Ist International Tournament of Young Mathematicians 27th June – 3rd July 2009, Paris, France

PROBLEM FIVE

INTEGER-VALUED POLYNOMIALS

An integer-valued polynomial $q(x)$ is a polynomial taking an integer value $q(n)$ for every positive integer n. Denote by $Q_0[x]$ the set of all integer-valued polynomials with rational coefficients, that is $Q_0[x]=\{q(x)\in Q[x]\,|\,q(n)\in Z, \forall n\in N\}$.

Let p be a prime number and let $Z_p=\{0,1,2,...,p-1\}$ be the set of residues modulo p.

1. Describe the set of integer-valued polynomials $q(x)\in Q_0[x]$ with the property $q(n)\equiv 0\,(\mathrm{mod}\,p)$ for all $n\in N$.
2. Let $q(x)$ be a polynomial from $Q_0[x]$. Define whether the sequence $((q(n)\bmod p)_{n\in N}$ is periodic and, if it is, find or estimate its period.
3. We say that a sequence $\{a_n\}_{n\in N}$ of elements of Z_p is realizable if there exists an integer-valued polynomial $q(x)\in Q_0[x]$ such that $q(n)\equiv a_n\,(\mathrm{mod}\,p)$ for all $n\in N$. Describe the set of realizable sequences.
4. Let $\{a_n\}_{n\in N}$ be a realizable sequence. Describe the set of integer-valued polynomials $q(x)\in Q_0[x]$ such that $q(n)\equiv a_n\,(\mathrm{mod}\,p)$ for all $n\in N$.
5. Describe the set $Q_0[x]$.

TEAM: **MATH HIGH SCHOOL *NANCHO POPOVICH*, BULGARIA**

Leaders: LOZANOV Chavdar, CHRISTOVA Madlen
Contestants: VALKOV Mladen, YORDANOVA Yoana, ALEKSANDROVA Polina, MARKOVA Magdalena, KOSTADINOVA Georgina, ENCHEV Ivaylo

Investigation

Below we will consider the variables as natural numbers, except if it is explicitly mentioned other thing.

Problem 1. We will prove that the set $Q_0[x]$ consist of all polynomials $q(x)=c_n\binom{x}{n}+c_{n-1}\binom{x}{n-1}+\ldots+c_1\binom{x}{1}+c_0\binom{x}{0}$, where c_i are integers.

Solution. We will present two proofs.

First proof. It is obvious that $\binom{x}{n}$ is of degree n. We will prove the statement with induction on n, i.e. with induction on the degree of the polynomial.

1) The basis is obvious – if the polynomial is of degree 0, so it is of the type $q(x)=c_0$ and from the condition follows that c_0 is an integer. Since $n=1$ hence $q(x)=c_1x+c_0=c_1\binom{x}{1}+c_0\binom{x}{0}$ and we have only to notice that c_1, c_0 are integers (That follows immediately, if we put $x=1$ and $x=2$).

2) Let the statement is proved for polynomials of degree less than n (i. e. they are of the wanted type).

3) Consider a polynomial of degree n and let it be $q(x)$, which has the wanted property. Let us notice that the polynomial $P(x)=q(x+1)-q(x)$ is of degree less than or equal to $n-1$ and takes integer values for each natural number (since for natural values of x from the property of $q(x)$ follows that $q(x)$ and $q(x+1)$ are integers – if x is a natural number, than $x+1$ is also natural). Therefore from the induction assumption $P(x)$ has the type: $P(x)=a_{n-1}\binom{x}{n-1}+a_{n-2}\binom{x}{n-2}+\ldots+a_1\binom{x}{1}+a_0\binom{x}{0}$, where a_i are integers. For each natural x we have the following:

$q(x)=P(x-1)+q(x-1)=P(x-1)+P(x-2)+q(x-2)=\ldots=$

$=P(x-1)+P(x-2)+P(x-3)+\ldots+P(1)+q(1)$.

And that is how we get $q(x)=P(x-1)+P(x-2)+P(x-3)+\ldots+P(1)+q(1)$.

