МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2002
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2002
Proceedings of Thirty First Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 3–6, 2002

USE OF POLYNOMIALS FOR ARITHMETICAL AND COMBINATORIAL PROBLEMS

Vladimir V. Barzov

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 notations:
(1) F_p – the field of the remainders 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 the different zeroes of a polynomial is greater than its degree, then this polynomial is equal to zero identically;
(2) If a polynomail $f \in F[x]$ has a zero 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 was given 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 $1 \leq a_1 < a_2 < \ldots < a_k \leq 2000$ define the set
$\Phi(S) = \begin{cases} \{a_1 + 1, a_2 + 1, \ldots, a_k + 1\}, \text{ if } a_k < 2000; \\ \{1, 2, \ldots, 2000\} \backslash \{a_1 + 1, a_2 + 1, \ldots, a_{k-1} + 1\}, \text{ if } a_k = 2000. \end{cases}$
Prove that $\Phi^{2001}(S) = S$, where $\Phi^{2001}(S)$ is the 2001-st iteration of Φ.

Solution. Consider the polynomial $f(x) = x^{a_1 - 1} + x^{a_2 - 1} + \ldots + x^{a_k - 1}$. Since $a_k - 1 \leq 1999$, then $\deg f \leq 1999$. Denote $a(x) = 1 + x + x^2 + \ldots + x^{2000}$, and define the polynomial sequence $f_0(x), f_1(x), f_2(x), \ldots$, with $f_0(x) = f(x)$, and

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

It is clear that if $\Phi^i(s) = \{b_1, b_2, \ldots, b_m\}$ for some positive integers $b_1 < b_2 < \ldots < b_m$, then $f_i(x) = x^{b_1 - 1} + x^{b_2 - 1} + \ldots + x^{b_m - 1}$, 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 degree at most $f_{2001}(x) = p(x)a(x) + x^{2001}f(x)$ 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 deg ≤ 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.

Problem 2. Prove that if $a_0, a_1, \ldots, a_{n-1}$ are real numbers with $a_0+a_1+\ldots+a_{n-1}=0$, and if the cyclic sum $\sum_C \frac{1}{a_i(a_i + a_{i+1})\ldots(a_i + a_{i+1} + \ldots + a_{i+n-2})}$ is well defined, then this sum is equal to 0.

Solution. Let $s_i = a_0 + a_1 + \cdots + a_{i-1}$ and $s_{k+n} = s_k$ for all $k \in \mathbb{Z}$. Now we have to prove that $\sum_C \frac{1}{(s_{i+1} - s_i)(s_{i+2} - s_i)\ldots(s_{i+n-1} - s_i)} = 0$.
Denoting s_{n-1} by x, let us consider the rational function

$$\frac{1}{(s_0 - x)(s_1 - x)\ldots(s_{n-2} - x)} +$$

$$= \sum_{i=0}^{n-2} \frac{1}{(s_0 - s_i)(s_1 - s_i)\ldots(s_{i-1} - s_i)(s_{i+1} - s_i)\ldots(x_{n-2} - s_i)(x - s_i)}.$$

It can be represented as

$$\frac{A + \sum_{i=0}^{n-2} A_i(x - s_0)(x - s_1)\ldots(x - s_{i-1})(x - s_{i+1})\ldots(x - s_{n-2})}{B(x - s_0)(x - s_1)\ldots(x - s_{n-2})} =$$

$$= \frac{P_n(x)}{B(x - s_0)(x - s_1)\ldots(x - s_{n-2})},$$

where $B = \prod_{i \neq j}(s_i - s_j)$, $A = (-1)^{n-1}B$, $A_i = \frac{B}{(x - s_0)(x - s_1)\ldots(x - s_{n-2})}$, $i = 0, 1, \ldots, n-2$, and the degree of the polynomial $P_n(x)$ is not greater than $n-2$. Note that $P_n(s_i) = 0$ for $i = 0, 1, \ldots, n-2$; therefore $P_n(x) \equiv 0$ and in particular $P_n(s_{n-1}) = 0$, which completes the proof.

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

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

This completes the proof.

The following problem is original:

Problem 4. Given are p (where p is a prime number greater than 3) integers, arranged on a circle. On each "turn" one adds simultaneously the right neighbor to every number, and subtracts its doubled left neighbor. Prove that after $p-1$ turns all the numbers become congruent modulo p.

Solution. Let the given numbers be $a_0, a_1, \ldots, a_{p-1}$. Consider a polynomial $f(x) \in \mathbb{Z}[x]$ such that:
$f(i) \equiv a_i \pmod{p}$, $i = 0, 1, \ldots, p-1, \deg f < p$. Such a polynomial exists, for example:

$$f_0(x) = (-a_0)(x-1)(x-2)\ldots(x-p+1) + (-a_1)x(x-2)\ldots(x-p+1) + \ldots +$$

$$+(-a_{p-1})x(x-1)\ldots(x-p+2).$$

Let us form the sequence $f_{k+1}(x) = f_k(x) + f_k(x+1) - 2f_k(x-1)$ for $k = 0, 1, \ldots, p-1$. Notice that the set $f_k(i), i = 0, 1, \ldots, p-1$ represents the remainders modulo p of the given integers after the k-th turn. Also, note that $p > \deg f_0 > \deg f_1 > \ldots > \deg f_{p-1}$. Consequently $\deg f_{p-1} \leq 0$, 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, q.e.d.

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 each $a = 1, 2, \ldots, n$.

