St. Petersburg 2003: An alternating sum of zero-sum subset numbers

Darij Grinberg

version 14 March 2008

In this note we will solve two problems in combinatorial number theory using an easy fact on finite differences.

We start with a few preliminaries:

For any assertion $\mathcal{A}$, we denote by $[\mathcal{A}]$ the Boolean value of the assertion $\mathcal{A}$ (that is, $[\mathcal{A}] = \left\{ \begin{array}{l} 1, \text{ if } \mathcal{A} \text{ is true;} \\ 0, \text{ if } \mathcal{A} \text{ is false} \end{array} \right.$).

It is then clear that if B is a set, and $\mathcal{A}(X)$ is an assertion for every subset X of B, then

$$\sum_{X \subseteq B} [\mathcal{A}(X)] = |\{X \subseteq B \mid \mathcal{A}(X) \text{ holds}\}|.$$

Also, if $\mathcal{A}_1$, $\mathcal{A}_2$, ..., $\mathcal{A}_m$ are m assertions, then $[\mathcal{A}_1 \text{ and } \mathcal{A}_2 \text{ and ... and } \mathcal{A}_m] = \prod_{j=1}^{m} [\mathcal{A}_j]$.

A very obvious fact:

> **Lemma 0.** For any prime number p, and for any element $x \in \mathbb{F}_p$, we have $[x = 0] = 1 - x^{p-1}$.

Proof of Lemma 0. If $x = 0$, then $[x = 0] = 1$ and $1 - x^{p-1} = 1 - 0^{p-1} = 1$, so that $[x = 0] = 1 - x^{p-1}$.

If $x \neq 0$, then $[x = 0] = 0$ and $1 - x^{p-1} = 1 - 1 = 0$ because $x^{p-1} = 1$ by Fermat's Little Theorem, so that $[x = 0] = 1 - x^{p-1}$.

Hence, in both cases $x = 0$ and $x \neq 0$ we have shown that $[x = 0] = 1 - x^{p-1}$. Lemma 0 is thus proven.

Next, we will derive our lemma about finite differences. First, a trivial fact on polynomials:

Assertion 1: If P is a polynomial of one variable X over a ring R, then there exists a polynomial Q of the variable X over R such that $P(0) - P(X) = X \cdot Q(X)$.

This assertion is obvious (let $P(X) = \sum_{i=0}^{m} a_i X^i$; then,

$$P(0) - P(X) = \sum_{i=0}^{m} a_i 0^i - \sum_{i=0}^{m} a_i X^i = \left(a_0 0^0 + \sum_{i=1}^{m} a_i \underbrace{0^i}_{=0} \right) - \left(a_0 X^0 + \sum_{i=1}^{m} a_i X^i \right)$$
$$= (a_0 + 0) - \left(a_0 + \sum_{i=1}^{m} a_i X^i \right) = -\sum_{i=1}^{m} a_i X^i = X \cdot \left(-\sum_{i=1}^{m} a_i X^{i-1} \right),$$

so that $P(0) - P(X) = X \cdot Q(X)$ for $Q(X) = -\sum_{i=1}^{m} a_i X^{i-1}$).

Now, here comes our Lemma, which generalizes this assertion:

Lemma 1. Let $n \geq 1$ be an integer. Let P be a polynomial of n variables X_1, X_2, ..., X_n over a ring R. Then, there exists a polynomial Q of the variables X_1, X_2, ..., X_n over R such that

$$\sum_{T \subseteq \{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = \prod_{i=1}^{n} X_i \cdot Q\left(X_1, X_2, ..., X_n\right).$$

Hereby, for any n-tuple $(\alpha_1, \alpha_2, ..., \alpha_n)$, we denote by $(\alpha_1, \alpha_2, ..., \alpha_n) \mid_T$ the n-tuple $(\beta_1, \beta_2, ..., \beta_n)$ defined by $\beta_i = [i \in T]\,\alpha_i = \begin{cases} \alpha_i, \text{ if } i \in T; \\ 0, \text{ if } i \notin T \end{cases}$ for all $i \in \{1, 2, ..., n\}$. (Thus, $(X_1, X_2, ..., X_n) \mid_T = ([1 \in T]\, X_1, [2 \in T]\, X_2, ..., [n \in T]\, X_n)$.)

