5. Integer-valued Polynomials

Orsay Team

1st ITYM

Introduction

Expression of these polynomials

We will show that

$$q(x) \in \mathbb{Q}_0[x] \Leftrightarrow q(x) = \sum_{i=0}^{n} b_i \binom{x}{i} \qquad b_i \in \mathbb{Z}$$

where $\binom{x}{i}$ is the binomial coefficient: $\binom{x}{i} = \frac{x(x-1)...(x-i+1)}{i!}$.

First, take $q(x)$ a polynomial from $\mathbb{Q}_0$[x] and let n be its degree. Then, we take $p(x)$ another polynomial defined by $p(x) = \sum_{i=0}^{n} b_i \binom{x}{i}$. It is clear that the degree of $p(x)$ is n if and only if $b_n \neq 0$, so $p(x)$ can have the same degree as $q(x)$.

So we can make $p(x) = q(x)$ by conveniently choosing the b_i. We know that $q(x)$ is an integer-valued polynomial, of degree n, so it is fully determined by its $n+1$ first values. Call $q(0) = a_0$, $q(1) = a_1$, ..., $q(n-1) = a_n$.

If we want $\forall x \in \mathbb{Z}, q(x) = p(x) = \sum_{i=0}^{n} b_i \binom{x}{i}$, we have to find the b_i by solving the system of $n+1$ equations :

$$\begin{aligned}
q(0) &= a_0 = b_0 \\
q(1) &= a_1 = b_1 + \binom{1}{0} b_0 \\
q(2) &= a_2 = b_2 + \binom{2}{1} b_1 + \binom{2}{0} b_0 \\
&\vdots \\
q(n) &= a_n = b_n + \binom{n}{n-1} b_{n-1} + \cdots + \binom{n}{0} b_0
\end{aligned}$$

We then find an unique integer value for b_0. Then, at step k, the only unknown is b_k. We know integer a_k from the definition of the polynomial and all the b_i for $0 \leq i < k$, form the past equations. All the b_i involved in

the past equations are integers, constants. This shows that b_k must also be an integer.

The polynomial, fully determined by its $n+1$ first values, is also determined by these $n+1$ equations, therefore it is determined by the b_i, $n+1$ integers. So, every polynomial form $\mathbb{Q}_0[x]$ can be written as $\sum_{i=0}^{n} b_i \binom{x}{i}$.

Conversely, we can see that with integer b_i and the fact that binomial coefficients always take integer values, any polynomial written under the form $\sum_{i=0}^{n} b_i \binom{x}{i}$ takes integer values for $x \in \mathbb{N}$ and is part of $\mathbb{Q}_0[x]$.

Question 1

Polynomials that p divides

Then we take $q(x) \in \mathbb{Q}_0[x]$, such that $\forall x \in \mathbb{N}$, $q(x) \equiv 0 \pmod{p}$.

Define, $\forall x \in \mathbb{Z}$, $g(x) = \frac{q(x)}{p}$. As $q(x)$ is an integer valued polynomial, with p dividing it, we have that $\forall x \in \mathbb{Z}$, $g(x) \in \mathbb{Z}$. So $g(x)$ is also an integer valued polynomial: $g(x) \in \mathbb{Q}_0[x]$.

The set of integer valued polynomials with the property $\forall x \in \mathbb{N}$, $q(x) \equiv 0 \pmod{p}$ is $p \times \mathbb{Q}_0[x]$.

Question 2

We take $q(x)$ a polynomial from $\mathbb{Q}_0[x]$ and search whether the sequence $(q(n) \bmod p)_{n\in\mathbb{N}}$ is periodic and what period it has.

- **Regarding the conventionnal writing of the polynomial** : q(x) $= a_n \times x^n + a_{n-1} \times x^{n-1} + ... + a_1 \times x + a_0$

  We can say that, in the case where $\forall i \in [0\ ;\ \mathrm{n}]$, $a_i \in \mathbb{Z}$, We have :

  $a_k \times (x+p)^k \equiv a_k \times \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i \pmod{p}$

  $a_k \times (x+p)^k \equiv a_n \binom{n}{0} x^n p^0 + a_k \times \sum_{i=1}^{n} \binom{n}{i} x^{n-i} y^i \pmod{p}$

  or $\forall$ m $\in \mathbb{Z}$, p $\times m \equiv 0 \pmod{\ }$ p.

