

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/265644350>

Lucas' theorem: its generalizations, extensions and applications (1878--2014)

Article · September 2014

Source: arXiv

CITATION

1

READS

284

1 author:



Romeo Meštrović

University of Montenegro

142 PUBLICATIONS 260 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Romeo mestrovic zarko pavicevic [View project](#)

LUCAS' THEOREM: ITS GENERALIZATIONS, EXTENSIONS AND APPLICATIONS (1878–2014)

ROMEO MEŠTROVIĆ

ABSTRACT. In 1878 É. Lucas proved a remarkable result which provides a simple way to compute the binomial coefficient $\binom{n}{m}$ modulo a prime p in terms of the binomial coefficients of the base- p digits of n and m : *If p is a prime, $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^s$ are the p -adic expansions of nonnegative integers n and m , then*

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

The above congruence, the so-called *Lucas' theorem* (or *Theorem of Lucas*), plays an important role in Number Theory and Combinatorics. In this article, consisting of six sections, we provide a historical survey of Lucas type congruences, generalizations of Lucas' theorem modulo prime powers, Lucas like theorems for some generalized binomial coefficients, and some their applications.

In Section 1 we present the fundamental congruences modulo a prime including the famous Lucas' theorem. In Section 2 we mention several known proofs and some consequences of Lucas' theorem. In Section 3 we present a number of extensions and variations of Lucas' theorem modulo prime powers. In Section 4 we consider the notions of the Lucas property and the double Lucas property, where we also present numerous integer sequences satisfying one of these properties or a certain Lucas type congruence. In Section 5 we collect several known Lucas type congruences for some generalized binomial coefficients. In particular, this concerns the Fibonomial coefficients, the Lucas u -nomial coefficients, the Gaussian q -nomial coefficients and their generalizations. Finally, some applications of Lucas' theorem in Number Theory and Combinatorics are given in Section 6.

2010 *Mathematics Subject Classification*. Primary 11B75, 11A07, 05A10, 11B65; Secondary 11B37, 11B39, 11B50, 11B73.

Keywords and phrases: prime, prime power, binomial coefficient, congruence modulo a prime (prime power), p -adic expansion of an integer, Lucas' theorem, Lucas' congruence, Wolstenholme type congruence, Lucas type congruence, variation of Lucas' theorem modulo prime powers, generalization of Lucas' theorem, Lucas property, double Lucas property, generalized binomial coefficient, Fibonomial coefficient, Lucas u -nomial coefficient, Gaussian q -nomial coefficient, Pascal's triangle, p -Lucas property.

CONTENTS

1 Introduction	3
2 Lucas' theorem and its variations	5
2.1 Lucas' theorem	5
2.2 Some consequences and extensions of Lucas' theorem	7
3 Lucas type congruences for prime powers	10
3.1 Wolstenholme type congruences	10
3.2 Variations of Lucas' theorem modulo prime powers	11
3.3 Characterizations of Wolstenholme primes	17
4 The Lucas property and the p-Lucas property	18
4.1 The Lucas property and the double Lucas property	18
4.2 Further Lucas type congruences	23
5 Lucas type theorems for some generalized binomial coefficients	27
5.1 Generalized binomial coefficients and related Lucas type congruences	27
5.2 Lucas type congruences for some classes of Lucas u -nomial coefficients	32
6 Some applications of Lucas' theorem	36
6.1 Lucas' theorem and the Pascal's triangle	36
6.2 Another applications of Lucas's theorem	40
References	43
Appendix	49

1. INTRODUCTION

Prime numbers have been studied since the earliest days of mathematics. Congruences modulo primes have been widely investigated since the time of Fermat. There are numerous useful and often remarkable congruences and divisibility results for binomial coefficients; see [36, Ch. XI] for older results and [52] for a modern perspective.

Let p be a prime. Then by *Fermat little theorem*, for each integer a not divisible by p

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, by *Wilson theorem*, for any prime p

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

In attempting to discover some analogous expression which should be divisible by n^2 , whenever n is a prime, but not divisible if n is a composite number, in 1819 Charles Babbage [9] is led to the congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$$

for all primes $p \geq 3$. In 1862 J. Wolstenholme [142] proved that the above congruence holds modulo p^3 for any prime $p \geq 5$.

