Triangle de Pascal dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier

Vincent Lefèvre
(Lycée P. de Fermat, Toulouse)

1990, 1991

1 Introduction

Nous allons étudier des propriétés du triangle de Pascal dans $\mathbb{Z}/p\mathbb{Z}$, p étant un nombre premier : propriétés générales, sur les lignes, puis sur les colonnes du triangle de Pascal. Enfin nous donnerons une démonstration du petit théorème de Fermat en utilisant le développement du binôme de Newton.

2 Propriétés générales de congruence des termes du triangle de Pascal

2.1 Démonstration par récurrence du théorème (1)

Soit q un nombre de la forme p^α avec p premier et $\alpha \in \mathbb{N}^*$. Soient m, n, m', n', 4 entiers naturels tels que :

- $n \leqslant m$;
- $m' < q$ et $n' < q$;
- si $m = n$, alors $n' \leqslant m'$, c'est-à-dire si $m' < n'$, alors $m \neq n$.

Donc on a toujours $qm+m' \geqslant qn+n'$. En effet, dans le cas $m = n$, on a $m' \geqslant n'$, d'où $qm+m' \geqslant qn+n'$, et dans le cas $m \neq n$, on a $qm + m' \geqslant qm \geqslant q(n+1) \geqslant qn + q \geqslant qn + n'$.

Démontrons que :

$$\boxed{\begin{array}{l} - \ n' \leqslant m' \Rightarrow \mathrm{C}_{qm+m'}^{qn+n'} \equiv \mathrm{C}_m^n \mathrm{C}_{m'}^{n'}. \\ - \ n' > m' \Rightarrow \mathrm{C}_{qm+m'}^{qn+n'} \equiv 0. \end{array}} \qquad (1)$$

Pour cela, on effectue une double récurrence sur m et sur m'.

a. (1) est vrai pour $m = 0$, car dans ce cas $n = m = 0$ (puisque $n \leqslant m$) et donc $m' \geqslant n'$.

b. Supposons que (1) soit vrai jusqu'au rang $m-1$ (quels que soient les 3 entiers n, m' et n' satisfaisant les 3 conditions), et démontrons que (1) est vrai au rang m (quels que soient les 3 entiers n, m' et n' satisfaisant les 3 conditions).

b.a. Démontrons d'abord que (1) est vrai pour $m' = 0$.

- Premier cas : $n' = 0$. Il faut démontrer que : pour $n \leqslant m$, $\mathrm{C}_{qm}^{qn} = \mathrm{C}_m^n$.

  C'est vrai pour $n = 0$ et pour $n = m$.

  Pour $0 < n < m$:

$$\begin{aligned}
\mathrm{C}_{qm}^{qn} &\equiv \mathrm{C}_{qm-1}^{qn-1} + \mathrm{C}_{qm-1}^{qn} \\
&\equiv \mathrm{C}_{q(m-1)+(q-1)}^{q(n-1)+(q-1)} + \mathrm{C}_{q(m-1)+(q-1)}^{qn} \\
&\equiv \mathrm{C}_{m-1}^{n-1}\mathrm{C}_{q-1}^{q-1} + \mathrm{C}_{m-1}^{n}\mathrm{C}_{q-1}^{0} \\
&\equiv \mathrm{C}_{m-1}^{n-1} + \mathrm{C}_{m-1}^{n}
\end{aligned}$$

  Donc $\mathrm{C}_{qm}^{qn} \equiv \mathrm{C}_m^n$.