Example: For $n = 3$, Lemma 1 says that if P is a polynomial of three variables X_1, X_2, X_3, then there exists a polynomial Q of the variables X_1, X_2, X_3 such that

$$\begin{aligned} & P(0,0,0) - P(X_1,0,0) - P(0,X_2,0) - P(0,0,X_3) \\ & + P(0,X_2,X_3) + P(X_1,0,X_3) + P(X_1,X_2,0) - P(X_1,X_2,X_3) \\ & = X_1X_2X_3 \cdot Q(X_1,X_2,X_3). \end{aligned}$$

Proof of Lemma 1. We will show Lemma 1 by induction over n:

Induction basis: We start the induction with the case $n = 1$. If $n = 1$, then Lemma 1 states that if P is a polynomial of one variable X_1 over a ring R, then there exists a polynomial Q of the variable X_1 over R such that $P(0) - P(X_1) = X_1 \cdot Q(X_1)$. This is exactly the statement of Assertion 1 (with X renamed as X_1), and hence correct. Thus, Lemma 1 is proven for $n = 1$.

Now to the *induction step*: Given some integer $n > 1$, and assume that we have proved Lemma 1 for $n - 1$ instead of n. That is, we have shown the following assertion:

Assertion 2: Let S be a polynomial of $n - 1$ variables X_1, X_2, ..., X_{n-1} over a ring R'. Then, there exists a polynomial Q of the variables X_1, X_2, ..., X_{n-1} over R' such that

$$\sum_{T \subseteq \{1,2,...,n-1\}} (-1)^{|T|} S\left((X_1, X_2, ..., X_{n-1}) \mid_T\right) = \prod_{i=1}^{n-1} X_i \cdot Q\left(X_1, X_2, ..., X_{n-1}\right).$$

Now we want to prove Lemma 1 for n; that is, we are given a polynomial P of n variables X_1, X_2, ..., X_n over a ring R, and we have to show that there exists a polynomial Q of the variables X_1, X_2, ..., X_n over R such that

$$\sum_{T \subseteq \{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = \prod_{i=1}^{n} X_i \cdot Q\left(X_1, X_2, ..., X_n\right).$$

In fact,

$$\begin{aligned}
&\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left(\left(X_1,X_2,...,X_n\right)\mid_T\right)\\
&= \sum_{\substack{T\subseteq\{1,2,...,n\};\\ n\notin T}} (-1)^{|T|} P\left(\left(X_1,X_2,...,X_n\right)\mid_T\right) + \sum_{\substack{T\subseteq\{1,2,...,n\};\\ n\in T}} (-1)^{|T|} P\left(\left(X_1,X_2,...,X_n\right)\mid_T\right)\\
&= \sum_{\substack{T\subseteq\{1,2,...,n\};\\ n\notin T}} (-1)^{|T|} P\left(\left(X_1,X_2,...,X_n\right)\mid_T\right) + \sum_{\substack{T'\subseteq\{1,2,...,n\};\\ n\notin T'}} (-1)^{|T'\cup\{n\}|} P\left(\left(X_1,X_2,...,X_n\right)\mid_{T'\cup\{n\}}\right)\\
&\qquad\left(\begin{array}{c}\text{here we have set } T'=T\setminus\{n\} \text{ in the second sum, and now we are}\\ \text{summing over } T' \text{ instead of summing over } T\text{, what obviously does not}\\ \text{change the sum (note that } T=T'\cup\{n\} \text{ because } n\in T\text{)}\end{array}\right)\\
&= \sum_{\substack{T\subseteq\{1,2,...,n\};\\ n\notin T}} (-1)^{|T|} P\left(\left(X_1,X_2,...,X_n\right)\mid_T\right) + \sum_{\substack{T\subseteq\{1,2,...,n\};\\ n\notin T}} (-1)^{|T\cup\{n\}|} P\left(\left(X_1,X_2,...,X_n\right)\mid_{T\cup\{n\}}\right)\\
&\qquad\text{(here we have renamed } T' \text{ into } T \text{ in the second sum)}\\
&= \sum_{\substack{T\subseteq\{1,2,...,n\};\\ n\notin T}} \left((-1)^{|T|} P\left(\left(X_1,X_2,...,X_n\right)\mid_T\right) + (-1)^{|T\cup\{n\}|} P\left(\left(X_1,X_2,...,X_n\right)\mid_{T\cup\{n\}}\right)\right)\\
&= \sum_{T\subseteq\{1,2,...,n-1\}} \left((-1)^{|T|} P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,0\right) + (-1)^{|T|+1} P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,X_n\right)\right)\\
&= \sum_{T\subseteq\{1,2,...,n-1\}} \left((-1)^{|T|} P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,0\right) - (-1)^{|T|} P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,X_n\right)\right)\\
&= \sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} \left(P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,0\right) - P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,X_n\right)\right).
\end{aligned} \tag{1}$$

