Journal of Number Theory 168 (2016) 154–166

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Gaussian binomial coefficients modulo cyclotomic polynomials

Yan Li [a], Daeyeoul Kim [b,*], Lianrong Ma [c]

[a] Department of Applied Mathematics, China Agricultural University, Beijing 100083, China
[b] National Institute for Mathematical Sciences, Yuseong-daero 1689-gil, Yuseong-gu, Daejeon 305-811, South Korea
[c] Department of Mathematical Sciences, Tsinghua University, 100084, Beijing, China

ARTICLE INFO

Article history:
Received 23 December 2014
Received in revised form 22 April 2016
Accepted 22 April 2016
Available online 6 June 2016
Communicated by David Goss

MSC:
11A07
11B65
05A10

Keywords:
Congruence
Binomial coefficients
Gaussian binomial coefficients
q-Series
Cyclotomic polynomials

ABSTRACT

In this paper, we give q-analogies of classical Kummer, Lucas and ASH (Anton, Stickelberger, Hensel)'s results on binomial coefficients modulo primes. Our results generalize the previous result by T. Cai (2001) [1].

* Corresponding author.
E-mail addresses: liyan_00@cau.edu.cn, liyan_00@mails.tsinghua.edu.cn (Y. Li), daeyeoul@nims.re.kr (D. Kim), lrma@math.tsinghua.edu.cn (L. Ma).

http://dx.doi.org/10.1016/j.jnt.2016.04.005
0022-314X/

1. Introduction

The binomial coefficients are very important in mathematics. Their congruence properties were studied by many mathematicians.

In 1852 Kummer discovered an elegant result on binomial coefficients:

Kummer's criteria: Let $n \geq m \geq 0$ be integers and p be any prime. The exact power of p dividing the binomial coefficient $\binom{n}{m}$ is given by the number of "carries" when adding m and $n-m$ in base p.

In the following, we define $\binom{n}{m} = 1$ if $m = 0$ and 0 if neither $n \geq m \geq 0$ nor $m = 0$.

In 1878 Lucas proved the following famous result.

Lucas' result: Let $n \geq m \geq 0$ be integers and p be a prime. Let $n = \sum_{i=0}^{d} n_i p^i$ and $m = \sum_{i=0}^{d} m_i p^i$ with $0 \leq n_i, m_i \leq p-1$ be their expansions in base p. Then we have

$$\binom{n}{m} \equiv \prod_{i=0}^{d} \binom{n_i}{m_i} \pmod{p}. \tag{1}$$

Lucas' result was originally written in his *Theorie des Nombres* (pp. 417–420).

The following result was discovered by each of Anton (1869), Stickelberger (1890), Hensel (1902) and many others since.

ASH's result: Let $n \geq m \geq 0$ be integers and p be a prime. Assume p^t exactly divides $\binom{n}{m}$. Denote $l = n - m$. Let $n = \sum_{i=0}^{d} n_i p^i$, $m = \sum_{i=0}^{d} m_i p^i$ and $l = \sum_{i=0}^{d} l_i p^i$ with $0 \leq n_i, m_i, l_i \leq p-1$ be their expansions in base p. Then

$$\frac{1}{p^t}\binom{n}{m} \equiv (-1)^t \left(\frac{n_0!}{m_0! l_0!}\right)\left(\frac{n_1!}{m_1! l_1!}\right)\cdots\left(\frac{n_d!}{m_d! l_d!}\right) \pmod{p}.$$

All of the above results can be found in Granville's nice paper [4], which also gives many interesting properties on the binomial coefficients modulo prime powers and historical reviews.

To state our results, we introduce some standard notations first.

Let

$$[n]_q = \frac{1-q^n}{1-q},$$
$$[n]_q! = [n]_q \cdot [n-1]_q \cdots [1]_q,$$
$$(a;q)_n = (1-a)(1-aq)\cdots(1-aq^{n-1})$$

be the q-bracket, the q-factorial, and the q-Pochhammer symbol, respectively, where n is a positive integer. Clearly, letting $q \to 1$, then $[n]_q \to n$ and $[n]_q! \to n!$.

Let the Gaussian binomial coefficients be

$$\binom{n}{m}_q = \frac{[n]_q!}{[m]_q![n-m]_q!} = \frac{(1-q)(1-q^2)\cdots(1-q^{n-1})(1-q^n)}{(1-q)\cdots(1-q^m)(1-q)\cdots(1-q^{n-m})},$$