1) = S(t + 1) - S(t)$$

So $S_2(t + 1)$ does not depend of $r$. Now, if $r \neq 0$ then $S_2(t + 1) = Q(t + 1, 1)$ and if $r = 0$ then $S_2(t + 1) = Q(t + 1, 0)$. Therefore $Q(t + 1, 1) = Q(t + 1, 0)$. Therefore $Q(t + 1, 1) = Q(t + 1, 0)$. The rest of the proof is a consequence of (31). The theorem is thus proved.

Example 3.9 We have (see (34))

$$Q(4, 1) = Q(4, 0) = \frac{(p+2)(p+1)p(p-1)}{4!p} = \frac{p^3 + 2p^2 - p - 2}{24} \quad (37)$$
We also can obtain (37) from (32) and (33). Since we have (see (28), (29) example 3.3 and example 2.5)

\[
(4, 1; A) = P(4, 1)/4! = \frac{p^3 - 10p^2 + 35p - 50}{24}
\]

\[
(4, 1; 0) = P(4, 0)/4! = \frac{p^3 - 10p^2 + 35p - 26}{24}
\]

\[
(1, 2 : 2, 1; A) = P(3, 1)/(1!2!) = \frac{p^2 - 6p + 11}{2}
\]

\[
(1, 2 : 2, 1; 0) = P(3, 0)/(1!2!) = \frac{p^2 - 6p + 5}{2}
\]

\[
(1, 3 : 1, 1; A) = P(2, 1)/(1!1!) = p - 3
\]

\[
(1, 3 : 1, 1; 0) = P(2, 0)/(1!1!) = p - 1
\]

\[
(2, 2; A) = P(2, 1)/2! = (p - 3)/2
\]

\[
(2, 2; 0) = P(2, 0)/2! = (p - 1)/2
\]

\[
(1, 4; A) = P(1, 1)/1! = 1
\]

\[
(1, 4; 0) = P(1, 0)/1! = 0
\]

Consequently (32) gives

\[
Q(4, 1) = (4, 1; A) + (1, 2 : 2, 1; A) + (1, 3 : 1, 1; A) + (2, 2; A) + (1, 4; A)
\]

\[
= \frac{p^3 + 2p^2 - p - 2}{24}
\]

and (33) gives

\[
Q(4, 0) = (4, 1; 0) + (1, 2 : 2, 1; 0) + (1, 3 : 1, 1; 0) + (2, 2; 0) + (1, 4; 0)
\]

\[
= \frac{p^3 + 2p^2 - p - 2}{24}
\]

ACKNOWLEDGEMENTS. The author is very grateful to Universidad Nacional de Luján.

References


Received: September, 2009