Now, we can consider the polynomial $P\in R\left[X_1,X_2,...,X_n\right]$ as a polynomial of one variable X_n over the ring $R\left[X_1,X_2,...,X_{n-1}\right]$. Applying Assertion 1 to this polynomial, we see that there exists a polynomial S of the variable X_n over the ring $R\left[X_1,X_2,...,X_{n-1}\right]$ such that $P(0)-P(X_n)=X_n\cdot S(X_n)$ (this polynomial S was called Q in Assertion 1, but we need the letter Q for something else now). Hereby, both P and S are viewed as polynomials of the variable X_n over the ring $R\left[X_1,X_2,...,X_{n-1}\right]$. If we consider P and S as polynomials of the n variables X_1, X_2, ..., X_n over the ring R, then this equality becomes

$$P\left(X_1,X_2,...,X_{n-1},0\right)-P\left(X_1,X_2,...,X_{n-1},X_n\right)=X_n\cdot S\left(X_1,X_2,...,X_{n-1},X_n\right).$$

Now this is an identity of polynomials over R, with X_1, X_2, ..., X_n being free variables; thus we can substitute anything we want for the variables X_1, X_2, ..., X_n. In particular, if T is any subset of $\{1,2,...,n-1\}$, then we can substitute $\left(X_1,X_2,...,X_{n-1}\right)\mid_T$ for $\left(X_1,X_2,...,X_{n-1}\right)$, and we obtain

$$P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,0\right)-P\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,X_n\right)=X_n\cdot S\left(\left(X_1,X_2,...,X_{n-1}\right)\mid_T,X_n\right).$$

Hence, using (1), we have

$$\begin{aligned}
&\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n)\mid_T\right) \\
&= \sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} \left(P\left((X_1, X_2, ..., X_{n-1})\mid_T, 0\right) - P\left((X_1, X_2, ..., X_{n-1})\mid_T, X_n\right)\right) \\
&= \sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} X_n \cdot S\left((X_1, X_2, ..., X_{n-1})\mid_T, X_n\right) \\
&= X_n \cdot \sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} S\left((X_1, X_2, ..., X_{n-1})\mid_T, X_n\right). \qquad (2)
\end{aligned}$$

Now we can consider the polynomial $S \in R[X_1, X_2, ..., X_n]$ as a polynomial of the $n-1$ variables X_1, X_2, ..., X_{n-1} over the ring $R[X_n]$. Applying Assertion 2 to this polynomial S (with $R[X_n]$ as R'), we see that there exists a polynomial Q of the variables X_1, X_2, ..., X_{n-1} over $R[X_n]$ such that

$$\sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} S\left((X_1, X_2, ..., X_{n-1})\mid_T\right) = \prod_{i=1}^{n-1} X_i \cdot Q\left(X_1, X_2, ..., X_{n-1}\right).$$

This identity makes sense if both S and Q are viewed as polynomials of the $n-1$ variables X_1, X_2, ..., X_{n-1} over the ring $R[X_n]$. If we view S and Q as polynomials of the n variables X_1, X_2, ..., X_n over the ring R, then this identity becomes

$$\sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} S\left((X_1, X_2, ..., X_{n-1})\mid_T, X_n\right) = \prod_{i=1}^{n-1} X_i \cdot Q\left(X_1, X_2, ..., X_{n-1}, X_n\right).$$