The study of arithmetic properties of binomial coefficients has a rich history. As noticed in [52], many great mathematicians of the nineteenth century considered problems involving binomial coefficients modulo a prime power (for instance Babbage [9], Cauchy, Cayley, Gauss [45], Hensel, Hermite [57], Kummer [80], Legendre, Lucas [86] and [87], and Stickelberger). They discovered a variety of elegant and surprising theorems which are often easy to prove. For more information on these classical results, their extensions, and new results about this subject, see books of Dickson [36, Chapter IX] and Guy [53], while a more modern treatment of the subject is given by A. Granville [52].

Suppose that a prime p and pair of integers $n \geq m \geq 0$ are given. A beautiful *theorem of E. Kummer* of 1852 ([80, pp. 115–116]; also see [36, p. 270]) states that *the exact power of the prime p which divides $\binom{n}{m}$ is given by the number of “carries” when m and $n - m$ are added in base p arithmetic*. This is a fundamental result in the study of divisibility properties of binomial coefficients.

If $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^s$ are the p -adic expansions of nonnegative integers n and m (so that $0 \leq m_i, n_i \leq p-1$ for each i), then by *Lucas's theorem* established by Édouard Lucas in 1878

[86] (also see [36, p. 271] and [52]),

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

The same result is without proof also presented by Lucas in 1878, in Section XXI of his massive journal paper [87, pp. 229–230].

This remarkable result by Lucas provides a simple way to compute the binomial coefficient $\binom{n}{m}$ modulo a prime p in terms of the binomial coefficients of the base- p digits of n and m . The above congruence, the so-called Lucas' theorem (or Theorem of Lucas) is a very important congruence in Combinatorial Number Theory and Combinatorics. In particular, this concerns the divisibility of binomial coefficients by primes. In this article, consisting of six sections, we provide a historical survey of Lucas type congruences, generalizations of Lucas' theorem modulo prime powers and Lucas like theorems for some classes of generalized binomial coefficients. Furthermore, we present some known applications of Lucas' theorem and certain of its variations in Number Theory and Combinatorics.

This article is organized as follows. In Section 2 we mention several known algebraic and combinatorial proofs of Lucas' theorem. We also give some consequences and variations of Lucas' theorem. In Section 3 we present a number of extensions and variations of Lucas' theorem modulo prime powers. In Section 4 we consider the notions of the Lucas property and the double Lucas property. In this section we also present numerous integer sequences satisfying one of these properties or a certain similar Lucas type congruence. In particular, these properties are closely related to the divisibility properties of certain binomial coefficients, matrices, different binomial sums, Apéry numbers, Delannoy numbers, Stirling numbers of the first and second kind etc. In Section 5 we collect several known Lucas type congruences for some generalized binomial coefficients. In particular, this concerns the Fibonomial coefficients, the Lucas u -nomial coefficients, the Gaussian q -nomial coefficients and some their generalizations. Finally, applications of Lucas' theorem are given in Section 6 of this survey article. Some of these applications are closely related to the determination of number of entries of Pascal's triangle with a prescribed divisibility property. We also present some known primality criteria whose proofs are based on Lucas' theorem. Furthermore, we give certain known results concerning the characterizations of the algebraicity of some classes of formal power series in terms of the notion of the p -Lucas property.

2. LUCAS' THEOREM AND ITS VARIATIONS

2.1. Lucas' theorem. As noticed above, if $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^s$ are the p -adic expansions of integers n and m such that $0 \leq m_i, n_i \leq p-1$ for each $i = 0, 1, \dots, s$, then a beautiful *Lucas's theorem* ([86]; also see [52] ([86] and [36, p. 271]) states that

$$(1) \quad \binom{n}{m} \equiv \prod_{i=0}^s \binom{n_i}{m_i} \pmod{p}.$$

(with the usual convention that $\binom{0}{0} = 1$, and $\binom{l}{r} = 0$ if $l < r$). The congruence (1) was established by Lucas by considering patterns in Pascal's triangle. Furthermore, (1) is equivalent to the following Lucas' earlier generalization [86, p. 52] of an 1869 result of H. Anton [7, pp. 303–306] (also see [36, p. 271]):

$$(2) \quad \binom{n}{m} \equiv \binom{n \operatorname{div} p}{m \operatorname{div} p} \binom{n \bmod p}{m \bmod p} \pmod{p},$$

where $n \operatorname{div} p$ denotes the integer quotient of n by a prime p , and $n \bmod p$ its remainder. The congruence (2) is in fact the equivalent form of Lucas' theorem which is often stated in the following way:

$$(3) \quad \binom{np+r}{mp+s} \equiv \binom{n}{m} \binom{r}{s} \pmod{p},$$

where p is a prime, n, m, r and s are nonnegative integers such that $0 \leq r, s \leq p-1$.

