Use of polynomials for arithmetical and combinatorial problems

Vladimir Barzov

Abstract

Sometimes number theory and combinatorics problems can be easily translated into algebra problems by introducing suitable polynomials. The present note considers such applications in connection with some problems from various mathematical competitions and olympiads.

We will use the following notation:
(1) $\mathbb{F}_p$ – the field of residues modulo p, where p is a prime number;
(2) $f \in F[x]$ will mean that $f(x)$ is a polynomial over the field F, i.e. its coefficients are elements of F.

Often, we will use the following facts:
(1) If the number of distinct roots of a polynomial is greater than its degree, then this polynomial is identically zero;
(2) If a polynomial $f \in F[x]$ has a root x_0, then $f(x)$ can be represented in the form $f(x) = (x - x_0)g(x)$ for some polynomial $g \in F[x]$.

The first problem appeared on the selection test for the Balkan Mathematical Olympiad in 2001.
Problem 1. For an arbitrary set $S = \{a_1, a_2, \ldots, a_k\}$ of integers with

$$1 \leq a_1 < a_2 < \cdots < a_k \leq 2000$$

define the set

$$\Phi(S) = \begin{cases} \{a_1 + 1, a_2 + 1, \ldots, a_k + 1\}, & \text{if } a_k < 2000, \\ \{1, 2, \ldots, 2000\} \setminus \{a_1 + 1, a_2 + 1, \ldots, a_{k-1} + 1\}, & \text{if } a_k = 2000. \end{cases}$$

Prove that $\Phi^{2001}(S) = S$, where $\Phi^{2001}(S)$ is the 2001st iteration of Φ.

Solution. Consider the polynomial

$$f(x) = x^{a_1-1} + x^{a_2-1} + \cdots + x^{a_k-1}.$$

Since $a_k - 1 \leq 1999$, $\deg f \leq 1999$. Denote

$$a(x) = 1 + x + x^2 + \cdots + x^{2000},$$

and define the polynomial sequence

$$f_0(x), f_1(x), f_2(x), \ldots,$$

with $f_0(x) = f(x)$, and

$$f_{i+1}(x) = \begin{cases} xf_i(x) & \text{if } \deg f_i(x) \leq 1998; \\ a(x) - xf_i(x) & \text{if } \deg f_i(x) = 1999. \end{cases}$$

It is clear that if $\Phi^i(S) = \{b_1, b_2, \ldots, b_m\}$ for some positive integers $b_1 < b_2 < \cdots < b_m$, then

$$f_i(x) = x^{b_1-1} + x^{b_2-1} + \cdots + x^{b_m-1},$$

which shows that the coefficients of $f_i(x)$ are equal to 1, and that the degree of $f_i(x)$ is less than 2000. Moreover, we have

$$f_i(x) = p_i(x)a(x) \pm x^i f(x).$$

For $i = 2001$ we get either

$$f_{2001}(x) = p(x)a(x) + x^{2001} f(x)$$

or

$$f_{2001}(x) = p(x)a(x) - x^{2001} f(x).$$

In the first case

$$f_{2001}(x) - f(x) = p(x)a(x) + (x^{2001} - 1)f(x) = a(x)(p(x) + (x-1)f(x)).$$

Then, the polynomial $f_{2001}(x) - f(x)$ is of degree ≤ 1999, and it is divisible by $a(x)$, hence it is identical to 0. Therefore, we have $f_{2001}(x) = f(x)$, which means that $\Phi^{2001}(S) = S$. Analogously, in the second case we obtain $f_{2001}(x) = -f(x)$, which is a contradiction, since the coefficients of $f(x)$ and $f_{2001}(x)$ are positive. $\square$

Problem 2. Prove that if $a_0, a_1, \ldots, a_{n-1}$ are real numbers with

$$a_0 + a_1 + \cdots + a_{n-1} = 0,$$

and if the cyclic sum

$$\sum_C \frac{1}{a_i(a_i + a_{i+1}) \cdots (a_i + a_{i+1} + \cdots + a_{i+n-2})}$$

is well defined, then this sum is equal to 0.

Solution. Clearly $n \geq 2$ for the cyclic sum to be well defined. Let

$$s_i = a_0 + a_1 + \cdots + a_{i-1}$$

and $s_{k+n} = s_k$ for all $k \in \mathbb{Z}$. We have to prove that

$$\sum_C \frac{1}{(s_{i+1} - s_i)(s_{i+2} - s_i) \cdots (s_{i+n-1} - s_i)} = 0.$$

