2009

Problem 5

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 $Q_0[x] = \{q(x) \in Q[x] \mid q(n) \in Z, \forall n \in N\}$.
Let p be a prime number and let $Z_p = \{0, 1, \ldots, p-1\}$ be the set of residues modulo p.

1. Describe the set of integer-valued polynomials $q(x) \in Q_0[x]$ with the property $q(n) \equiv 0 \bmod p$ 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 realisable if there exists an integer- valued polynomial $q(x) \in Q_0[x]$ such that $q(n) \equiv a_n \bmod p$ for all $n \in N$. Describe the set of realisable sequences.

4. Let $(a_n)_{n \in N}$ be a realisable sequence. Describe the set of integer-valued polynomials $q(x) \in Q_0[x]$ such that $q(n) \equiv a_n \bmod p$ for all $n \in N$.

5. Describe the set $Q_0[x]$.

Sofia High School of Mathematics

6/25/2009

2 Problem 5

$$Q_0[x] = \{q(x) \in Q[x] \mid q(n) \in Z, \forall n \in N\}$$

Let $q(x) \in Q_0[x]$ and the degree of $q[x]$ be $\deg(q[x]) = k$. We know from [1], that $q[x]$ can be expressed as follows:

$$q[x] = b_0\binom{x}{k} + b_1\binom{x}{k-1} + \mathbf{K} + b_{k-1}\binom{x}{1} + b_k,$$

where $b_0, b_1, \mathbf{K}, b_k$ are integers. Indeed, the polynomials $\binom{x}{m}$ are integer-valued and the coefficients $b_0, b_1, \mathbf{K}, b_k$ satisfy the following equalities:

$$q(0) = b_k$$

$$q(1) = b_{k-1}\binom{1}{1} + b_k$$

$$q(2) = b_{k-2}\binom{2}{2} + b_{k-1}\binom{2}{1} + b_k$$

M

$$q(k) = b_0\binom{k}{k} + b_1\binom{k}{k-1} + \mathbf{K} + b_k,$$

whence we conclude that $b_i \in$ Z for i$\in$ {0,1, 2,. . . , k}.

1. Describe the set of integer-valued polynomials q(x) $\in$ Q0[x] with the property q(n) $\equiv$ 0 mod p for all n $\in$N.

We will first investigate the case when $\deg(q(x)) = k < p$. From the following identity

$$q(p) = b_0\binom{p}{k} + b_1\binom{p}{k-1} + \mathbf{K} + b_{k-1}\binom{p}{1} + b_k,$$

we conclude that $q(p) \equiv b_k \equiv 0 \pmod{p}$. In addition, from

$$q(1) = b_{k-1}\binom{1}{1} + b_k \equiv 0 (\mathrm{mod}\ p)$$

$$q(2) = b_{k-2}\binom{2}{2} + b_{k-1}\binom{2}{1} + b_k \equiv 0 (\mathrm{mod}\ p)$$

M

$$q(k) = b_0\binom{k}{k} + b_1\binom{k}{k-1} + \mathbf{K} + b_k \equiv 0 (\mathrm{mod}\ p),$$

Problem 5

we get $b_i \equiv 0 \pmod p$ for every $i \in \{0,1,2,\ldots, k\}$.

In the case when $\deg(q(x)) = k > p$ we have that in order $q(x)$ to be congruent to 0 mod p, the coefficients $b_0, b_1, \mathbf{K}, b_k$ must be divisible by p or $q(x)$ is a multiple of the polynomial $h(x)=x^p-x$.

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.