- Second cas : $n' \neq 0$. Il faut démontrer que : $\mathrm{C}_{qm}^{qn+n'} \equiv 0$. Puisque $m' < n'$, alors $m \neq n$. Donc $m > n$.

$$\begin{aligned}
\mathrm{C}_{qm}^{qn+n'} &\equiv \mathrm{C}_{q(m-1)+(q-1)}^{qn+(n'-1)} + \mathrm{C}_{q(m-1)+(q-1)}^{qn+n'} \\
&\equiv \mathrm{C}_{m-1}^{n}\mathrm{C}_{q-1}^{n'-1} + \mathrm{C}_{m-1}^{n}\mathrm{C}_{q-1}^{n'} \quad \text{(puisque } m > n\text{)} \\
&\equiv \mathrm{C}_{m-1}^{n}\mathrm{C}_{q}^{n'}
\end{aligned}$$

  Or, puisque $n' < q$, alors

$$\mathrm{C}_q^{n'} = \frac{q}{q-n'}\mathrm{C}_{q-1}^{n'} = \frac{p^\alpha}{p^\alpha - n'}\mathrm{C}_{q-1}^{n'}.$$

  Donc, puisque $n' > 0$, $\mathrm{C}_q^{n'}$ est divisible par p. Alors $\mathrm{C}_q^{n'} \equiv 0$, et $\mathrm{C}_{qm}^{qn+n'} \equiv 0$.

- Donc (1) est vrai au rang m pour $m' = 0$.

b.b. Supposons que les congruences soient vraies du rang $(m;0)$ jusqu'au rang $(m;m'-1)$ (avec $0 < m' < q$), quels que soient les entiers n et n' satisfaisant les 3 conditions. Démontrons qu'elles sont vraies au rang $(m;m')$, quels que soient les entiers n et n' satisfaisant les 3 conditions.

- Si $n' = 0$:

  - Si $n = 0$:

$$\mathrm{C}_{qm+m'}^{qn+n'} = 1 \equiv \mathrm{C}_m^n\mathrm{C}_{m'}^{n'}.$$

  - Si $n > 0$:

$$\begin{aligned}
\mathrm{C}_{qm+m'}^{qn+n'} &\equiv \mathrm{C}_{qm+(m'-1)}^{q(n-1)+(q-1)} + \mathrm{C}_{qm+(m'-1)}^{qn} \\
&\equiv 0 + \mathrm{C}_m^n\mathrm{C}_{m'-1}^{0} \quad \text{(puisque } q-1 > m'-1\text{)} \\
&\equiv \mathrm{C}_m^n \\
&\equiv \mathrm{C}_m^n\mathrm{C}_{m'}^{n'} \quad \text{(puisque } \mathrm{C}_{m'}^{n'} = \mathrm{C}_{m'}^{0} = 1\text{)}
\end{aligned}$$

– Si $0 < n' < m'$:

$$\begin{aligned}
\mathrm{C}_{qm+m'}^{qn+n'} &\equiv \mathrm{C}_{qm+(m'-1)}^{qn+(n'-1)} + \mathrm{C}_{qm+(m'-1)}^{qn+n'} \\
&\equiv \mathrm{C}_m^n \mathrm{C}_{m'-1}^{n'-1} + \mathrm{C}_m^n \mathrm{C}_{m'-1}^{n'} \\
&\equiv \mathrm{C}_m^n \mathrm{C}_{m'}^{n'}
\end{aligned}$$

– Si $n' = m'$:

  – Si $n < m$:

$$\begin{aligned}
\mathrm{C}_{qm+m'}^{qn+n'} &\equiv \mathrm{C}_{qm+(m'-1)}^{qn+(n'-1)} + \mathrm{C}_{qm+(m'-1)}^{qn+n'} \\
&\equiv \mathrm{C}_m^n \mathrm{C}_{m'-1}^{n'-1} + 0 \quad (\text{puisque } n' > m'-1) \\
&\equiv \mathrm{C}_m^n \mathrm{C}_{m'}^{n'} \quad (\text{puisque } \mathrm{C}_{m'}^{n'} = \mathrm{C}_{m'-1}^{n'-1} = 1)
\end{aligned}$$

  – Si $n = m$:

$$\mathrm{C}_{qm+m'}^{qn+n'} = 1 \equiv \mathrm{C}_m^n \mathrm{C}_{m'}^{n'}.$$

– Si $n' > m'$: (Dans ce cas, $n < m$).