Notice that if $i \neq j$ for $i, j \in [0, n-2]$, then $s_i \neq s_j$ since the cyclic sum is well defined. Replacing s_{n-1} by x, let us consider the rational function

$$\begin{aligned} S(x) = &\frac{1}{(s_0 - x)(s_1 - x) \cdots (s_{n-2} - x)} + \\ &\sum_{i=0}^{n-2} \frac{1}{(s_0 - s_i)(s_1 - s_i) \cdots (s_{i-1} - s_i)(s_{i+1} - s_i) \cdots (s_{n-2} - s_i)(x - s_i)} = \\ &\frac{(-1)^{n-1} A + \sum_{i=0}^{n-2} A_i (x - s_0)(x - s_1) \cdots (x - s_{i-1})(x - s_{i+1}) \cdots (x - s_{n-2})}{A(x - s_0)(x - s_1) \cdots (x - s_{n-2})} = \\ &\frac{P(x)}{A(x - s_0)(x - s_1) \cdots (x - s_{n-2})}, \end{aligned}$$

where $A, A_0, A_1, \ldots, A_{n-2}$ are constants defined by

$$A = \prod_{0 \leq i < j \leq n-2} (s_i - s_j),$$

$$A_i = \frac{A}{(s_0 - s_i)(s_1 - s_i) \cdots (s_{i-1} - s_i)(s_{i+1} - s_i) \cdots (s_{n-2} - s_i)}$$

and the degree of the polynomial $P(x)$ is not greater than $n-2$. Note that $P(s_i) = 0$ for $i = 0, 1, \ldots, n-2$, which yields $n-1$ distinct roots of $P(x)$.

Therefore $P(x) \equiv 0$ and in particular $P(s_{n-1}) = 0$, hence $S(s_{n-1}) = 0$ and the proof is complete. $\square$

Problem 3. Prove that

$$\sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} \binom{kn-1}{n-1} = 1$$

for every positive integer n.

Solution. Let

$$f_0(x) = \frac{(xn-1)(xn-2)\cdots(xn-n+1)}{(n-1)!},$$

and consider the sequence of polynomials

$$f_0(x), f_1(x), \ldots$$

defined by the recurrence

$$f_{k+1}(x) = f_k(x) - f_k(x+1).$$

Since $\deg f_0 = n-1$ and $\deg f_{k+1} < \deg f_k$, it follows that $f_n \equiv 0$. Then, from the identities

$$f_i(x) = \sum_{k=0}^{i} (-1)^k \binom{i}{k} f_0(x+k)$$

and

$$f_0(k) = \binom{kn-1}{n-1}$$

we obtain

$$0 = f_n(0) = f_0(0) + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \binom{kn-1}{n-1}.$$

Therefore

$$\sum_{k=1}^{n} (-1)^k \binom{n}{k} \binom{kn-1}{n-1} = -f_0(0) = (-1)^n,$$

and multiplying both sides by $(-1)^n$ completes the proof. $\square$

The following problem is original to the author.

Problem 4. Let $p > 2$ be prime. There are p numbers written in a circle.

At each move, simultaneously each number is replaced by the number plus its right neighbor minus twice its left neighbor. Prove that after $p-1$ moves all numbers will have the same remainder modulo p.

Solution. Let the given numbers be $a_0, a_1, \ldots, a_{p-1}$. Consider the following polynomial $f_0(x) \in \mathbb{Z}[x]$:

$$\begin{aligned} f_0(x) =& (-a_0)(x-1)(x-2)\cdots(x-p+1)+ \\ & (-a_1)x(x-2)\cdots(x-p+1)+ \\ & (-a_2)x(x-1)(x-3)\cdots(x-p+1)+ \\ & \cdots + \\ & (-a_{p-1})x(x-1)\cdots(x-p+2). \end{aligned}$$

Notice that $\deg f_0 \leq p-1$. Furthermore, observe that

$$f_0(i) = (-a_i)i!(p-1-i)!(-1)^{p-1-i} \equiv (-a_i)(p-1)! \equiv a_i \pmod{p}$$

from Wilson's theorem. Define the sequence

$$f_{k+1}(x) = f_k(x) + f_k(x+1) - 2f_k(x-1).$$

Notice that the set of values $f_k(i)$, $i = 0, 1, \ldots, p-1$ represents the residues modulo p of the given integers after the k-th move. Since the leading term cancels at each step, we have

$$\deg f_{k+1} < \deg f_k,$$

unless $\deg f_k = 0$, in which case $\deg f_{k+1} = 0$. Since $\deg f_0 \leq p-1$ we get $\deg f_{p-1} \leq 0$, which yields that f_{p-1} is a constant polynomial. Hence the numbers $f_{p-1}(i)$ for $i = 0, 1, \ldots, p-1$ are equal. □

The next problem is from the final round of the Romanian Mathematical Olympiad in 2001.

Problem 5. Find all pairs (m, n) of positive integers, such that m divides $a^n - 1$ for $a = 1, 2, \ldots, n$.