Thus, (2) becomes

$$\begin{aligned}
&\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n)\mid_T\right) \\
&= X_n \cdot \sum_{T\subseteq\{1,2,...,n-1\}} (-1)^{|T|} S\left((X_1, X_2, ..., X_{n-1})\mid_T, X_n\right) \\
&= X_n \cdot \prod_{i=1}^{n-1} X_i \cdot Q\left(X_1, X_2, ..., X_{n-1}, X_n\right) = \prod_{i=1}^{n} X_i \cdot Q\left(X_1, X_2, ..., X_{n-1}, X_n\right).
\end{aligned}$$

Thus, Lemma 1 is proved for n. This completes the induction step, and thus the proof of Lemma 1 is completed.

We can make Lemma 1 a bit stronger using the notion of the total degree:

If P is a polynomial of n variables X_1, X_2, ..., X_n over the ring R, then the *total degree* $\deg P$ of the polynomial P is defined as the maximal integer κ such that the polynomial P contains a term $a_{\lambda_1,\lambda_2,...,\lambda_n} X_1^{\lambda_1} X_2^{\lambda_2} ... X_n^{\lambda_n}$ with $a_{\lambda_1,\lambda_2,...,\lambda_n} \neq 0$ and $\lambda_1 + \lambda_2 + ... + \lambda_n = \kappa$. Now we have:

Lemma 2. Let $n \geq 1$ be an integer. Let P be a polynomial of n variables X_1, X_2, ..., X_n over a ring R. Then, there exists a polynomial Q of the variables X_1, X_2, ..., X_n over R such that

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = \prod_{i=1}^{n} X_i \cdot Q\left(X_1, X_2, ..., X_n\right)$$

and $\deg Q \leq \deg P - n$.

Proof of Lemma 2. According to Lemma 1, there exists a polynomial Q of the variables X_1, X_2, ..., X_n over R such that

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = \prod_{i=1}^{n} X_i \cdot Q\left(X_1, X_2, ..., X_n\right).$$

Remains to show that $\deg Q \leq \deg P - n$. In fact,

$$\deg\left(\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right)\right) \leq \deg P$$

(because $\deg P\left((X_1, X_2, ..., X_n) \mid_T\right) \leq \deg P$ for every $T \subseteq \{1, 2, ..., n\}$, and the total degree of a sum of polynomials is not larger than the greatest of their total degrees), so that

$$\deg P \geq \deg\left(\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right)\right) = \deg\left(\prod_{i=1}^{n} X_i \cdot Q\left(X_1, X_2, ..., X_n\right)\right)$$
$$= \deg\left(\prod_{i=1}^{n} X_i \cdot Q\right) = n + \deg Q,$$

and thus $\deg Q \leq \deg P - n$. Hereby, we have $\deg\left(\prod\limits_{i=1}^{n} X_i \cdot Q\right) = n + \deg Q$ because multiplying a polynomial by $\prod\limits_{i=1}^{n} X_i$ means replacing each coefficient $a_{\lambda_1,\lambda_2,...,\lambda_n}$ by $a_{\lambda_1-1,\lambda_2-1,...,\lambda_n-1}$ (and this obviously increases the total degree by n). Thus, Lemma 2 is proven.

As a consequence of Lemma 2, we have:

Lemma 3. Let $n \geq 1$ be an integer. Let P be a polynomial of n variables X_1, X_2, ..., X_n over a ring R such that $\deg P < n$. Then,

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = 0.$$

Example: For $n = 3$, Lemma 3 says that if P is a polynomial of three variables X_1, X_2, X_3 such that $\deg P < 3$, then

$$P(0,0,0) - P(X_1,0,0) - P(0,X_2,0) - P(0,0,X_3)$$
$$+ P(0,X_2,X_3) + P(X_1,0,X_3) + P(X_1,X_2,0) - P(X_1,X_2,X_3) = 0.$$

Proof of Lemma 3. After Lemma 2, there exists a polynomial Q of the variables X_1, X_2, ..., X_n over R such that

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = \prod_{i=1}^n X_i \cdot Q\left(X_1, X_2, ..., X_n\right)$$

and $\deg Q \leq \deg P - n$. Since $\deg P < n$, this yields

$$\deg Q \leq \deg P - n < n - n = 0,$$

so that $Q = 0$, and thus

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n) \mid_T\right) = \prod_{i=1}^n X_i \cdot Q\left(X_1, X_2, ..., X_n\right) = \prod_{i=1}^n X_i \cdot 0 = 0.$$

This proves Lemma 3.