$$\mathrm{C}_{qm+m'}^{qn+n'} \equiv \mathrm{C}_{qm+(m'-1)}^{qn+(n'-1)} + \mathrm{C}_{qm+(m'-1)}^{qn+n'} \equiv 0 + 0 \equiv 0$$

– Donc les 2 congruences sont vraies au rang $(m; m')$, quels que soient les entiers n et n' satisfaisant les 3 conditions.

b.c. Donc elles sont vraies au rang m, quels que soient les 3 entiers n, m' et n' satisfaisant les 3 conditions.

c. Les deux congruences sont démontrées.

2.2 Autre démonstration du théorème (1)

Pour $i < j$, on pose $\mathrm{C}_i^j = 0$. Ainsi pour tout $(i, j) \in \mathbb{N}^2$, $\mathrm{C}_i^j + \mathrm{C}_i^{j+1} = \mathrm{C}_{i+1}^{j+1}$.
La formule de Vandermonde donne :

$$\mathrm{C}_{qm+m'}^{qn+n'} = \sum_{i=0}^{n'} \mathrm{C}_{qm}^{qn+n'-i} \mathrm{C}_{m'}^{i}.$$

Démontrons que si $0 < k < q$, alors $\mathrm{C}_{qm}^{qn+k} \equiv 0$. On a : $\mathrm{C}_{qm}^{qn+k} = \dfrac{qm}{qm - qn - k} \mathrm{C}_{qm-1}^{qn+k}$. qm est divisible par p^α, mais pas $qm - qn - k$, car $k < p^\alpha$. Donc $\dfrac{qm}{qm - qn - k}$ est divisible par p. Donc $\mathrm{C}_{qm}^{qn+k} \equiv 0$.

Donc si $0 \leqslant i < n'$, alors $\mathrm{C}_{qm}^{qn+n'-i} \equiv 0$. Donc $\mathrm{C}_{qm+m'}^{qn+n'} \equiv \mathrm{C}_{qm}^{qn} \mathrm{C}_{m'}^{n'}$.

Démontrons maintenant que $\mathrm{C}_{pm}^{pn} \equiv \mathrm{C}_m^n$.

$$
\mathrm{C}_{pm}^{pn} = \frac{(pm)!}{(pn)!\,(p(m-n))!} = \frac{\displaystyle\prod_{i=0}^{m-1}\prod_{j=1}^{p} ip+j}{\left(\displaystyle\prod_{i=0}^{n-1}\prod_{j=1}^{p} ip+j\right)\left(\displaystyle\prod_{i=0}^{m-n-1}\prod_{j=1}^{p} ip+j\right)}
$$

$$
= \frac{\displaystyle\prod_{i=0}^{m-1}\prod_{j=1}^{p-1} ip+j}{\left(\displaystyle\prod_{i=0}^{n-1}\prod_{j=1}^{p-1} ip+j\right)\left(\displaystyle\prod_{i=0}^{m-n-1}\prod_{j=1}^{p-1} ip+j\right)} \times \frac{p^m m!}{p^n n! p^{m-n}(m-n)!}
$$

Dans le membre de gauche de ce produit, aucun terme n'est nul modulo p. Par suite, ce membre est congru à :

$$
\frac{\displaystyle\prod_{i=0}^{m-1}\prod_{j=1}^{p-1} j}{\left(\displaystyle\prod_{i=0}^{n-1}\prod_{j=1}^{p-1} j\right)\left(\displaystyle\prod_{i=0}^{m-n-1}\prod_{j=1}^{p-1} j\right)} \equiv \frac{(p-1)!^m}{(p-1)!^n (p-1)!^{m-n}} \equiv 1.
$$

Et le membre de droite est égal à : $\dfrac{m!}{n!(m-n)!} = \mathrm{C}_m^n$. Il en résulte que $\mathrm{C}_{pm}^{pn} \equiv \mathrm{C}_m^n$.