Solution. Evidently, the pairs $\{1, k\}$ and $\{k, 1\}$ satisfy the requirements for every natural k. Now, suppose $m, n > 1$. Let p be an arbitrary prime divisor of m. Since $p|(a^n - 1)$ for $a = 1, 2, \ldots, n$, it follows that $n < p$. Otherwise we would get a contradiction with $p/(p^n - 1)$. Then, we have that the polynomial $f(x) = x^n - 1 \in F_p[x]$ can be factorized over F_p: $x^n - 1 \equiv (x-1)(x-2)\ldots(x-n) \pmod{p}$. Comparing the coefficients of x^{n-1}, we get $0 \equiv 1 + 2 + \ldots + n = n(n+1) \pmod{p}$. From here $p|(n+1)$, 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 $p^2/(a^{p-1} - 1)$ for $a = 1, 2, \ldots, p-1$. On the other hand, from $p = n + 1 > 2$, we have $(p-1)^{p-1} - 1 \equiv p(p-1) \not\equiv 0 \pmod{p^2}$. 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 Poland Mathematical Olympiad in 1995:

Problem 6. Let $p \geq 3$ be a given prime. Define the sequence (a_n) by $a_n = n$ for $n = 0, 1, \ldots, p-1$, and $a_n = a_{n-1} + a_{n-p}$ for $n > p$. Determine the remainder of a_{p^3} modulo 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 $(b_n)_{n \geq p}$. Now, if $x_1, x_2, \ldots, x_p$ are the zeroes 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 $b_n = \lambda_1 x_1^n + \lambda_2 x_2^n + \ldots + \lambda_p x_p^n$. Obviously, if $f(x)$ is a polynomial and $f \in \mathbb{Z}[x]$, 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: T $x^{p^2} \equiv (x^p)^p \equiv (1-x-t(x))^p \equiv (1-x)^p + t(x)u(x) \equiv 1 - x^p + t(x)u(x) \equiv x + t(x)(u(x)+1) \equiv x + t(x)v(x) \pmod{p}$. Putting $x = 0$ we obtain $0 \equiv 0^{p^2} - 0 \equiv t(0)v(0) \equiv v(0) \pmod{p}$, 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

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

where c_n is an integer according to the observation above.
Finally, $a_{p^3} = b_0 = b_{p^3-p} - p(c_0 + c_1 + \ldots + c_{p-1}) = a_p + pC$, and the answer is $p - 1$.

The next problem was used for the preparation of the Bulgarian team for the 41^{st} 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 diven. (A multiset is a set with possible repetitions). Prove that if the multisets $\{a_i + a_j | 1 \leq i < j \leq n\}$ and $\{b_i + b_j | 1 \leq i < j \leq n\}$ 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 $g(x) = x^{b_1} + x^{b_2} + \ldots + x^{b_n}$. 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 $h(x) = (x-1)^m p(x)$, $p(1) \neq 0$, 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, $2n = f(1) + g(1) = 2^m \Rightarrow n = 2^{m-1}$.

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 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 the Fermat theorem, $i^p \equiv i \pmod p$, and hence, if $i \in [1; p-1]$, $i^{p-2} = \frac{1}{i}$ in 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 $f(x) = \sum_{i=1}^{p-1} \frac{x^i}{i}, f \in F_p[x]$. The assertion reduces to the equality $f(2) = f(-1)$. Actually, a stronger assertion holds true: $f\left(x + \frac{1}{2}\right) = f\left(-x + \frac{1}{2}\right)$. The hypothesis follows by putting $x = \frac{3}{2}$. Note that $f'(x) = 1 + x + \cdots + x^{p-2} = \frac{x^{p-1} - 1}{x - 1}$ for $x \neq 1$. Moreover, $f'(0) + f'(1) = 1 + p - 1 = 0$, so the polynomial $f'\left(x + \frac{1}{2}\right) + f'\left(-x + \frac{1}{2}\right)$ has at least $p-1$ different zeroes, and is of degree less than $p-1$. Hence, $f'\left(x + \frac{1}{2}\right) + f'\left(-x + \frac{1}{2}\right) \equiv 0$, and $f\left(x + \frac{1}{2}\right) = f\left(-x + \frac{1}{2}\right)$, 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 $f_k(x) = \prod_{a \in S_k} (x - a), f_k \in F_p[x]$ 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 senior coefficients of f_k are units, so that $\sum_{k/d} b_k \equiv 0 \pmod p$ for $d > 1$. As it is known, $\sum_{k/d} \mu(k) \equiv 0 \pmod p$ 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 – in F_p is $-b_{p-1} = \mu(p-1)$, and we are done.

In conclusion, I wish to thank Mr. Sava Grozdev and Mr. Ivan Dimovsky for their help in the preparation and editing of the paper.

REFERENCES

[1] Crux 3/94, 10/95.
[2] T. Nagel. Introduction to number theory, Sofia, 1971.

Vladimir Vladimirov Barzov
Student in 12th grade of
Sofia High School of Mathematics
61, Iskar Str.
1000 Sofia, Bulgaria
e-mail: vbarzov@yahoo.com

ПРИЛОЖЕНИЕ НА ПОЛИНОМИ ЗА РЕШАВАНЕ НА АРИТМЕТИЧНИ И КОМБИНАТОРНИ ЗАДАЧИ

Владимир В. Барзов

Понякога задачи от областа на теорията на числата и комбинаториката могат да бъдат преведени на алгебричен език чрез въвеждането на подходящи полиноми. Настоящият доклад разглежда такива приложения във връзка със задачи от различни математически състезания и олимпиади.