If a prime p divides $\binom{n}{m}$ then (1) follows easily from Kummer's theorem. However, if p^l is the exact power of p dividing $\binom{n}{m}$, then we might ask for the value of $\frac{1}{p^l} \binom{n}{m} \pmod{p}$. The related result was discovered by H. Anton in 1869 [7] (see also [52], [75, pp. 3–4] and [121]) who proved that if p^l is the exact power of p dividing $\binom{n}{m}$, (l is by Kummer's theorem, the number of "carries" when m and $n-m$ are added in base p arithmetic), then

$$(4) \quad \frac{(-1)^l}{p^l} \binom{n}{m} \equiv \frac{n_0!}{m_0!r_0!} \cdot \frac{n_1!}{m_1!r_1!} \cdots \frac{n_s!}{m_s!r_s!} \pmod{p},$$

where $n = n_0 + n_1p + \cdots + n_sp^s$, $m = m_0 + m_1p + \cdots + m_sp^s$, and $r = n - m = r_0 + r_1p + \cdots + r_sp^s$ with $0 \leq m_i, n_i, r_i \leq p-1$ for each $i = 0, 1, \dots, s$.

Remark 1. Numerous authors have asked whether there is an analogous congruence modulo p^l to (4), for arbitrary $l \geq 1$. In 1995 A. Granville [52, Theorem 1] gave a positive answer to this question (see the congruence (33)) in Subsection 3.2. \square

The several proofs offered for Lucas' theorem are primarily of two types—algebraic and combinatorial. The well known algebraic proof of Lucas' theorem due to N.J. Fine [39] in 1947 is based on the binomial theorem for expansion of $(1+x)^n$. This proof runs as follows. Since by Kummer's theorem, the binomial coefficient $\binom{p}{k}$ is divisible by a prime p for every $k = 1, 2, \dots, p-1$, by the binomial expansion it follows that

$$(1+X)^p \equiv 1+X^p \pmod{p}.$$

Continuing by induction, we have that for every nonnegative integer i

$$(1+X)^{p^i} \equiv 1+X^{p^i} \pmod{p}.$$

Write n and m in base p , so that $n = \sum_{i=0}^s n_i$ and $m = \sum_{i=0}^s m_i$ for some nonnegative integers $s, n_0, \dots, n_s, m_0, \dots, m_s$ with $0 \leq n_i, m_i \leq p-1$ for all $i = 0, 1, \dots, s$. Then

$$\begin{aligned} \sum_{m=0}^n \binom{n}{m} X^m &= (1+X)^n = \prod_{i=0}^s \left((1+X)^{p^i} \right)^{n_i} \\ &\equiv \prod_{i=0}^s \left(1+X^{p^i} \right)^{n_i} = \prod_{i=0}^s \left(\sum_{m_i=0}^{n_i} \binom{n_i}{m_i} X^{m_i p^i} \right) \pmod{p} \\ &= \prod_{i=0}^s \left(\sum_{m_i=0}^{p-1} \binom{n_i}{m_i} X^{m_i p^i} \right) \\ &= \sum_{m=0}^n \left(\prod_{i=0}^s \binom{n_i}{m_i} \right) X^m \pmod{p}. \end{aligned}$$

By comparing the coefficients of X^m on the left hand side and on the right hand side of the above congruence immediately yields Lucas' theorem given by (1).

As an application of a counting technique due to M. Hausner in 1983 [55], in the same paper [55, Example 4] the author established another combinatorial proof of (3). Another proof of the congruence (3) based on a simple combinatorial lemma is presented in 2005 by P.G. Anderson, A.T. Benjamin and J.A. Rouse in [6, p. 268] (see also [13]). Another two proofs of Lucas' theorem, based on techniques from Elementary Number Theory were obtained in 2010 by S.-C. Liu and J.C.-C. Yeh [83] and in 2012 by A. Laugier and M.P. Saikia [82].