  So here, if we have integer a_i

  $a_k \times (x+p)^k \equiv a_n \times x^n \pmod{\ }$ p

  The polynomial is then periodic modulo p, with p as a period. But only with integer a_i, what isn't always the case.

- **Regarding the writing of q(x) established in Question 1.**

  - As $q(x) \in \mathbb{Q}_0[x]$, we can write $q(x) = \sum_{i=0}^{n} b_i \binom{x}{i}$.
  - We take $k \in \mathbb{N}$, as $p^{k-1} \leq \deg(q(x)) = n < p^k$, so that, from the expression of $q(n)$, $i \leq \deg(q(x))$, then we have $i < p^k$.

Then, regarding the expression of $q(n)$, for proving that this sequence is periodic modulo p with period p^k leads us to prove that the sequence $\binom{n}{i}_{n\in\mathbb{N}}$ is it too. That is a sufficient condition for the sequence to be periodic, but we have not shown it necessary.

The Lucas Theorem tells us that :

$$\binom{n}{i} \equiv \prod_{s=0}^{k-1} \binom{c_s}{a_s} \pmod{p}$$

where :

$$i = a_0 + pa_1 + p^2a_2 + \cdots + p^{k-1}a_{k-1} \quad \text{and } 0 \leq a_s \leq p-1$$
$$n = c_0 + pc_1 + p^2c_2 + \cdots + p^{k-1}c_{k-1} \quad \text{and } 0 \leq c_s \leq p-1$$

So i is given by $\overline{a_{k-1}\dots a_2a_1a_0}$ in base p, and as $i < p^k$, i cannot have any greater decimals: we have $\forall s \geq k, a_s = 0$. Moreover, $\overline{c_{k-1}\dots c_2c_1c_0}$ is the corresponding (perhaps truncated) decomposition of n in base p. Greater decimals of n can exist, but anyway $\binom{n}{0} = 1$: they don't change the product.

When we add p^k to n, we only increase the k^{th} decimal (in base p) of n, (or higher ones); as we don't change i, in which $\forall s \geq k$, $a_s = 0$, this does not change $\binom{n}{i} \mod p$. Therefore, $\binom{n+p^k}{i} \equiv \binom{n}{i} \pmod{p}$.

As $\binom{n}{i}$ is periodic with period p^k, the sequence $q(n)$ is also periodic, because the b_i are constants. The period of the sequence will always divide p^k : $1|$ period $|p^k$.

Question 3

We concentrate on the polynomials $q(x) \in \mathbb{Q}_0[x]$ for which $\deg(q(x)) < p^k$. We search for 'realizable' sequences, sequences $(\alpha_n)_{n\in\mathbb{N}}$ for which $\alpha_n \equiv q(n) \pmod{p}$.

Modulo p

We first study what binds two polynomials that are equal modulo p.

We can suppose that $(q, \tilde{q}) \in \mathbb{Q}_0[x]^2$ are two of these polynomials with $\deg(q) < p^k$ and $\deg(\tilde{q}) < p^k$, such that $\forall n \in \mathbb{N}$, $q(n) \equiv \tilde{q}(n) \pmod{p}$. They can both be written as $\sum_{i=0}^{n} b_i\binom{x}{i}$, ($\tilde{b_i}$ for $\tilde{q}(x)$).

Then, we have $\forall n \in \mathbb{N}$, $(q(n) - \tilde{q}(n)) \equiv 0 \pmod{p}$. This imply, according to the first question, that $\exists\ q_0(\mathrm{x}) \in Q_0[\mathrm{x}]$, such as q(x) - $\tilde{q}$(x) = p $\times$ q_0(x)

But q(x) - $\tilde{q}$(x) = $\sum_{i=0}^{n}(b_i - \tilde{b_i})\binom{x}{i}$.