Solution. Clearly, the pairs $(1, k)$ and $(k, 1)$ satisfy the requirements for every natural k. Now, suppose that $m, n > 1$. Let p be any prime divisor of m. Since $p \mid (a^n - 1)$ for $a = 1, 2, \ldots, n$, it follows that $n < p$, otherwise we would get a contradiction with $p \nmid (p^n - 1)$. Then, we have that the polynomial

$$f(x) = x^n - 1 \in \mathbb{F}_p[x]$$

can be factored over $\mathbb{F}_p$:

$$x^n - 1 \equiv (x-1)(x-2)\cdots(x-n) \pmod{p}.$$

Comparing the coefficients of x^{n-1}, we get

$$0 \equiv 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \pmod{p}.$$

From here $p \mid (n+1)$, and therefore $n+1 = p$. This means that m has exactly one prime divisor, and thus $m = p^\alpha$ for some positive integer α. Assuming that $\alpha \geq 2$, we have

$$p^2 \mid (a^{p-1} - 1)$$

for $a = 1, 2, \ldots, p-1$. On the other hand, from $p = n+1 > 2$, we have

$$(p-1)^{p-1} - 1 \equiv \binom{p-1}{1} p(-1)^{p-2} = -p(p-1) \not\equiv 0 \pmod{p^2}.$$

Thus, $\alpha \leq 1$. It is easy to see that the pair $(p, p-1)$ is a solution for any prime p. Finally, the answer is: $(1, k)$, $(k, 1)$, and $(p, p-1)$ for every prime p and natural k.

The following problem is from the Polish Mathematical Olympiad in 1995.

Problem 6. Let $p \geq 3$ be a given prime. Define the sequence (a_n) by

$$a_n = \begin{cases} n, & 0 \leq n \leq p-1 \\ a_{n-1} + a_{n-p}, & n \geq p \end{cases}.$$

Determine $a_{p^3} \pmod{p}$.

Solution. Define another sequence (b_n) by $b_n = a_{p^3-n}$ for $n = 0, 1, \ldots, p^3$. Obviously, it satisfies

$$b_n = b_{n-p} - b_{n-p+1}$$

for $n \geq p$. We can extend this sequence using this recurrence by defining b_n for $n \geq p^3$. Now, if $x_1, x_2, \ldots, x_p$ are the roots of

$$t(x) = 1 - x - x^p,$$

then it is easy to see that $x_i \neq x_j$ for $i \neq j$. Hence, there exist unique numbers $\lambda_i \in \mathbb{C}, i = 1, 2, \ldots, p$, such that

$$b_n = \lambda_1 x_1^n + \lambda_2 x_2^n + \cdots + \lambda_p x_p^n.$$

Obviously, if $f \in \mathbb{Z}[x]$ then

$$\sum_{i=1}^{p} \lambda_i f(x_i)$$

is an integer, as it is a linear combination of some of the terms of (b_n). We will show that

$$b_n \equiv b_{n+p^2-1} \pmod{p}$$

for $n \geq 0$. Now we have:

$$\begin{aligned} x^{p^2} =& (x^p)^p = (1 - x - t(x))^p = (1-x)^p + t(x)u(x) \equiv \\ & 1 - x^p + t(x)u(x) = x + t(x)(u(x)+1) = x + t(x)v(x) \pmod{p}. \end{aligned}$$

Putting $x = 0$ we obtain

$$0 = 0^{p^2} - 0 \equiv t(0)v(0) = v(0) \pmod{p},$$

since $t(0) = 1$. Consequently,

$$v(x) \equiv xA(x) \pmod{p},$$

and

$$t(x)A(x) \equiv x^{p^2-1} - 1 \pmod{p}.$$

So, there exists a polynomial $B(x) \in \mathbb{Z}[x]$, such that

$$t(x)A(x) + pB(x) = x^{p^2-1} - 1.$$

Then, since $t(x_i) = 0$ for $i = 1, 2, \ldots, p$, we have

$$\begin{aligned} b_{n+p^2-1} - b_n = \sum_{i=1}^{p} \lambda_i x_i^n (x_i^{p^2-1} - 1) = \\ \sum_{i=1}^{p} \lambda_i x_i^n pB(x_i) = \\ p \sum_{i=1}^{p} \lambda_i x_i^n B(x_i) = pc_n, \end{aligned}$$

where c_n is an integer according to the observation above. Finally,

$$a_{p^3} = b_0 = b_{p^3-p} - p(c_0 + c_1 + \cdots + c_{p-1}) = a_p + pC,$$

and the answer is $p - 1$. □

The next problem was used for the preparation of the Bulgarian team for the 41st IMO in South Korea.

Problem 7. Two different multisets $\{a_1, a_2, \ldots, a_n\}$ and $\{b_1, b_2, \ldots, b_n\}$ are given. A multiset is a set with possible repetitions. Prove that if the multisets

$$\{a_i + a_j \mid 1 \leq i < j \leq n\}$$

and

$$\{b_i + b_j \mid 1 \leq i < j \leq n\}$$

coincide, then n is a power of 2.

