Integer Valued Polynomials

June 26, 2009

We are going to introduce a family of polynomials that will lead to a simple description of the subset $\mathbb{Q}_0$. We denote C_n the polynomial that "generalize" the binomial coefficient $\binom{m}{n}$ to $\mathbb{R}$

$$C_n(X) = \frac{X(X-1)\dots(X-n+1)}{n!} = \frac{\prod_{i=0}^{n-1}(X-i)}{n!}$$
$$C_0 = 1$$

We can notice now some important properties of the polynomial C_j :

$$\forall i \in [0, j-1], C_j(i) = 0$$
$$\forall j \in \mathbb{N}, C_j(j) = 1$$
$$\forall n \in \mathbb{N}, i \in \mathbb{N}, C_n(i) \in \mathbb{Z}$$

The last propertie needs some explanations:
- For $i \in [0, j-1], C_j(i) = 0$
- For $m \geq n$,

$$\mathrm{C}_n(m) = \frac{\prod_{i=0}^{n-1}(m-i)}{n!} = \frac{m!}{n!(m-n)!} = \binom{m}{n} \in \mathbb{N}.$$

-For $k < 0$ we can write $k = -m$ with $m \in \mathbb{N}$ so

$$\mathrm{C}_n(k) = C_n(-m) = \frac{\prod_{i=0}^{n-1}(-m-i)}{n!}$$
$$= (-1)^n \frac{\prod_{i=0}^{n-1}(m+i)}{n!}$$
$$= (-1)^n \frac{\prod_{i=m}^{m+n-1}(i)}{n!}$$
$$= (-1)^n \frac{(m+n-1)!}{n!(m-1)!} = (-1)^n \binom{m+n-1}{n} \in \mathbb{Z}$$

The other important propertie of this family of polynomial is that $(C_n)_{n\in\mathbb{N}}$ is a basis of $\mathbb{R}[X]$, that we call the binomial basis. Because, the family C_n has its degree increasing, if we can write a polynomial P as a linear combination of elements of the binomial family, there is no polynomial C_k with k >n in this sum. We can prove by induction on the degree n that for any polynomial P of degree n, there is a unique n-tuple $(b_i)_{0\leq i\leq n}$ such that :

$$P(x) = \sum_{i=0}^{n} b_i C_i(x)$$

For n=0, it's true. Giving the statement for n-1, let P be a polynomial with $\deg P = n$ and $P = \sum_{i=0}^{n} a_i x^i$. The dominant coefficient of C_n is $\frac{1}{n!}$ and because C_n is the only polynomial that contains x^n, there is a unique possibilitie for b_n that is $b_n = a_n \cdot n!$. Then the polynomial $Q = P - b_n C_n$ is a polynomial of the (n-1)-th degree at the very most and the induction hypophesis provides n-1 real numbers b_i such that $Q = \sum_{i=0}^{n-1} b_i C_i$ then $P = \sum_{i=0}^{n} b_i C_i$ More generally, we can show that any family of polynomials $(P_n)_{n\in\mathbb{N}}$ such that $\deg P_n = n$ is a basis of R[X].
For the rest of the text, when there is no doubt, by $(b_i)_{0\leq i\leq n}$ we will refer to the coordonates of a polynomial in the binomial basis.

We can already describe the set $\mathbb{Q}_0[X]$ with the following equivalence :

$$P \in \mathbb{Q}_0, \quad \deg P = n \Leftrightarrow \forall i \in [0,n], b_i \in \mathbb{Z}$$

Let P be a polynomial of $\mathbb{Q}_0[X]$ and n its degree. We can prove by induction on k, $k \leq n$, the statement H_k :

$$\mathrm{H}_k : \forall i \in [0,k], b_i \in \mathbb{Z}.$$

For k = 0, $b_0 = P(0) \in \mathbb{Z}$. Because of the propertie:

$\forall i \in [0, j-1] C_j(i) = 0$
We have, for $k < n$

$$\mathrm{P(k)} = \sum_{i=0}^{n} b_i C_i(k)$$
$$= \sum_{i=0}^{i=k} b_i C_i(k)$$

$= b_k C_k(k) + \sum_{i=0}^{i=k-1} b_i C_i(k)$ and $C_k(k) = 1$

Hence $b_k = P(k) - \sum_{i=0}^{i=k-1} b_i C_i(k)$

$P \in \mathbb{Q}_0[X]$ so $P(k) \in \mathbb{Z}$ and by the induction hypophesis and the previous remark on the C_n polynomials, b_i and $C_i(k)$ are integers and therefore b_k is an integer.