Now comes the first application of Lemma 3 - a problem from the Saint Petersburg Mathematical Olympiad 2003 [1]:

> **Problem 1.** Let p be a prime number, and n an integer with $n \geq p$. Let a_1, a_2, ..., a_n be n integers. Prove that
>
> $$p \mid \sum_{k=0}^n (-1)^k \left|\left\{T \subseteq \{1, 2, ..., n\} \;\mid\; |T| = k \text{ and } p \mid \sum_{t\in T} a_t\right\}\right|.$$

Solution of Problem 1. For every $k \in \{0, 1, ..., n\}$, we have

$$\left|\left\{T \subseteq \{1, 2, ..., n\} \;\mid\; |T| = k \text{ and } p \mid \sum_{t\in T} a_t\right\}\right| = \sum_{T\subseteq\{1,2,...,n\}} \left[|T| = k \text{ and } p \mid \sum_{t\in T} a_t\right].$$

Thus,

$$\begin{aligned}
&\sum_{k=0}^n (-1)^k \left|\left\{T \subseteq \{1, 2, ..., n\} \;\mid\; |T| = k \text{ and } p \mid \sum_{t\in T} a_t\right\}\right| \\
&= \sum_{k=0}^n (-1)^k \sum_{T\subseteq\{1,2,...,n\}} \left[|T| = k \text{ and } p \mid \sum_{t\in T} a_t\right] \\
&= \sum_{T\subseteq\{1,2,...,n\}} \sum_{k=0}^n (-1)^k \left[|T| = k \text{ and } p \mid \sum_{t\in T} a_t\right] \\
&= \sum_{T\subseteq\{1,2,...,n\}} \underbrace{\sum_{k=0}^n (-1)^k \left[|T| = k\right] \cdot}_{=(-1)^{|T|}} \left[p \mid \sum_{t\in T} a_t\right] \\
&= \sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left[p \mid \sum_{t\in T} a_t\right]. \qquad (3)
\end{aligned}$$

[1] posted on MathLinks in the topic
http://www.mathlinks.ro/Forum/viewtopic.php?t=188350

If we denote by b_1, b_2, ..., b_n the residue classes of the integers a_1, a_2, ..., a_n modulo the prime p (these b_1, b_2, ..., b_n are elements of the field $\mathbb{F}_p$), then $p \mid \sum\limits_{t\in T} a_t$ is equivalent to $\sum\limits_{t\in T} b_t = 0$ (as an equation in $\mathbb{F}_p$). Thus, $\left[p \mid \sum\limits_{t\in T} a_t\right] = \left[\sum\limits_{t\in T} b_t = 0\right]$. Hence, (3) becomes

$$\sum_{k=0}^{n} (-1)^k \left|\left\{T \subseteq \{1,2,...,n\} \ \mid\ |T| = k \text{ and } p \mid \sum_{t\in T} a_t\right\}\right| = \sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left[\sum_{t\in T} b_t = 0\right].$$

Thus, in order to prove that

$$p \mid \sum_{k=0}^{n} (-1)^k \left|\left\{T \subseteq \{1,2,...,n\} \ \mid\ |T| = k \text{ and } p \mid \sum_{t\in T} a_t\right\}\right|$$

(this is what the problem 1 wants us to show), it is enough to prove that

$$p \mid \sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left[\sum_{t\in T} b_t = 0\right],$$

i. e., to prove that

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left[\sum_{t\in T} b_t = 0\right] = 0 \tag{4}$$

as an equality in the field $\mathbb{F}_p$.

Lemma 0 (applied to $x = \sum\limits_{t\in T} b_t$) yields $\left[\sum\limits_{t\in T} b_t = 0\right] = 1 - \left(\sum\limits_{t\in T} b_t\right)^{p-1}$. Hence, (4) is equivalent to

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left(1 - \left(\sum_{t\in T} b_t\right)^{p-1}\right) = 0 \tag{5}$$

as an equality in the field $\mathbb{F}_p$.