Solution. Consider the polynomials

$$f(x) = x^{a_1} + x^{a_2} + \cdots + x^{a_n}$$

and

$$g(x) = x^{b_1} + x^{b_2} + \cdots + x^{b_n}.$$

From the hypothesis we have

$$f(x)f(x) - f(x^2) = g(x)g(x) - g(x^2).$$

Denoting

$$h(x) = f(x) - g(x) \not\equiv 0,$$

we get

$$h(x)(f(x) + g(x)) = h(x^2).$$

If now

$$h(x) = (x-1)^m p(x), \quad p(1) \neq 0,$$

then

$$p(x)(f(x) + g(x)) = (x+1)^m p(x^2),$$

and

$$p(1)(f(1) + g(1)) = (1+1)^m p(1).$$

Therefore,

$$2n = f(1) + g(1) = 2^m \Rightarrow n = 2^{m-1}$$

and the proof is complete. □

The next problem is taken from the American Mathematical Monthly.

Problem 8. Let p be an odd prime. Prove that

$$\sum_{i=1}^{p-1} 2^i i^{p-2} \equiv \sum_{i=1}^{\frac{p-1}{2}} i^{p-2} \pmod{p}.$$

Solution. This congruence, considered as an identity in $\mathbb{F}_p$, can be written in the form

$$\sum_{i=1}^{p-1} \frac{2^i}{i} = \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i}.$$

Indeed, by Fermat's theorem, $i^p \equiv i \pmod{p}$, and hence $i \in [1, p-1] \Rightarrow i^{p-2} = \dfrac{1}{i}$ in $\mathbb{F}_p$. Since

$$\sum_{i=1}^{p-1} \frac{1}{i} \equiv \sum_{i=1}^{p-1} i \equiv 0 \pmod{p},$$

then

$$\sum_{i=1}^{p-1} \frac{(-1)^i}{i} = \sum_{i=1}^{\frac{p-1}{2}} \frac{-2}{2i-1} = \sum_{i=1}^{\frac{p-1}{2}} \frac{2}{p-(2i-1)} = \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{\frac{p-2i+1}{2}} = \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i}.$$

Further, we consider the polynomial

$$f(x) = \sum_{i=1}^{p-1} \frac{x^i}{i}, \qquad f \in \mathbb{F}_p[x].$$

The assertion reduces to proving the equality

$$f(2) = f(-1).$$

Actually, a stronger assertion holds:

$$f\left(x + \frac{1}{2}\right) = f\left(-x + \frac{1}{2}\right).$$

The claim follows by putting $x = \dfrac{3}{2}$. Note that

$$f'(x) = 1 + x + \cdots + x^{p-2} = \frac{x^{p-1} - 1}{x - 1}$$

for $x \neq 1$. Moreover, the polynomial

$$f'\left(x + \frac{1}{2}\right) + f'\left(-x + \frac{1}{2}\right)$$

has $p-1$ distinct roots $x_i = \dfrac{k}{2}$ for $k = 1, 2, \ldots, p-1$ and is of degree less than $p-1$, hence

$$f'\left(x+\frac{1}{2}\right) + f'\left(-x+\frac{1}{2}\right) \equiv 0.$$

Therefore

$$f\left(x+\frac{1}{2}\right) = f\left(-x+\frac{1}{2}\right),$$

which completes the proof. □

Problem 9. Compute the sum modulo p of all the primitive roots of p, where p is a prime number.

Solution. Let S_k be the set of all the numbers $a \in [1, p-1]$, such that $a^k \equiv 1 \pmod{p}$, and $a^l \not\equiv 1 \pmod{p}$ for $l \in [1, k-1]$. (S_k could be empty for some k.) Denote

$$f_k(x) = \prod_{a \in S_k} (x-a), \qquad f_k \in \mathbb{F}_p[x]$$

for every positive divisor k of $p-1$, and let b_k be the coefficient of $x^{\deg f_k - 1}$. Note that

$$\prod_{k|d} f_k(x) \equiv x^d - 1 \pmod{p}$$

for every divisor d of $p-1$. Moreover, the leading coefficients of f_k are units, so that

$$\sum_{k|d} b_k \equiv 0 \pmod{p}$$

for $d > 1$. As it is known for the Möbius function μ,

$$\sum_{k|d} \mu(k) = 0$$

for $d > 1$, so an easy induction proves that

$$b_k \equiv -\mu(k) \pmod{p}.$$

Therefore, the sum of the roots of f_{p-1} – the primitive roots modulo p – in $\mathbb{F}_p$ is

$$-b_{p-1} = \mu(p-1).$$