Now we use that $\binom{1}{k}+\ldots+\binom{x-1}{k}=\binom{x}{k+1}$ (which is proved easily, for example by induction) in this way:

$q(x)=P(x-1)+P(x-2)+P(x-3)+\ldots+P(1)+q(1)=$

$=a_{n-1}\left[\binom{x-1}{n-1}+\binom{x-2}{n-1}+\ldots+\binom{1}{n-1}\right]+a_{n-2}\left[\binom{x-1}{n-2}+\binom{x-2}{n-2}+\ldots+\binom{1}{n-2}\right]+\ldots+$

$+a_0\left[\binom{x-1}{0}+\ldots+\binom{1}{0}\right]+q(1)=a_{n-1}\binom{x}{n}+a_{n-2}\binom{x}{n-1}+\ldots+a_0\binom{x}{1}+q(1)$

Now we have only to put $c_n=a_{n-1}, c_{n-1}=a_{n-2},\ldots,c_1=a_0, c_0=q(1)$, wherefrom obviously follows that $c_1,\ldots,c_n$ are integers (from the induction assumption), and $q(1)$ is integer

because 1 is natural and then from the properties of $q(x)$ we have that $q(1)$ is an integer.
Backward: Obviously polynomial from the type we have found complies with the condition (the binomial coefficients are integers).
With that the proof is completed.

Second proof. First, we are going to prove the following
Lemma 1. Each polynomial $f(x)$ with real coefficients of degree n can be represented as

$$f(x)=b_n\binom{x}{n}+b_{n-1}\binom{x}{n-1}+...+b_1\binom{x}{1}+b_0\binom{x}{0}$$

Proof of the lemma. We will make the proof using induction on n.

1) If $n=0$, $f(x)=const=a$ and then $f(x)=a.\binom{x}{0}$

2) Let the statement be true for all polynomials of degree less than n.

3) Now let $f(x)=a_nx^n+...$. Put $b_n=n!a_n$. Then the polynomial

$$g(x)=f(x)-b_n\binom{x}{n}=a_nx^n+a_{n-1}x^{n-1}+...+a_0-a_nn!\frac{x(x-1)...(x-n+1)}{n!}$$

will be of degree less than or equal to $n-1$ and from the induction assumption there would be numbers $b_0,...,b_{n-1}$, such that $g(x)=b_{n-1}\binom{x}{n-1}+...+b_0\binom{x}{0}$. Then we have:

$f(x)-b_n\binom{x}{n}=b_{n-1}\binom{x}{n-1}+...+b_0\binom{x}{0}$, т.е. $f(x)=b_n\binom{x}{n}+b_{n-1}\binom{x}{n-1}+...+b_0\binom{x}{0}$, which leads to the end of the induction and the lemma is proved.

Let us go back to the problem. Let $q(x)$ is one of the polynomials, described in the problem's condition. From the lemma we have that there are such numbers $b_n,...,b_0$, that:

$$q(x)=b_n\binom{x}{n}+b_{n-1}\binom{x}{n-1}+...+b_0\binom{x}{0}.$$

We only have to prove that these $b_n,...,b_0$ are integers. For that purpose we are going to prove the following
Lemma 2. When $x=0$ the polynomial $q(x)$ takes again an integer value.

Proof of lemma 2. It is clear that we can write $q(x)=\frac{P(x)}{d}$, where $P(x)$ is a polynomial with integer coefficients, and d is an integer number – a constant (for the purpose only reduce all the coefficients to a common denominator, and this common denominator actually is d, and the numerator turns into a polynomial with integer coefficients). Now we have to notice that choosing x, which could be divided by d, $P(x)$ will take the type $P(x)=\frac{dR(x)+t}{d}=R(x)+\frac{t}{d}$, where $R(x)$ is a polynomial with integer coefficients and t is the constant term of $P(x)$ and then from the condition follows, that t is divisible by d, and wherefrom if we go back to the primary type of

$q(x)=\frac{P(x)}{d}$ (we divide $P(x)$ with d) the constant term of $q(x)$ will be $\frac{t}{d}$, which as le have already noted is an integer number. Since $q(0)$ actually gives the constant term of $q(x)$, then $q(0)=\frac{t}{d}\in Z$.