In order to solve the problem 1, it thus remains to verify this equality (5). We do this as follows: We define a polynomial P of the n variables X_1, X_2, ..., X_n over the ring $\mathbb{F}_p$ by setting $P(X_1, X_2, ..., X_n) = 1 - \left(\sum\limits_{t=1}^{n} X_t\right)^{p-1}$. Then, $\deg P \leq p-1$, so that $\deg P < n$ (since $p - 1 < n$ because $n \geq p$), and thus Lemma 3 yields

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P\left((X_1, X_2, ..., X_n)\mid_T\right) = 0.$$

Since for any $T \subseteq \{1,2,...,n\}$, we have

$$\begin{aligned} P\left((X_1, X_2, ..., X_n)\mid_T\right) &= P\left([1\in T] X_1, [2\in T] X_2, ..., [n\in T] X_n\right) \\ &= 1 - \left(\sum_{t=1}^{n} [t\in T] X_t\right)^{p-1} = 1 - \left(\sum_{t\in T} X_t\right)^{p-1}, \end{aligned}$$

this becomes

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left(1-\left(\sum_{t\in T} X_t\right)^{p-1}\right) = 0.$$

This is a polynomial identity; substituting $X_1 = b_1$, $X_2 = b_2$, ..., $X_n = b_n$, we thus get

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \left(1-\left(\sum_{t\in T} b_t\right)^{p-1}\right) = 0,$$

so that (5) is proven. Since (5) is equivalent to (4), and (4) yields the assertion of the problem 1, we have thus solved the problem 1.

Using the same technique, we can solve a question posed by Lzw75 in

`http://www.mathlinks.ro/Forum/viewtopic.php?t=193724`

namely the following one:

> **Problem 2.** Let p be a prime, let m be an integer, and let $n > (p-1)\,m$ be an integer. Let a_1, a_2, ..., a_n be n elements of the vector space $\mathbb{F}_p^m$. Prove that there exists a non-empty subset $T \subseteq \{1,2,...,n\}$ such that $\sum\limits_{t\in T} a_t = 0$.

Solution of Problem 2. In the following, all our computations will be in the field $\mathbb{F}_p$.

For every $t \in \{1,2,...,n\}$ and every $j \in \{1,2,...,m\}$, let $a_{t,j}$ be the j-th coordinate of the vector $a_t \in \mathbb{F}_p^m$. Then, $a_t = (a_{t,1}, a_{t,2}, ..., a_{t,m})^T$ for every $t \in \{1,2,...,n\}$.

We define a polynomial P of the n variables X_1, X_2, ..., X_n over the ring $\mathbb{F}_p$ by setting

$$P(X_1, X_2, ..., X_n) = \prod_{j=1}^{m} \left(1-\left(\sum_{t=1}^{n} a_{t,j}X_t\right)^{p-1}\right).$$

Then, $\deg P \leq (p-1)\,m$ (because P is the product of the m polynomials $1-\left(\sum\limits_{t=1}^{n} a_{t,j}X_t\right)^{p-1}$, each of whom has degree $\leq p-1$), so that $\deg P < n$ (since $n > (p-1)\,m$), and thus Lemma 3 yields

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} P((X_1, X_2, ..., X_n)\,|_T) = 0.$$

Since for any $T \subseteq \{1,2,...,n\}$, we have

$$\begin{aligned} P((X_1, X_2, ..., X_n)\,|_T) &= P([1\in T]\,X_1, [2\in T]\,X_2, ..., [n\in T]\,X_n) \\ &= \prod_{j=1}^{m} \left(1-\left(\sum_{t=1}^{n} a_{t,j}\,[t\in T]\,X_t\right)^{p-1}\right) \\ &= \prod_{j=1}^{m} \left(1-\left(\sum_{t\in T} a_{t,j}X_t\right)^{p-1}\right), \end{aligned}$$

this becomes

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \prod_{j=1}^{m} \left(1-\left(\sum_{t\in T} a_{t,j} X_t\right)^{p-1}\right) = 0.$$