On démontre par récurrence sur α que, si $q = p^\alpha$, alors $\mathrm{C}_{qm}^{qn} \equiv \mathrm{C}_m^n$.

Donc $\boxed{\mathrm{C}_{qm+m'}^{qn+n'} \equiv \mathrm{C}_m^n \mathrm{C}_{m'}^{n'}}$.

Si $m' < n'$, alors $\mathrm{C}_{m'}^{n'} = 0$ et donc $\mathrm{C}_{qm+m'}^{qn+n'} \equiv 0$.

2.3 Remarques (exemples avec $p = 2$, $p = 3$ et $p = 5$)

```
p = 2 :           1
                 1 1
                1 0 1
               1 1 1 1
              1 0 0 0 1
             1 1 0 0 1 1
            1 0 1 0 1 0 1
           1 1 1 1 1 1 1 1
          1 0 0 0 0 0 0 0 1
         1 1 0 0 0 0 0 0 1 1
        1 0 1 0 0 0 0 0 1 0 1
       1 1 1 1 0 0 0 0 1 1 1 1
      1 0 0 0 1 0 0 0 1 0 0 0 1
     1 1 0 0 1 1 0 0 1 1 0 0 1 1
    1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
   1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
  1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1
```

```
p = 3 :           1
                 1 1
                1 2 1
               1 0 0 1
              1 1 0 1 1
             1 2 1 1 2 1
            1 0 0 2 0 0 1
           1 1 0 2 2 0 1 1
          1 2 1 2 1 2 1 2 1
         1 0 0 0 0 0 0 0 0 1
        1 1 0 0 0 0 0 0 0 1 1
       1 2 1 0 0 0 0 0 0 1 2 1
      1 0 0 1 0 0 0 0 0 1 0 0 1
     1 1 0 1 1 0 0 0 0 1 1 0 1 1
    1 2 1 1 2 1 0 0 0 1 2 1 1 2 1
   1 0 0 2 0 0 1 0 0 1 0 0 2 0 0 1
  1 1 0 2 2 0 1 1 0 1 1 0 2 2 0 1 1
 1 2 1 2 1 2 1 2 1 1 2 1 2 1 2 1 2 1
```

```
p = 5 :                                 [1]                                           Ligne  0
                                       1   1                                          Ligne  1
                                     1   2   1                                        Ligne  2
                                   1   3   3   1                                      Ligne  3
                                 1   4   1   4   1                                    Ligne  4
                              [1]  0   0   0   0  [1]                                 Ligne  5
                             1   1   0   0   0   1   1                                Ligne  6
                           1   2   1   0   0   1   2   1                              Ligne  7
                         1   3   3   1   0   1   3   3   1                            Ligne  8
                       1   4   1   4   1   1   4   1   4   1                          Ligne  9
                    [1]  0   0   0   0  [2]  0   0   0   0  [1]                       Ligne 10
                   1   1   0   0   0   2   2   0   0   0   1   1                      Ligne 11
                 1   2   1   0   0   2   4   2   0   0   1   2   1                    Ligne 12
               1   3   3   1   0   2   1   1   2   0   1   3   3   1                  Ligne 13
             1   4   1   4   1   2   3   2   3   2   1   4   1   4   1                Ligne 14
          [1]  0   0   0   0  [3]  0   0   0   0  [3]  0   0   0   0  [1]             Ligne 15
         1   1   0   0   0   3   3   0   0   0   3   3   0   0   0   1   1            Ligne 16
       1   2   1   0   0   3   1   3   0   0   3   1   3   0   0   1   2   1          Ligne 17
     1   3   3   1   0   3   4   4   3   0   3   4   4   3   0   1   3   3   1        Ligne 18
   1   4   1   4   1   3   2   3   2   3   3   2   3   2   3   1   4   1   4   1      Ligne 19
[1]  0   0   0   0  [4]  0   0   0   0  [1]  0   0   0   0  [4]  0   0   0   0  [1]   Ligne 20
```

Voici quelques propriétés (analogues à celles des fractals) du triangle de Pascal dans $\mathbb{Z}/p\mathbb{Z}$, dues à la formule (1) :

- On retrouve les termes du triangle de Pascal en prenant les $\mathrm{C}_{kp}^{k'p}$.
- On retrouve les premières lignes de triangles de Pascal dont les termes sont multipliés par une constante (nombre au sommet).
- Pour $p = 2$, on peut construire le napperon de Sierpinsky, qui est un fractal.