With this we have proved the second lemma.

Now the problem is solved almost directly:

We have $\binom{0}{n}=...=\binom{0}{1}=\binom{1}{n}=\binom{1}{2}=...=\binom{n-2}{n}=\binom{n-2}{n-1}=\binom{n-1}{n}=0$ (i.e. $\binom{k}{d}=0$, if $k<d$) и $\binom{1}{1}=\binom{2}{2}=...=\binom{n}{n}=1$.

Then we have consecutively $q(0)=b_0$ and therefore b_0 are integer.

$q(1)=b_1\binom{1}{1}+b_0$ and therefore $b_1=q(1)-b_0$ and then b_1 is also an integer.

.....

$$q(n)=b_0+b_1\binom{n}{1}+...+b_{n-1}\binom{n}{n-1}+b_n\binom{n}{n}$$

and then $b_n=q(n)-b_0-b_1\binom{n}{1}-...-b_{n-1}\binom{n}{n-1}$.

Since we have already proved that $b_0,...,b_{n-1}$ are integers, hence, all of b_i are integers, which we had to prove.

We will show how the above formula works:

For example, if we consider the polynomial

$$q(x)=\binom{x}{2}+\binom{x}{1}+\binom{x}{0}=\frac{x(x-1)}{2}+x+1=\frac{x^2-x+2x+2}{2}=\frac{x^2+x+2}{2}$$

according to the proved above it follows that the polynomial takes only integer values, when x is a natural number. And really $q(x)=\frac{x^2+x+2}{2}=\frac{x(x+1)}{2}+1$ takes integer values, because as it is well-known $\frac{x(x+1)}{2}=\binom{x+1}{2}$ gets only integer values (the product of two consecutive numbers always is divisible by 2).

Problem 2. Prove that all the polynomials $q(x)\in Q_0[x]$ with the property $q(n)\equiv 0\,(\mathrm{mod}\,p)$ for each $n\in N$, are of the type

$$q(x)=pc_n\binom{x}{n}+pc_{n-1}\binom{x}{n-1}+...+pc_1\binom{x}{1}+pc_0\binom{x}{0},$$

where c_i are integers.

Solution. Let first $q(x)$ be of the wanted type. Then the polynomial $Q(x)=\frac{q(x)}{p}$ for natural numbers takes integer values hence it is of the type: $Q(x)=c_n\binom{x}{n}+c_{n-1}\binom{x}{n-1}+...+c_1\binom{x}{1}+c_0\binom{x}{0}$, where c_i are integers. Then $q(x)=pc_n\binom{x}{n}+pc_{n-1}\binom{x}{n-1}+...+pc_1\binom{x}{1}+pc_0\binom{x}{0}$, c_i are integers.

Backward: Obviously a polynomial of the type, we have found complies with the condition.

With this the proof is completed.

For example

$$q(x)=2p\binom{x}{2}+3p\binom{x}{1}+5p\binom{x}{0}=2p\frac{x(x-1)}{2}+3px+5p=px(x-1)+3px+5p=px^2+2px+5p$$

is one polynomial, obtained by the formula above, which obviously complies with the condition.

Problem 3. Let $q(x)\in Q_0[x]$. Prove that the sequence $(q(n) \bmod p)_{n\in N}$ is periodical and find its period.

Solution. First we will prove that the sequence is periodical.

Let us consider the binomial coefficient $\binom{x}{n}=\frac{x(x-1)...(x-n+1)}{n!}$. Let the highest degree of p, which divides $n!$ is k, i.e. $p^k \| n!$ ($p^l \| r$ means that the highest degree of p, which divides r is l).

We will prove that $\binom{x+p^{k+1}}{n}\equiv\binom{x}{n}(\bmod p)$.