And $q_0(\mathrm{x}) = \sum_{i=0}^{n}(c_i - \tilde{c_i})\binom{x}{i}$.

So $\forall$ 0 $\leq$ i $\leq$ n, b_i - $\tilde{b_i}$ = p $\times$ $c_i \Leftrightarrow b_i \equiv \tilde{b_i} \pmod{p}$.

In this case, all the coefficients of both polynomials are equal modulo p.

Counting the polynomials

Then, we count all polynomials that can be created with their coefficients (b_i) chosen between 0 and $p-1$.

- With this condition, we are sure to find every sequence reached by the polynomials modulo p.

  Indeed, any other polynomial for which one or more b_i don't lie in $[0; p-1] \cap \mathbb{N}$ would be equal (modulo p) to a polynomial with all its coefficients satisfying this condition, and also they would both generate the same sequence.

- A polynomial is completely determined by its coefficients (according to introduction): $0 \leq b_i \leq p-1$ who can take p different values.

- These p values have to be placed in a coefficient (chosen form b_0 to b_{p^k-1}), that is among p^k places. With this, the degree of the polynomial will always be lower than p^k.

- Then we find p^{p^k} of these polynomials

Counting the sequences

Then, we the count the possible 'realizable' sequences: to be realizable, a sequence needs to have the same period as the polynomial, or a divisor of it, so its period has to be p^k or any divisor.

- We will work with p^k. Indeed, for every counted polynomial on the previous step, $(q(n))$ has a period $\leq p^k$. By taking p^k as a period for our sequences, we are sure not to miss any of the reached sequences, or to count any of them twice.

- Then, creating such a sequence reduces to choosing p^k integers between 0 and $p-1$ (as we are working modulo p). Therefore, there are p^{p^k} of these sequences.

As there is the same number of polynomials and sequences and as there are no two polynomials generating the same sequence, every counted sequences is reached. This show there exists a bijection between these two sets.

- The set of the realizable sequences is therefore the set of all possible successions of p^k integers between 0 and $p-1$, or any sequence containing one of the previous sequence repeated an integer number of times.

- A realizable sequence is defined by p^k integers a_i = p × q(i) + r_i with $r_i \in$ [0 ; p-1] and q(x) any polynomial form Q_0[x]

- In this set we will find sequences in which some pattern is repeated an integer number of times, that is, sequences reached by polynomials of lower period (keeping in mind that the period of a polynomial modulo p can only be a divisor of p^k).

Question 4

On the other hand, if we let $(\alpha_n)_{n\in\mathbb{N}}$ be a realizable sequence, with p^k as a period, we have shown in question 3 that there is only one polynomial $q_0(x)$, with its b_i between 0 and $p-1$, and from degree $\leq p^k$ that generates this sequence.

We search for other integer-valued polynomials $q(x)$, generating the same sequence.

They have to satisfy $\forall x \in \mathbb{N}, q(x) \equiv q_0(x) \pmod{p}$.

So $q(x) = q_0(x) + p \times q_m(x)$ with q_m any integer-valued polynomial (difference between two such functions) form $\mathbb{Q}_0[x]$.

With this, we also take care about the polynomials form higher degree. Indeed, a polynomial form degree p^k can be written as if it had a p^{k+1} as degree.

The set of polynomials that generate the same realizable sequence is finally $\{q(x) \in \mathbb{Q}_0[x], q(x) = q_0(x) + p \times q_m(x)\}$.

Question 5

The set $\mathbb{Q}_0[x]$ is the set of the polynomials that can be written as $\sum_{i=0}^{n} b_i \binom{x}{i}$, with n its degree. We have shown that any of the polynomials of this set is fully determined by its $n+1$ coefficients b_i.

This set is also defined by the fact that under any prime modulo p, k beeing a prime number, its polynomials such as $\deg(q(x)) \leq p^k$ generates the set of all possible sequences of period $\leq p^k$.