2.4 Calcul rapide d'un terme du triangle de Pascal

Soient $m = \overline{m_a m_{a-1} \dots m_1 m_0}$ et $n = \overline{n_a n_{a-1} \dots n_1 n_0}$ (écriture de m et n en base p) avec $m \geqslant n$. Démontrons que :

$$\boxed{\text{Si } \forall\, r \in [0, a],\ m_r \geqslant n_r, \text{ alors } \mathrm{C}_m^n \equiv \prod_{i=0}^{a} \mathrm{C}_{m_i}^{n_i}. \text{ Sinon, } \mathrm{C}_m^n \equiv 0.}$$

On pose :

$$m(r) = \sum_{i=0}^{r} m_i p^i = \overline{m_r m_{r-1} \dots m_1 m_0},$$

$$n(r) = \sum_{i=0}^{r} n_i p^i = \overline{n_r n_{r-1} \dots n_1 n_0},$$

$$m'(r) = \sum_{i=r}^{a} m_i p^{i-r} = \overline{m_a m_{a-1} \dots m_{r+1} m_r}$$

et

$$n'(r) = \sum_{i=r}^{a} n_i p^{i-r} = \overline{n_a n_{a-1} \dots n_{r+1} n_r}.$$

$$\forall\, r \in [0,a],\ \mathrm{C}_m^n = \mathrm{C}_{m'(r+1)\cdot p^{r+1}+m(r)}^{n'(r+1)\cdot p^{r+1}+n(r)} \quad \text{avec} \quad \begin{cases} n'(r+1) \leqslant m'(r+1) \text{ puisque } n \leqslant m, \\ m(r) < p^{r+1} \text{ et } n(r) < p^{r+1}. \end{cases}$$

Note : la 3^e^ condition du théorème (1) est nécessairement satisfaite, sinon on aurait $m < n$.

- Premier cas : si $\exists\, r \in [0,a],\ m_r < n_r$, alors $\mathrm{C}_m^n \equiv 0$, car $m(r) < n(r)$.
- Second cas : si $\forall\, r \in [0,a],\ m_r \geqslant n_r$, alors

$$\begin{aligned} \mathrm{C}_m^n &\equiv \mathrm{C}_{m(a)}^{n(a)} \equiv \mathrm{C}_{m_a\cdot p^a+m(a-1)}^{n_a\cdot p^a+n(a-1)} \equiv \mathrm{C}_{m(a-1)}^{n(a-1)}\mathrm{C}_{m_a}^{n_a} \\ &\equiv \mathrm{C}_{m_{a-1}\cdot p^{a-1}+m(a-2)}^{n_{a-1}\cdot p^{a-1}+n(a-2)}\mathrm{C}_{m_a}^{n_a} \equiv \mathrm{C}_{m(a-2)}^{n(a-2)}\mathrm{C}_{m_{a-1}}^{n_{a-1}}\mathrm{C}_{m_a}^{n_a} \equiv \cdots \equiv \prod_{i=0}^{a}\mathrm{C}_{m_i}^{n_i} \end{aligned}$$

Conclusion : $$\boxed{\text{Si } \forall\, r \in [0,a],\ m_r \geqslant n_r, \text{ alors } \mathrm{C}_m^n \equiv \prod_{i=0}^{a}\mathrm{C}_{m_i}^{n_i}. \text{ Sinon, } \mathrm{C}_m^n \equiv 0.} \qquad (2)$$

Cette formule permet de calculer rapidement n'importe quel terme du triangle de Pascal.