Truly we have

$$\binom{x+p^{k+1}}{n}=\frac{(x+p^{k+1})(x-1+p^{k+1})...(x-n+1+p^{k+1})}{n!}=$$

$$=\frac{x(x-1)...(x-n+1)+p^{k+1}A}{n!}=\binom{x}{n}+\frac{p^{k+1}A}{n!}$$

where A is a polynomial with integer coefficients.

However from $p^k \| n!$ follows that $\frac{p^{k+1}A}{n!}$ in Z_p (which is a field) will be 0, i.e. $\binom{x+p^{k+1}}{n}$ and $\binom{x}{n}$ will be equal in Z_p and therefore they are comparable by modulo p, which we wanted to prove.

Note: If the highest degree of p, which divides $n!$ is less than k the statement is also true, because of the same considerations $\frac{p^{k+1}A}{n!}$ in Z_p will be 0 again.

Now we only have to find the period of the sequence.
Let us consider one polynomial $q(x) \in Q_0[x]$. Let it be of degree n. Then it is of the type $q(x) = c_n\binom{x}{n} + c_{n-1}\binom{x}{n-1} + \ldots + c_1\binom{x}{1} + c_0\binom{x}{0}$. So if $p^k \| n!$, then according to the note above for each i from 0 to n we will have $\binom{x+p^{k+1}}{i} \equiv \binom{x}{i} \pmod p$. Then $q(x+p^{k+1}) \equiv q(x) \pmod p$. But then it is clear that the sequence is periodical and its period must divide p^{k+1}, i.e. its period is from the type p^a for some non-negative integer a.

For example:

1) If we consider the polynomial $q(x) = v = const$ it is obvious that it has a period $1 = p^0$.

2) If the polynomial is from degree 1 it is clear that its period will be either 1, or p: the constant term does not matter for the period and therefore we can consider only the polynomials $q(x) = ax$. Hence, it is clear that, if a is divisible by p, then the period is 1, otherwise the period is p. For example, if we consider the polynomial $q(x) = \binom{x}{1} + 0\binom{x}{0} = x$, then easily can be seen that it has a period p.

3) Let us consider a polynomial of second degree: $q(x) = c_2\binom{x}{2} + c_1\binom{x}{1} + c_0\binom{x}{0}$. As it was said above we can consider only the polynomials of the type

$$q(x) = c_2\binom{x}{2} + c_1\binom{x}{1} = c_2\frac{x(x-1)}{2} + c_1 x = \frac{c_2 x(x-1) + 2c_1 x}{2} = \frac{c_2 x^2 + x(2c_1 - c_2)}{2} = \frac{ax^2 + bx}{2},$$

where $a = c_2$, $b = 2c_1 - c_2$.
If $p \neq 2$, it is enough to see how much the period of the numeral can be (by $p \neq 2$ in Z_p we have that, if $k = l$, then also $\frac{k}{2} = \frac{l}{2}$, so that if the numeral has a period T, the whole fraction has a period T). Also it is clear that $ax^2 + bx \equiv a(x+p)^2 + b(x+p) \pmod p$ so that the period can be only 1 or p. It is easy to see that is a and b are divisible by p, the period is 1, and if only a is divisible by p, then it is p. So, if $p \neq 2$, then the period of a quadratic polynomial is 1 or p.
Let $p = 2$. According to the proved in problem 3 it follows that the period of each quadratic polynomial divides $p^2 = 4$ (because 1 is the highest degree of $2 = p$, which divides $2! = 2$, i.e. $p^1 \| 2!$ and then in the symbols from problem 2 we have $k = 1$, wherefrom the period of the polynomial divides $p^{k+1} = 2^2 = 4$). Therefore the period can be1, 2 or 4. It is easy to see, for example the polynomial $q(x) = 2\binom{x}{2} + 2\binom{x}{1} + 2\binom{x}{0}$ has period 1, and the polynomial $q(x) = 2\binom{x}{2} + \binom{x}{1} + 2\binom{x}{0}$ has period $2 = p$. We will

prove that the polynomial $q(x)=\binom{x}{2}=\frac{x(x-1)}{2}$ has period 4 by modulo 2: as $q(1)\equiv 0(\mathrm{mod}\,2),\ q(2)\equiv 1(\mathrm{mod}\,2),\ q(3)\equiv 1(\mathrm{mod}\,2),\ q(4)\equiv 0(\mathrm{mod}\,2)$, so it is clear that the polynomial has a period of at least 3 and as long as it has to be a divisor of 4, the period has to be equal to 4.