1. Let p be a prime number, describe the set N_p of the polynomials that are the zero polynomial modulo p.

we will show that :

$$\forall n \in \mathbb{N}, P(n) \equiv 0 \bmod p, \deg P = n \Leftrightarrow \forall i \in [0, n], b_i \equiv 0 \bmod p$$

We can prove this again by induction on k that : $\forall i \leq k, b_i \equiv 0 \bmod p$. For k=0, $b = P(0) \equiv 0 \bmod p$. We have the previous relation :

$$b_{k+1} = P(k+1) - \sum_{i=0}^{i=k} b_i C_i(k)$$

By the induction hypophesis, we have $\forall i \leq k, b_i \equiv 0 \bmod p$ and $C_i k \in \mathbb{Z}$ so we get :
$b_{k+1} \equiv P(k+1) \equiv 0 \bmod p$

Although the binomial polynomials give a simple description of the set $\mathbb{Q}_0[X]$ and the set of polynomials that are the zero polynomial modulo p, we try to give some properties of the polynomials without changing the basis of $\mathbb{R}[X]$. We start from a polynomial P of $\mathbb{Q}_0[X]$ that we write $P(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i$ with a_i and b_i integers. We denote by $L(P)$ the lcm (least common multple) of the $(b_0, \ldots, b_n)$, then we can write :

$= \sum_{i=0}^{n} \frac{a_i . b'_i}{L(P)} x^i$ with b'_i such that $b'_i . b_i = L(p)$

$= \frac{1}{L(P)} . \sum_{i=0}^{n} c_i x^i$ with $c_i = a_i . b'_i \in \mathbb{N}$

Thus from a polynomial of $\mathbb{Q}_0[X]$, ie a integer valued with rational coefficient, we can get a polynomial with integer coefficient.
We call , and denote r, the order of the polynomial P the integer $r = 1 + v_p(L(P))$. But because we have the integer L(P) in the denominator of the expression of P, we must now study the propertie of the polynomial P not only modulo p but also modulo p^k. Indeed,

$$\begin{aligned} P(X) \equiv m \bmod p &\Leftrightarrow p|(\frac{1}{L(P)}.\sum_{i=0}^{n} c_i x^i - m) \\ &\Leftrightarrow v_p(\frac{1}{L(P)}.(\sum_{i=0}^{n} c_i x^i - mL(P)) \geq 1 \\ &\Leftrightarrow v_p(\sum_{i=0}^{n} c_i x^i - mL(P)) \geq 1 + v_p(L(P)) = r \\ &\Leftrightarrow p^r | \sum_{i=0}^{n} c_i x^i - mL(P) \\ &\Leftrightarrow \sum_{i=0}^{n} c_i x^i \equiv mL(P) \bmod p^r \end{aligned}$$

We dote P_N the polynomial with integer coefficient associated to P, we have

$$P = \tfrac{1}{L(P)}.P_N$$

and

$$P(x) \equiv m \bmod p \Leftrightarrow P_N \equiv mL(P) \bmod p^r$$

We denote $\mathbb{Z}[X]$ the set of polynomials with integer coefficients. Any polynomial P of $\mathbb{Z}[X]$ is periodic modulo p and its period divides p.
Indeed,

$$x \equiv y \bmod p \Rightarrow \forall i \in N, x^i \equiv y^i \bmod p$$

then because the coefficient are integers,

$$\begin{aligned} P(x+p) = \sum_{i=0}^{n} a_i (x+p)^i &\equiv \sum_{i=0}^{n} a_i (x)^i \bmod p \\ &\equiv P(x) \bmod p \end{aligned}$$

Then the smallest period is a divisor of p , which is a prime number. Consequently, any polynomial of $\mathbb{N}_0[X]$ is a constant polynomial modulo p or is

periodic of period p modulo p. For a polynomial which belongs to $\mathbb{Q}_0[X]$ with its order r, its period is a divisor of p^r. Indeed,

$$\begin{aligned} P(x+t) \equiv P(x) \bmod p &\Leftrightarrow p|\frac{1}{L(P)}(P_N(x+t) - P_N(x)) \\ &\Leftrightarrow p^r|P_N(x+t) - P_N(x) \\ &\Leftrightarrow P_N(x+t) \equiv P_N(x) \bmod p^r \\ &\Leftrightarrow \text{ t is a period of } P_N \end{aligned}$$