3 Propriétés de divisibilité par p des termes d'une ligne du triangle de Pascal

3.1 Caractère de divisibilité par p d'un terme du triangle de Pascal

Dans le second cas de 2.4 : $\forall i,\ \mathrm{C}_{m_i}^{n_i} \not\equiv 0$ car $\mathrm{C}_{m_i}^{n_i} = \dfrac{m_i!}{n_i!\,(m_i-n_i)!}$ avec $m_i < p$ et $n_i < p$, et comme $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre, alors $\prod \mathrm{C}_{m_i}^{n_i} \not\equiv 0$. Donc $\mathrm{C}_m^n \not\equiv 0$.

Donc $\boxed{\mathrm{C}_m^n \text{ n'est pas divisible par } p \text{ si et seulement si } \forall i,\ m_i \geqslant n_i.}$ (3)

3.2 Calcul du nombre de termes non divisibles par p de la m^{e} ligne du triangle de Pascal

On donne m et on veut choisir n tel que $m \geqslant n$ et C_m^n ne soit pas divisible par p. Il faut donc que $\forall i,\ m_i \geqslant n_i$. m_i étant fixe, on a $m_i + 1$ possibilités de choisir le chiffre de rang i du nombre n. On a donc en tout $\prod(m_i+1)$ nombres n satisfaisants.

Donc *le nombre de termes non divisibles par p de la n^{e} ligne du triangle de Pascal est égal au produit des chiffres de n augmentés de 1 en base p.* (4)

4 Propriétés de congruences sur les colonnes du triangle de Pascal

4.1 Formule d'interpolation de Newton et propriétés

Les résultats de cette section seront utilisés dans la section suivante 4.2.

4.1.1 Formule d'interpolation de Newton

Soit F une fonction définie sur $\mathbb{N}$. On pose

$$\Delta^{(n)}F(p) = \Delta^{(n-1)}F(p+1) - \Delta^{(n-1)}F(p),$$

avec $\Delta^{(0)}F(p) = F(p)$ et $k_n = \Delta^{(n)}F(0)$.

Démontrons que

$$F(p) = \sum_{i=0}^{p} k_i \mathrm{C}_p^i \quad \text{(Formule d'interpolation de Newton).}$$

On démontre par récurrence sur n que

$$\Delta^{(n)}F(p) = \sum_{i=0}^{n} (-1)^{n-i} \mathrm{C}_n^i F(p+i).$$

Donc

$$k_n = \sum_{i=0}^{n} (-1)^{n-i} \mathrm{C}_n^i F(i).$$

$$\begin{aligned}
\sum_{i=0}^{p} k_i \mathrm{C}_p^i &= \sum_{i=0}^{p}\sum_{j=0}^{i} (-1)^{i-j} \mathrm{C}_p^i \mathrm{C}_i^j F(j) = \sum_{j=0}^{p}\sum_{i=j}^{p} (-1)^{i-j} \mathrm{C}_p^i \mathrm{C}_i^j F(j) \\
&= \sum_{j=0}^{p} F(j) \sum_{i=j}^{p} (-1)^{i-j} \frac{p!}{(p-i)!\,(i-j)!\,j!} \\
&= \sum_{j=0}^{p} F(j) \frac{p!}{j!} \sum_{i=j}^{p} (-1)^{i-j} \frac{1}{(p-i)!\,(i-j)!} \\
&= \sum_{j=0}^{p} F(j) \frac{p!}{j!} \sum_{i=j}^{p} (-1)^{i-j} \frac{(p-j)!}{(p-i)!\,(i-j)!\,(p-j)!} \\
&= \sum_{j=0}^{p} F(j) \frac{p!}{j!\,(p-j)!} \sum_{i=j}^{p} (-1)^{i-j} \mathrm{C}_{p-j}^{i-j} = \sum_{j=0}^{p} F(j) \cdot \mathrm{C}_p^j \sum_{i=0}^{p-j} (-1)^i \mathrm{C}_{p-j}^i \\
&= F(p) + \sum_{j=0}^{p-1} F(j) \cdot \mathrm{C}_p^j \sum_{i=0}^{p-j} (-1)^i \mathrm{C}_{p-j}^i \\
&= F(p) + \sum_{j=0}^{p-1} F(j) \cdot \mathrm{C}_p^j \cdot 0 = F(p)
\end{aligned}$$