So, quadratic polynomial has a period 1 or p for $p\neq 2$ and it has a period 1, 2 or 4 for $p=2$ (i.e. 1, p or p^2).

Problem 4. Find realizable sequences $\{a_n\}_{n\in N}$ and the respective polynomials $q(x)\in Q_0[x]$, such that $q(n)\equiv a_n\ (\mathrm{mod}\ p)$ for every natural number n.

Solution.

1) It is clear that, if $a_i=t=const$, then $\{a_n\}_{n\in N}$ will be a realizable sequence

– For it a polynomial, in which the coefficients of the terms (binomial coefficients) are divisible by p with exception of the last one, and it is equal for example to t (or a number *l*, $l\equiv t(\mathrm{mod}\,p)$), i.e. $q(x)=pc_n\binom{x}{n}+pc_{n-1}\binom{x}{n-1}+\ldots+pc_1\binom{x}{1}+t$.

2) Another realizable sequence is: $a_i\equiv s.i(\mathrm{mod}\,p)$, where $s=const$

- Here this polynomial works: $q(x)=pc_n\binom{x}{n}+pc_{n-1}\binom{x}{n-1}+\ldots+s\binom{x}{1}+pc_0\binom{x}{0}$, where all of the coefficients of the terms (binomial coefficients) with exception of the last one – $\binom{x}{1}$, are divisible by p, and the coefficient of $\binom{x}{1}$ is s.

3) From the last two observations it follows also that the sequence $a_i\equiv s.i+r(\mathrm{mod}\,p)$, where s and r are integer numbers, also is realizable (for the purpose we consider the polynomial $q(x)=pc_n\binom{x}{n}+pc_{n-1}\binom{x}{n-1}+\ldots+s\binom{x}{1}+r\binom{x}{0}$ where all the coefficients in front of the terms with exception of the last two are divisible by p.

Summary

1. We have presented two proofs that the set $Q_0[x]$ consist of all the polynomials of the type $q(x)=c_n\binom{x}{n}+c_{n-1}\binom{x}{n-1}+...+c_1\binom{x}{1}+c_0\binom{x}{0}$, where the numbers c_i are integers. In the second one we also proof two lemmas, which say that each polynomial $f(x)$ with real coefficients of degree n can be represented as $f(x)=b_n\binom{x}{n}+b_{n-1}\binom{x}{n-1}+...+b_1\binom{x}{1}+b_0\binom{x}{0}$ and the other claims that when $x=0$ the polynomial $q(x)$ have again an integer value.

2. We have shown how the formula we have found works.

3. We have proved that all the polynomials $q(x)\in Q_0[x]$ with the property $q(n)\equiv 0\,(\mathrm{mod}\,p)$ for each $n\in N$, are of the type

$q(x)=pc_n\binom{x}{n}+pc_{n-1}\binom{x}{n-1}+...+pc_1\binom{x}{1}+pc_0\binom{x}{0}$, where c_i are integers.

4. We have given an example for the proved statement.

5. We have proved that the sequence is periodical. We have found the period of the sequence.

6. An example for the reasoning.

7. We have found the realizable sequences $\{a_n\}_{n\in N}$ and the respective polynomials $q(x)\in Q_0[x]$, for which $q(n)\equiv a_n\,(\mathrm{mod}\,p)$ for every natural number n.

References

[1.] Davidov, L., *Polynomials*, Sofia, 1989

[2.] Cahen Paul- Jean,Jean-Luc Chabert, *Integer-Valued Polynomials*, AMC, 1997