We will prove that the sequence $(q(n) \bmod p)_{n \in N}$ is either periodic with period p or a constant number modulo p. First, the congruence $q(s) \equiv q(s+pm) \pmod p$ holds since the denominator of an arbitrary binomial coefficient $\binom{a}{b}$ is not congruent to 0 modulo p. Therefore, p is always a possible period of $(q(n) \bmod p)_{n \in N}$. Furthermore, let the sequence $(q(n) \bmod p)_{n \in N}$ have a period t less than p, meaning that $\gcd(t, p) = 1$ and $q(s) \equiv q(s+tm) \pmod p$ for $m \in \mathbb{Z}$. Hence, there exists a unique number t^{-1} modulo p, such that $tt^{-1} \equiv 1 \pmod p$. Let $m \equiv -st^{-1} \pmod p$. Then $q(s) \equiv q(s-stt^{-1}) \equiv q(0) \equiv b_k \pmod p$. But s is an arbitrary natural number and therefore $q(n) \equiv b_k \pmod p$ for every $n \in \mathbb{N}$. We construct the polynomial $q'(n) = q(n) - b_k$. Thus, $q'(n) \equiv 0 \pmod p$ for every $n \in \mathbb{N}$. Therefore, $q'(x)$ has the form discussed in 1. Hence, the polynomial $q(n)$ is a constant number modulo p for every $n \in \mathbb{N}$.

3. We say that a sequence $(a_n)_{n \in N}$ of elements of Z_p is realisable if there exists an integer- valued polynomial $q(x) \in Q_0[x]$ such that $q(n) \equiv a_n \bmod p$ for all $n \in N$. Describe the set of realisable sequences.

Since $q(n) \equiv q(n+lp) \pmod p$ for $l \in \mathbb{Z}$, it follows that $a_i \equiv a_{i+lp} \pmod p$ where i is an arbitrary natural number and l is an integer. Hence, we conclude the realisable sequences are either constant sequences or periodic sequences with period p.

4. Let $(a_n)_{n \in N}$ be a realisable sequence. Describe the set of integer-valued polynomials $q(x) \in Q_0[x]$ such that $q(n) \equiv a_n \bmod p$ for all $n \in N$.

Since $(a_n)_{n \in N}$ is realisable, then there exists such a polynomial $q(x)$ that $q(n) \equiv a_n \pmod p$ for all $n \in N$. The polynomials of the form $g(x)=q(x)+tp$, where t is an integer are also such that $g(n) \equiv a_n \pmod p$ for all $n \in N$.

5. Describe the set $Q_0[x]$.

4 Problem 5

We will prove that the set $Q_o[x]$ consisting of integer-valued polynomials with rational coefficients is the abelian group generated by the linear combinations of $1, \binom{x}{1}, \binom{x}{2}, \ldots, \binom{x}{k}, \ldots$ with integer coefficients. [1]

First, consider the set of linear combinations of $1, \binom{x}{1}, \binom{x}{2}, \ldots, \binom{x}{k}, \ldots$ with integer coefficients. Since the polynomials $\binom{x}{i}$ are integer valued, it follows that this set is a subset of $Q_o[x]$.

Conversely, let $g(x) \in Q_o[x]$ such that $g(x) = d_k\binom{x}{k} + d_{k-1}\binom{x}{k-1} + \mathbf{K} + d_1\binom{x}{1} + d_0$, where $d_0, d_1, d_2, \mathbf{K}, d_k \in Q$. We have $d_k = g(0) \in Z$. Suppose $d_i \in Z$ for all $i \le l < k$. Then consider the polynomial $g_l(x) = g(x) - \sum_{i=0}^{l} d_i\binom{x}{i}$. It is integer-valued and, furthermore, $g_l(x) = d_{l+1}\binom{x}{l+1} + \mathbf{K} + d_k\binom{x}{k}$. It follows that $d_{l+1} = g_l(l+1) \in Z$.

Therefore, abelian group generated by the linear combinations of $1, \binom{x}{1}, \binom{x}{2}, \ldots, \binom{x}{k}, \ldots$ with integer coefficients coincides with the set $Q_o[x]$.

References

[1] *Integer-Valued Polynomials*. Paul-Jean Cahen, Jean-Luc Chabert. Mathematical Surveys and Monographs, Volume 48 - American Mathematical Society, 01/1997