Donc $\boxed{F(p) = \sum_{i=0}^{p} k_i \mathrm{C}_p^i}$

4.1.2 Remarque importante

On démontre aussi que F est un polynôme de degré d si et seulement si $k_d \neq 0$ et $\forall\, i > d,\ k_i = 0$.

4.2 Somme partielle des termes d'une colonne du triangle de Pascal élevés à une puissance entière

On appelle colonne du triangle de Pascal la suite des termes C_n^n, C_{n+1}^n, C_{n+2}^n, $\ldots$, C_p^n.

$$
\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 3 & & 3 & & 5 & & 1 & & \\
 & 1 & & 6 & & 1 & & 6 & & 1 & & 6 & & 1 & \\
1 & & 0 & & 0 & & 0 & & 0 & & 0 & & 0 & & 1
\end{array}
$$

FIG. 1 - *Exemple ($n = 2$, $p = 7$)*

On considère la somme partielle des termes d'une telle colonne élevés à une puissance entière α. Nous allons démontrer que pour p premier, si n et α vérifient $n\alpha < p - 1$, alors

$$\sum_{i=n}^{p} (\mathrm{C}_i^n)^\alpha \equiv 0 \pmod{p}.$$

Pour $n < q$, on pose $\mathrm{C}_n^q = 0$.

Soit $f(p, n, \alpha) = \displaystyle\sum_{i=n}^{p} (\mathrm{C}_i^n)^\alpha$ avec $\alpha \in \mathbb{N}^*$, $n \in \mathbb{N}^*$ et $p \in \mathbb{N}$. Si $n > p$, $f(p, n, \alpha) = 0$.

On note $\mathrm{d}^\circ(P)$ le degré d'un polynôme P. $\mathrm{d}^\circ\left(\mathrm{C}_i^n\right) = n$ où C_i^n est un polynôme en i, puisque

$$\forall\, (i, n) \in \mathbb{N}^2,\ \mathrm{C}_i^n = \frac{i!}{n!\,(i-n)!} = \frac{1}{n!}\prod_{a=1}^{n} i - n + a.$$

Notons que cette formule reste vraie quand $i < n$, car pour $a = n - i$, $i - n + a = 0$.

Donc $\mathrm{d}^\circ\left((\mathrm{C}_i^n)^\alpha\right) = n\alpha$ où $(\mathrm{C}_i^n)^\alpha$ est un polynôme en i.

Soit $F(p) = \displaystyle\sum_{i=0}^{p} (\mathrm{C}_i^n)^\alpha$ où $p \in \mathbb{N}$.

Les termes du polynôme $(\mathrm{C}_i^n)^\alpha$ se construisent par différence des termes de la fonction F : $\Delta^{(1)}F(p) = \left(\mathrm{C}_{p+1}^n\right)^\alpha$, et plus généralement :

$$\Delta^{(m+1)}F(p) = \Delta^{(m)}\left(\mathrm{C}_{p+1}^n\right)^\alpha.$$

Or pour $p = 0$, $\Delta^{(n\alpha)}\left(\mathrm{C}_{p+1}^{n}\right)^{\alpha} \neq 0$, et pour tout $m > n\alpha$, $\Delta^{(m)}\left(\mathrm{C}_{p+1}^{n}\right)^{\alpha} = 0$. Donc $\Delta^{(n\alpha+1)}F(0) \neq 0$, et pour tout $m > n\alpha + 1$, $\Delta^{(m)}F(0) = 0$. Donc $\mathrm{d}^\circ(F(p)) = n\alpha + 1$.

