Generalized Lucas' Theorem

[a]Mourad ABCHICHE and [b]Hacène BELBACHIR
USTHB/ [a]LTN Lab., [b]RECITS Lab., DG-RSDT,
BP 32, El Alia, 16111 Bab Ezzouar, Algiers, Algeria.
mabchiche@usthb.dz, hbelbachir@usthb.dz

Abstract

We generalize the well known congruence Lucas' Theorem for binomial coefficient to the bi^{s}nomial coefficients.

AMS classification. 11A07; 05A10; 11B65.
Keys words. Binomial coefficient; Lucas' Theorem; Congruence.

1 Introduction

Let p be a prime number. It is well known that, for $1 \leq k \leq p-1$, p divide $\binom{p}{k}$. This gives $(1+x)^p \equiv 1 + x^p \pmod{p}$. Let $n = n_0 + n_1 p$ and $k = k_0 + k_1 p$ $(0 \leq n_0, k_0 < p)$ and $n_1, k_1 \in \mathbb{N}$, then $(1+x)^n = (1+x^p)^{n_1}(1+x)^{n_0} \pmod{p}$. Identifying the coefficients of x^k in the two expressions, we get

$$\binom{n}{k} = \binom{n_0 + n_1 p}{k_0 + k_1 p} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1} \pmod{p}.$$

More generally, let $n = n_0 + n_1 p + \cdots + n_m p^m$ and $k = k_0 + k_1 p + \cdots + k_m p^m$, $0 \leq n_i, k_i < p$ $(0 \leq i \leq m-1)$ and $n_m, k_m \in \mathbb{N}$, we get

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1} \cdots \binom{n_m}{k_m} \pmod{p}.$$

It is known as formula of Lucas since 1878, [3]. It expresses the remainder of division of $\binom{n}{m}$ by p. For an historical development, we refer to Granville [4].

2 Bi^{s}nomial coefficients

The bi^{s}nomial coefficients are a natural extension of binomial coefficients (see [2, 1] for a recent overview). Letting $s, L \in \mathbb{N}$, for an integer $k = 0, 1, \ldots, sL$, the bi^{s}nomial coefficient $\binom{L}{k}_s$ is the k-th term of the expansion

$$\left(1 + x + x^2 + \cdots + x^s\right)^L = \sum_{k \geq 0} \binom{L}{k}_s x^k. \tag{1}$$

with $\binom{L}{k}_1 = \binom{L}{k}$ (being the usual binomial coefficient) and $\binom{L}{k}_s = 0$ for $k > sL$. Using the classical binomial coefficient, one has

$$\binom{L}{k}_s = \sum_{j_1 + j_2 + \cdots + j_s = k} \binom{L}{j_1} \binom{j_1}{j_2} \cdots \binom{j_{s-1}}{j_s}. \tag{2}$$

Combinatorial interpretation: $\binom{L}{k}_s$ *count the number of ways of distributing "k" balls among "L" cells with at most "s" balls by cell.*

3 Generalized Lucas' Theorem

We start by expressing the cyclotomic polynomial of degree s.

Theorem 1 *Let p be a prime number, $n = n_0 + n_1 p$ and $k = k_0 + k_1 p$ two integers with $0 \leq n_0, k_0 < p$ and $n_1, k_1 \in \mathbb{N}$. The following identity holds*

$$\binom{n}{k}_s \equiv \sum_{i=0}^{s-1} \binom{n_0}{k_0 + ip}_s \binom{n_1}{k_1 - i}_s \pmod{p}. \tag{3}$$

Proof. The induction gives $(1+x+\cdots+x^s)^p \equiv 1+x^p+\cdots+x^{sp} (\bmod p)$. Then

$$\begin{aligned}(1+x+\cdots+x^s)^n &= (1+x+\cdots+x^s)^{n_1 p}(1+x+\cdots+x^s)^{n_0}\\ &\equiv (1+x^p\cdots+x^{sp})^{n_1}(1+x\cdots+x^s)^{n_0} (\bmod p)\\ &\equiv \textstyle\sum_{i=0}^{sn_1}\binom{n_1}{i}_s x^{pi}\sum_{j=0}^{sn_0}\binom{n_0}{j}_s x^j \ (\bmod p)\\ &\equiv \textstyle\sum_{k=0}^{sn}\sum_{pi+j=k}\binom{n_1}{i}_s\binom{n_0}{j}_s x^k (\bmod p).\end{aligned}$$