Thus, if t is a period of P, then t is a divisor of p^r and we have the following inequalities, that we get for other reasons, one using the pigeonhole principle :

$$t \leq n!p$$

$$t \leq (n+1)(p^{n+1}+1)$$

3. At first we can give a formal description of the set S of the realisable sequences.
We denote S_n the set of the sequences such that for each sequence S_n, there exists a polynomial P that realizes this sequence with $\deg P = n$. We denote, for n different from 0, $\mathbb{Q}_n[X]$ the subset of $\mathbb{Q}_0[X]$ of the polynomials of n-th degree. A polynomial P is entirely described by his first n +1 values, becauce P has at most n roots. Then, to an element of $\mathbb{Z}^{n+1}$, we can associate an only polynomial of $\mathbb{Q}_n[X]$. S_0 is the set of the constant sequence α with α an integer. Consequently we have a bijection of between S_n and $\mathbb{Z}^{n+1}$. Moreover we have :

$$S = \bigcup_{k=0}^{\infty} S_k$$

Thus, we get a bijection between S and $\bigcup_{k=1}^{\infty} \mathbb{Z}^k$.
Because a sequence realisable is equal modulo p to polynomial P, the sequence is also periodic and its period has the same propertie as the one of his realizing polynomial. Given a sequence and its period t, and assuming that it belongs to S_n , we wonder how we can pratically determinate if this sequence is realisable or not. Because the period t satisfies the previous inequalities, we just have a finite numbers of polynomials to test.
Moreover, we have:
any sequence that is periodic, of period p a prime number, is realisable.

4. We denote R_α the set of the polynomials that realizes the sequence $(\alpha_n)_{n\in\mathbb{N}}$. With the previous algorithm, we know how to get a polynomial P_0

that realizes the sequence $(\alpha_n)_{n\in\mathbb{N}}$.Then,

$$\begin{aligned}\text{Q realizes } (\alpha_n)_{n\in\mathbb{N}} &\Leftrightarrow \forall n \in \mathbb{N}, Q(n) \equiv \alpha_n \bmod p \\ &\Leftrightarrow \forall n \in \mathbb{N}, Q(n) - P(n) \equiv 0 \bmod p \\ &\Leftrightarrow (Q - P) \in N_p\end{aligned}$$

Therefore :

$$R_\alpha = (P_0 + Q | Q \in N_p)$$

5. As we said and proved in the beginning that :

$$P \in \mathbb{Q}_0, \quad \deg P = n \Leftrightarrow \forall i \in [0, n], b_i \in \mathbb{Z}$$

We will now give an other possibilitie to answer to some questions. We showed that for every polynomial P of $\mathbb{Q}_0[X]$ we have :

$$P = \frac{1}{L(P)} P_N$$

The study of the divisibility of P by p can be done through the divisibility of P_N by p^r. We take a polynome P of $\mathbb{Z}[X]$ that belongs to N_p , $P(x) = \sum_{i=0}^{n} a_i x^i$. Because, P is a polynomial of $\mathbb{Z}[X]$, we can suppose that the a_i belongs to $\mathbb{Z}_p$ without loss of generality.
We have the Euler's theorem about the Euler's totient function :

$$\forall (n, x) \in {\mathbb{N}^*}^2 \text{ such that } gcd(n, x) = 1, \quad x^{\varphi(n)} \equiv 1 \bmod n$$

For $n = p^r$, $\varphi(p^r) = p^r - p^{r-1}$. Moreover , for a and n relatively prime , b and n relatively prime and also x and n relatively prime with $a \geq b$:

$$\begin{aligned}x^a \equiv x^b \bmod n &\Leftrightarrow x^a - x^b \equiv 0 \bmod n \\ &\Leftrightarrow x^b(x^{a-b} - 1) \equiv 0 \bmod n \\ &\Leftrightarrow x^{a-b} - 1 \equiv 0 \bmod n \text{ due to to the Euclid's lemma}\end{aligned}$$

Therefore, if we take a and b such that :

$$a \equiv b \bmod \varphi(n)$$

There exists an integer k such that :

$$a - b = k\varphi(n)$$

and

$$x^{a-b} \equiv (x^{\varphi(n)})^k$$

then

$$x^{a-b} \equiv 1 \bmod n$$

So we have

$$x^a \equiv x^b \bmod n$$

The sequence $(x^i)_{i\in\mathbb{N}}$ is periodic modulo p^r and its period divides $\varphi(n)$. Thus we can write P as :

$$\begin{aligned} \forall x \text{ such that } gcd(n,x) = 1, P(x) &= \sum_{i=0}^{n} a_i x^i \\ &= \sum_{i=0}^{\varphi(p^r)-1} c_i x^i \end{aligned}$$

where the integers c_i, we can suppose in $\mathbb{Z}_{p^r}$ are defined by :

$$\forall i \in \mathbb{Z}_{\varphi(n)}, c_i \quad = \sum_{j\equiv i \bmod \varphi(n)} a_j$$