Comme $\forall\, i < n,\ \mathrm{C}_i^n = 0$, alors $F(p) = f(p, n, \alpha)$. Pour $p \in \mathbb{N}$, f est donc un polynôme en p de degré $n\alpha + 1$ et sans terme constant : $f(0) = F(0) = 0$.

D'après la formule d'interpolation de Newton,

$$f(p, n, \alpha) = \sum_{i=1}^{p} k_i \mathrm{C}_p^i = \sum_{i=1}^{p} k_i \frac{p!}{i!\,(p-i)!}.$$

Comme $\mathrm{d}^\circ(f) = n\alpha + 1$, alors $\forall\, i > n\alpha + 1,\ k_i = 0$.

Puisque $\forall\, p \in \mathbb{N},\ F(p) \in \mathbb{N}$, alors $\forall\, i \in \mathbb{N},\ k_i \in \mathbb{Z}$.

Soit p un nombre premier. Si $p > n\alpha + 1$,

$$f(p, n, \alpha) = \sum_{i=1}^{n\alpha+1} k_i \frac{p!}{i!\,(p-i)!}$$

puisque $\forall\, i > n\alpha + 1,\ k_i = 0$.

Puisque pour $0 < i < p$, $\dfrac{p!}{i!\,(p-i)!} \equiv 0 \pmod{p}$, alors

si p est un nombre premier et si $p > n\alpha + 1$, alors

$$\sum_{i=n}^{p} (\mathrm{C}_i^n)^\alpha \equiv 0 \pmod{p}.$$

5 Démonstration et généralisation du petit théorème de Fermat

5.1 Démonstration par récurrence du petit théorème de Fermat

On a évidemment : pour tout p, $1^p \equiv 1 \pmod{p}$. Supposons que, pour un entier naturel non nul a, on ait pour tout p premier, $a^p \equiv a \pmod{p}$. Démontrons que : pour tout p premier, $(a+1)^p \equiv a+1 \pmod{p}$.

D'après la formule du développement du binôme de Newton, on a :

$$\forall p,\ (a+1)^p = \sum_{i=0}^{p} a^i \mathrm{C}_p^i.$$

Or, pour p premier et $0 < i < p$, $\mathrm{C}_p^i \equiv 0 \pmod{p}$. Donc, pour tout p premier,

$$(a+1)^p \equiv a^0 \mathrm{C}_p^0 + a^p \mathrm{C}_p^p \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

Donc $\boxed{\text{pour tout } a \in \mathbb{N}^* \text{ et } p \text{ premier, } a^p \equiv a \pmod{p}.}$ (Petit théorème de Fermat)

5.2 Généralisation du petit théorème de Fermat

Soit $n \in \mathbb{N}^*$ tel que $n \equiv 1 \pmod{p-1}$. Démontrons que :

$$\forall\, a \in \mathbb{N}^*,\ \ a^n \equiv a \pmod{p}.$$

Si $a \equiv 0 \pmod{p}$, c'est évident.

Si $a \not\equiv 0 \pmod{p}$, alors soit $k = \frac{n-1}{p-1}$. On a : $a^p \equiv a \pmod{p}$, et puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, alors $a^{p-1} \equiv 1 \pmod{p}$. Donc

$$a^{n-1} = a^{k(p-1)} = (a^{p-1})^k \equiv 1^k \equiv 1 \pmod{p}.$$

Donc $a^n \equiv a \pmod{p}$.

Donc $\boxed{\text{si } p \text{ est premier et } n \equiv 1 \pmod{p-1}, \text{ alors } \forall\, a \in \mathbb{N}^*,\ a^n \equiv a \pmod{p}.}$

Le texte original présenté au concours du Prix Fermat Junior a été assez largement remanié, suite aux suggestions des membres du jury du Prix Fermat Junior et de Daniel Loeb de Bordeaux. Qu'ils en soient remerciés.