The congruence (3) immediately yields

$$(5) \quad \binom{np}{mp} \equiv \binom{n}{m} \pmod{p}$$

since the same products of binomial coefficients are formed on the right side of Lucas's theorem in both cases, other than an extra $\binom{0}{0} = 1$.

A direct proof of the congruence (5), based on a polynomial method, is given in [133, Solution of Problem A-5, p. 173] as follows. It is well known that $\binom{p}{i} \equiv 0 \pmod{p}$ for each $i = 1, 2, \dots, p-1$ (see (11)) or equivalently that in the ring $\mathbb{Z}_p[x]$ we have $(1+x)^p = 1+x^p$, where \mathbb{Z}_p is the field of the integers modulo p . Thus in $\mathbb{Z}_p[x]$,

$$\sum_{k=0}^{np} \binom{np}{k} x^k = (1+x)^{np} = ((1+x)^p)^n = (1+x^p)^n = \sum_{j=0}^n \binom{n}{j} x^{jp}.$$

Since coefficients of like powers must be congruent modulo p in the equality

$$\sum_{k=0}^{np} \binom{np}{k} x^k = \sum_{j=0}^n \binom{n}{j} x^{jp}$$

in $\mathbb{Z}_p[x]$, we see that

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p} \quad \text{for } m = 0, 1, \dots, n.$$

Further, notice that the Lucas' congruence (3) easily follows by induction on the sum $r+s \geq 0$ using the base induction $r+s=0$ with $r=s=0$ satisfying via the congruence (5), and the Pascal formulas:

$$\binom{np+(r+1)}{mp+s} = \binom{np+r}{mp+(s-1)} + \binom{np+r}{mp+s}$$

and

$$\binom{np+r}{mp+(s+1)} = \binom{np+(r-1)}{mp+s} + \binom{np+(r-1)}{mp+(s+1)}.$$

Remark 2. The Lucas' congruence (3) also can be interpreted as a result about cellular automata (cf. Granville [52, Section 5]). Namely, Lucas' theorem can be interpreted as a two-dimensional p -automaton (for a formal definition see [3]). \square

2.2. Some consequences and extensions of Lucas' theorem. Here, as always in the sequel, p will denote any prime.

As noticed in 2011 by A. Nowicki [103, the congruences 7.3.1–7.33], if $n = n_0 + n_1p + \dots + n_sp^s$ is the p -adic expansion of a positive integer n , then for each $k = 0, 1, \dots, s$

$$(6) \quad \binom{n}{p^k} \equiv n_k \equiv \left\lfloor \frac{n}{p^k} \right\rfloor \pmod{p},$$

holds, and consequently,

$$(7) \quad \binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p},$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x .

Remark 3. The congruence (7) is proposed by L.E. Clarke [26] in 1956 as a problem which is solved in 1957 by P.A. Piza [108]. \square

Moreover, if $0 \leq r < p^f$ and $0 \leq m < p^f$, then the Lucas' congruence (3) immediately yields (see [103, the congruence 7.3.6])

$$(8) \quad \binom{p^f + r}{m} \equiv \binom{r}{m} \pmod{p}.$$

Furthermore, if $0 \leq r < p^f$, $0 \leq m < p^f$ and $a \geq 0$, then by Lucas' theorem (see [103, the congruence 7.3.7]),

$$(9) \quad \binom{ap^f + r}{m} \equiv \binom{r}{m} \pmod{p}.$$

Moreover, if $0 \leq r < p^f$ and $p^f \leq m$, then by [103, the congruence 7.3.8],

$$(10) \quad \binom{p^f + r}{m} \equiv \binom{r}{m - p^f} \pmod{p}.$$

Lucas' theorem immediately yields the following well known congruence:

$$(11) \quad \binom{p}{k} \equiv 0 \pmod{p},$$

where p is a prime and k is an integer such that $1 \leq k \leq p - 1$.