This is a polynomial identity; substituting $X_1 = 1$, $X_2 = 1$, ..., $X_n = 1$, we thus get

$$\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \prod_{j=1}^{m} \left(1-\left(\sum_{t\in T} a_{t,j} \cdot 1\right)^{p-1}\right) = 0. \tag{6}$$

For every $T \subseteq \{1, 2, ..., n\}$, we have[2]

$$\begin{aligned}
&\left[\sum_{t\in T} a_t = 0\right] = \left[\sum_{t\in T} (a_{t,1}, a_{t,2}, ..., a_{t,m})^T = 0\right] \\
&= \left[\left(\sum_{t\in T} a_{t,1}, \sum_{t\in T} a_{t,2}, ..., \sum_{t\in T} a_{t,m}\right)^T = 0\right] \\
&= \left[\sum_{t\in T} a_{t,1} = 0 \text{ and } \sum_{t\in T} a_{t,2} = 0 \text{ and ... and } \sum_{t\in T} a_{t,m} = 0\right] \\
&= \prod_{j=1}^{m} \left[\sum_{t\in T} a_{t,j} = 0\right] = \prod_{j=1}^{m} \left(1-\left(\sum_{t\in T} a_{t,j}\right)^{p-1}\right)
\end{aligned}$$

(since for every $j \in \{1, 2, ..., m\}$, we have $\left[\sum\limits_{t\in T} a_{t,j} = 0\right] = 1 - \left(\sum\limits_{t\in T} a_{t,j}\right)^{p-1}$ by Lemma 0, applied to $x = \sum\limits_{t\in T} a_{t,j}$). Hence,

$$\begin{aligned}
&\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \cdot \left[\sum_{t\in T} a_t = 0\right] \\
&= \sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \cdot \prod_{j=1}^{m} \left(1-\left(\sum_{t\in T} a_{t,j}\right)^{p-1}\right) \\
&= \sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \prod_{j=1}^{m} \left(1-\left(\sum_{t\in T} a_{t,j} \cdot 1\right)^{p-1}\right) = 0
\end{aligned} \tag{7}$$

by (6).

Now, assume that there is no non-empty subset $T \subseteq \{1, 2, ..., n\}$ such that $\sum\limits_{t\in T} a_t = 0$. This means that for every non-empty subset $T \subseteq \{1, 2, ..., n\}$, the assertion $\sum\limits_{t\in T} a_t = 0$ is wrong, i. e. we have $\left[\sum\limits_{t\in T} a_t = 0\right] = 0$. On the other hand, the empty subset $\varnothing$

[2] Remember that we are working in the field $\mathbb{F}_p$, not in $\mathbb{Z}$.

obviously satisfies $\sum_{t\in\varnothing} a_t = 0$, so that $\left[\sum_{t\in\varnothing} a_t = 0\right] = 1$. Thus,

$$\begin{aligned}
&\sum_{T\subseteq\{1,2,...,n\}} (-1)^{|T|} \cdot \left[\sum_{t\in T} a_t = 0\right] \\
&= (-1)^{|\varnothing|} \cdot \underbrace{\left[\sum_{t\in\varnothing} a_t = 0\right]}_{=1} + \sum_{\substack{\text{non-empty} \\ T\subseteq\{1,2,...,n\}}} (-1)^{|T|} \cdot \underbrace{\left[\sum_{t\in T} a_t = 0\right]}_{=0} \\
&= (-1)^{|\varnothing|} \cdot 1 + \sum_{\substack{\text{non-empty} \\ T\subseteq\{1,2,...,n\}}} (-1)^{|T|} \cdot 0 = (-1)^0 \cdot 1 + \sum_{\substack{\text{non-empty} \\ T\subseteq\{1,2,...,n\}}} 0 = 1 \cdot 1 + 0 = 1,
\end{aligned}$$

contradicting (7) (since $0 \neq 1$ in the field $\mathbb{F}_p$).

This contradiction shows that our assumption (that there is no non-empty subset $T \subseteq \{1, 2, ..., n\}$ such that $\sum_{t\in T} a_t = 0$) was wrong. Hence, there exists a non-empty subset $T \subseteq \{1, 2, ..., n\}$ such that $\sum_{t\in T} a_t = 0$. Problem 2 is solved.