From a polynomial P_N of $\mathbb{Z}[X]$, we get a polynomial with its degree equal to $\varphi(n) - 1$ at most and with its coefficient in $\mathbb{Z}_{p^r}$, this polynomial is unique, we denote this polynomial $\tilde{P}$ and the set of these polynomials $\mathbb{Z}[X][p^r]$. Thus we have the surjective function :

$$\begin{aligned} f : \mathbb{Z}[X] &\to \mathbb{Z}[X][p^r] \\ : P &\to \tilde{P} \end{aligned}$$

We would like to prove that :

$$P_N \in N_{p^r} \Rightarrow \tilde{P} = \bar{0}$$

We denote $\tilde{N}_{p^r}$ the set of the polynomials P of $\mathbb{Z}[X][p^r]$ such that P(n) is divisible by p^r for each integer n.

- If the order of the polynomials is 1 :

Then $\mathbb{Z}_p$ is a field and we have an euclidian division in $\mathbb{Z}[X][p]$. We denote by M_1 the polynomial of $\tilde{N}_p$ with its dominant coefficient equal to 1 and its degree minimal. M_1 exists because there is a minimal degree and a polynomial of that degree and ,because $\mathbb{Z}_p$ is a field, we can multiply P by the inverse of its dominant coefficient of P modulo p.
If $P \in \tilde{N}_p$, we can find two polynomials Q and R such that

$$P = QM_1 + R$$

with $\deg R < \deg M_1$.
Because of the choice of M_1, we must have $R = \bar{0}$.

Therefore, M_1 divides every polynomials of $\tilde{N_p}$ and because, a polynomial of $\tilde{N_p}$ belongs to N_p and that the constant polynomial p belongs to N_p we must have $M_1 = \bar{0}$. So we have :

$$P_N \in N_{p^r} \Rightarrow \tilde{P} = \bar{0}$$

Another proof using Cramer's rules (we are still in the case r = 1):

We take P a polynomial of $\tilde{N_p}$ and we denote by $(b_i)_{i\in[1,p-1]}$ the (p-1) tuple such that :

$$\text{P(i)} = \sum_{i=0}^{p-2} a_i i^k = b_i p \qquad (E_i)$$

We consider these p - 1 equations as a system where the coefficients $(a_i)_{i\in[0,p-2]}$ of the polynomial are the variables.
We have the following expression, known as the Vandermonde determinant or polynomial :

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ x_0^2 & x_1^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_0^n & x_1^n & \dots & x_n^n \end{vmatrix} = \prod_{0\le i<j\le n} (x_j - x_i)$$

Now if P is a polynomial of $\tilde{N_p}$, we have :

$$\forall i \in [1, p-1], P(i) \equiv 0 \bmod p \Rightarrow$$

$$\sum_{i=0}^{p-2} a_i \equiv 0 \bmod p \quad \textit{and}$$

$$\dots$$

$$\sum_{i=0}^{p-2} a_i j^i \equiv 0 \bmod p \quad \textit{and}$$

$$\dots$$

$$\sum_{i=0}^{p-2} a_i (p-1)^i \equiv 0 \bmod p$$

The matrix A of this system is :

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & p-1 \\ 1 & 2^2 & \dots & (p-1)^2 \\ \dots & \dots & \dots & \dots \\ 1 & 2^n & \dots & (p-1)^n \end{pmatrix}$$

and :

$$\det A = \prod_{0 \leq i < j < \leq p-2} (j - i)$$

Then, with the Cramer's rules, the solutions a_i are :

$$a_i = \frac{\det A_i}{\det A}$$

where A_i is the matrix we get by changing the i-th column of A by the vector ($b_1 p$,.., $b_{p-1} p$). Then we get:

$$a_i = \frac{p \det A'_i}{\det A}$$

But because $v_p(\det A) = 0$, either $\det A$ divides $\det A'_i$ and a_i is an multiple of p, either a_i is a non integer rational number.Because we took P a polynomial of $\mathbb{Z}[X][p]$, a_i must be a multiple of p and then $a_i \equiv 0 \bmod p$.