Furthermore, if p is a prime and f a positive integer, then by Lucas' theorem for any $f \geq 1$ and $1 \leq k \leq p^f - 1$ we have (see, e.g., [13, Theorem 24])

$$(12) \quad \binom{p^f}{k} \equiv 0 \pmod{p}.$$

Further, if p is a prime and n , m and k are positive integers with $m \leq n$, then the congruence (5) by induction easily yields (see [96, Lemma 2.1])

$$(13) \quad \binom{np^k}{mp^k} \equiv \binom{n}{m} \pmod{p}.$$

An alternative version of Lucas' theorem was noticed in 1994 by J. M. Holte [60, p. 60] (also see [61, p. 227]) as follows: If

$$B(m, n) := \binom{m+n}{m} = \frac{(m+n)!}{m!n!},$$

then

$$(14) \quad B(m, n) \equiv B(m \operatorname{div} p, n \operatorname{div} p) B(m \bmod p, n \bmod p) \pmod{p},$$

where $m \operatorname{div} p$ is the integer quotient of m by p and $m \bmod p$ is the remainder of m by division by p . (similarly, for n instead of m). It follows that if $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^s$, where $0 \leq m_i, n_i \leq p-1$ for each $i = 0, 1, \dots, s$, then

$$(15) \quad B(m, n) \equiv \prod_{i=0}^s B(m_i, n_i) \pmod{p}.$$

Consequently, $p \mid B(m, n)$ if and only if $p \mid B(m_i, n_i)$ for some $i \in \{0, 1, \dots, s\}$.

Following Granville [52, Section 6], for an integer polynomial $f(X)$ of degree d , define the numbers $\binom{m}{n}_f$ with $m, n \in \mathbb{Z}$ by the generating function

$$f(X)^m = \sum_{n=0}^{md} \binom{m}{n}_f X^n,$$

and let $\binom{m}{n}_f = 0$ if $n < 0$ or $n > md$ (note that $\binom{m}{n}_f = \binom{m}{n}$ when $f(X) = X + 1$). Clearly, by Fermat little theorem, $f(X)^p \equiv f(X^p) \pmod{p}$, and using this in 1995 A. Granville [52, Section 6, the congruence (24)] proved the following generalization of the congruence (4): *If p is a prime, m, n nonnegative integers such that $m = pl + m_0$, $n = pt + n_0$, $l, t, m_0, n_0 \in \mathbb{N}$ and $0 \leq m_0, n_0 \leq p-1$, then*

$$(16) \quad \binom{m}{n}_f \equiv \sum_{k=0}^{d-1} \binom{\lfloor m/p \rfloor}{\lfloor n/p \rfloor - k}_f \binom{m_0}{n_0 + kp}_f \pmod{p}.$$

Notice that when $f(X) = X + 1$ then the congruence (16) becomes

$$\binom{m}{n} \equiv \binom{\lfloor m/p \rfloor}{\lfloor n/p \rfloor} \binom{m_0}{n_0} \pmod{p},$$

which is in fact the Lucas's congruence (3).

By using a congruence based on Burnside's theorem, in 2005, T.J. Evans [38, Theorem 3] proved the following extension of Lucas' theorem involving Euler's totient function φ : *If $n \geq 1$, m, M, m_0, r, R and r_0 are nonnegative integers such that $m = Mn + m_0$, $r = Rn + r_0$, with $0 \leq m_0, r_0 < n$, then*

$$(17) \quad \sum_{d|n} \varphi\left(\frac{n}{d}\right) \sum_{j=-(d-1)}^{d-1} \sum_{\substack{\|a\|_d= \\ R-(j/d)}} \binom{M}{a_1} \cdots \binom{M}{a_d} \binom{m_0}{r_0 + (n/d)j} \equiv 0 \pmod{n},$$

where the summation runs among all positive divisors d of n .

Remark 4. It was proved in [38, Corollary 3] that Lucas' theorem easily follows from the congruence (17). \square

3. LUCAS TYPE CONGRUENCES FOR PRIME POWERS

3.1. Wolstenholme type congruences. Notice that for any prime p the congruence (5) with $n = 2$ and $m = 1$ becomes

$$\binom{2p}{p} \equiv 2 \pmod{p},$$

whence by the identity $\binom{2p}{p} = 2\binom{2p-1}{p-1}$ it follows that for any prime p

$$(18) \quad \binom{2p-1}{p-1} \equiv 1 \pmod{p}.$$

As noticed in 1, in 1819 Charles Babbage [9] (also see [52, Introduction] or [36, page 271]) showed that the congruence (18) holds modulo p^2 , that is, for a prime $p \geq 3$ holds

$$(19) \quad \binom{2p-1}{p-1} \equiv 1 \pmod{p^2}.$$

Remark 5. A combinatorial proof of the congruence (19) can be found in [126, Exercise 14(c) on page 118]. \square

The congruence (19) was generalized in 1862 by Joseph Wolstenholme [142] as it is presented in the next section. Namely, *Wolstenholme's theorem* asserts that

$$(20) \quad \binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$$

for all primes $p \geq 5$.