Identifying with $\sum_{k=0}^{sn}\binom{n}{k}_s x^k$, we get $\binom{n}{k}_s \equiv \sum_{pi+j=k}\binom{n_1}{i}_s\binom{n_0}{j}_s (\bmod p)$. The equality $pi+j=k_1p+k_0$ $(0 \le j \le sn_0 < sp)$ gives $i=k_1$, $j=k_0$, or $i<k_1$, $j>k_0$, thus $p(k_1-i)=j-k_0$ so p divide $j-k_0$. We conclude that $(i,j) \in \{(k_1,k_0),(k_1-1,k_0+p),...,(k_1-s+1,k_0+(s-1)p)\}$.
□

The following result generalizes the above one.

Theorem 2 *Let p be a prime number, $n=n_0+n_1p+\cdots+n_mp^m$ and $k=k_0+k_1p+\cdots+k_mp^m$ two integers with $0 \le n_i,k_i < p$ $(0 \le i \le m-1)$ and $n_m,k_m \in \mathbb{N}$. The following identity holds*

$$\binom{n}{k}_s \equiv \sum_{0\le i_0,i_1,\ldots,i_{m-1}\le s-1}\ \prod_{j=0}^{m}\binom{n_j}{k_j+i_jp-i_{j-1}}_s (\bmod p), \qquad (4)$$

with $i_{-1}=0$ and $i_m=0$.

Proof. The case $m=1$ gives the identity of Theorem 1. Assuming that the identity (4) is true for an integer m, we shall prove it for $m+1$. Let $n=n_0+n_1p+\cdots+n_{m+1}p^{m+1}$ *and* $k=k_0+k_1p+\cdots+k_{m+1}p^{m+1}$, Theorem 1 gives

$$\binom{n}{k}_s \equiv \sum_{i_0=0}^{s-1}\binom{n_0}{k_0+i_0p}_s\binom{n_1+n_2p+\cdots+n_{m+1}p^m}{k_1-i_0+k_2p+\cdots+k_{m+1}p^m}_s (\bmod p).$$

Then

$$\begin{aligned}\binom{n}{k}_s &\equiv \sum_{i_0=0}^{s-1}\binom{n_0}{k_0+i_0p}_s \sum_{0\le i_1,\dots,i_m\le s-1}\binom{n_1}{k_1+i_1p-i_0}_s \\ &\qquad \prod_{j=2}^{m+1}\binom{n_j}{k_j+i_jp-i_{j-1}}_s \pmod p\\ &\equiv \sum_{0\le i_1,\dots,i_m\le s-1}\sum_{i_0=0}^{s-1}\binom{n_0}{k_0+i_0p}_s\binom{n_1}{k_1+i_1p-i_0}_s \\ &\qquad \prod_{j=2}^{m+1}\binom{n_j}{k_j+i_jp-i_{j-1}}_s \pmod p\\ &\equiv \sum_{0\le i_0,i_1,\dots,i_m\le s-1}\prod_{j=0}^{m+1}\binom{n_j}{k_j+i_jp-i_{j-1}}_s \pmod p,\end{aligned}$$

with $i_{-1} = 0$ and $i_{m+1} = 0$. □

Acknowledgments. The authors thank the referee for valuable advice and comments which helped to improve the quality of this paper.

References

[1] H. Belbachir (2011), Determining the mode for convolution powers for discrete uniform distribution, Probab. Engrg. Inform. Sci. 25, 4, 469–475.

[2] H. Belbachir, S. Bouroubi, A. Khelladi (2008), Connection between bi^{s}nomial coefficients, Fibonacci numbers, Bell polynomials and discrete uniform distribution, Annales Mathematicae et Informaticae, 35, 21–30.

[3] E. Lucas (1878), Théorie des Fonctions Numériques Simplement Périodiques, American Journal of Mathematics 1 (3), 197–240 (part 2).

[4] A. Granville (1997), Arithmetic Properties of Binomial Coefficients I: Binomial coefficients modulo prime powers. Canadian Mathematical Society Conference Proceedings 20, 253–275.