For a survey of Wolstenholme's theorem see [93] and for its extensions see [146] and [100].

By Glaisher's congruence [49, p. 323] (also see [93, Section 6]), for any positive integer n and a prime $p \geq 5$ holds

$$\binom{np-1}{p-1} \equiv 1 \pmod{p^3},$$

which by the identity $\binom{np}{p} = n\binom{np-1}{p-1}$ yields [103, the congruence 7.1.5]

$$(21) \quad \binom{np}{p} \equiv n \pmod{p^3}.$$

In 1949 W. Ljunggren [19] generalized the congruence (21) as follows (also see [10, Theorem 4], [52] and [126, Problem 1.6 (d)], and for a simple

proof see [123]): if $p \geq 5$ is a prime, n and m are positive integers with $m \leq n$, then

$$(22) \quad \binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}.$$

Remark 6. Ljunggren's congruence (22) is refined modulo p^5 in 2007 by J. Zhao [145, Theorem 3.5]. \square

Remark 7. Note that the congruence (22) with $m = 1$ and $n = 2$ reduces to the Wolstenholme's congruence (20). \square

Further, the congruence (22) is refined in 1952 by E. Jacobsthal [19] (also see [52]) as follows: if $p \geq 5$ is a prime, n and m are positive integers with $m \leq n$, then

$$(23) \quad \binom{np}{mp} \equiv \binom{n}{m} \pmod{p^t},$$

where t is the power of p dividing $p^3nm(n-m)$ (this exponent t can only be increased if p divides B_{p-3} , the $(p-3)$ rd Bernoulli number).

Remark 8. In the literature, the congruence (23) is often called *Jacobsthal-Kazandzidis congruence* (see e.g., [27, Section 11.6, p. 380]). \square

In 2008 C. Helou and G. Terjanian [56, the congruence (1) of Corollary on page 490] refined the Jacobsthal's result as follows (also see [27, Section 11.6, Corollary 11.6.22, p. 381] for a stronger form): If $p \geq 5$ is a prime, n and m are positive integers with $m \leq n$, then

$$(24) \quad \binom{np}{mp} \equiv \binom{n}{m} \pmod{p^t},$$

where t is the power of p dividing $p^3m(n-m)\binom{n}{m}$.

By a problem N4 of Short list of 48th IMO 2006 [35], for every integer $k \geq 2$, 2^{3k} divides the number

$$(25) \quad \binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$$

but 2^{3k+1} does not.

3.2. Variations of Lucas' theorem modulo prime powers. In 1991 D.F. Bailey [11, Theorem 4] proved that if p is a prime, n and r are nonnegative integers and s a positive integer less than p , then

$$(26) \quad \binom{np}{rp+s} \equiv (r+1) \binom{n}{r+1} \binom{p}{s} \pmod{p^2}.$$

In the same paper [11, Theorem 5], the author extended the previous congruence as follows: *if $p \geq 5$ is a prime, $0 \leq m \leq n$, $0 \leq r < p$ and $1 \leq s < p$, then*

$$(27) \quad \binom{np^2}{mp^2 + rp + s} \equiv (m+1) \binom{n}{m+1} \binom{p^2}{rp + s} \pmod{p^3}.$$

Remark 9. Notice that Bailey's proof of the congruence (27) (proof of Theorem 5 in [10]) is deduced applying the Ljunggren's congruence (22) (Theorem 4 in [10]) and a counting technique of M. Hausner from [55]. \square

In 1992 D.F. Bailey [12, Theorem 2.1] generalized his congruence (27) modulo any prime power as follows: *if $p \geq 5$ is a prime, $0 \leq m \leq n$, $s \geq 1$, and a_0, a_1, \dots, a_{s-1} are nonnegative integers such that $1 \leq a_0 < p$ and $0 \leq a_k < p$ for every $k = 1, 2, \dots, s-1$, then*

$$(28) \quad \binom{np^s}{mp^s + a_{s-1}p^{s-1} + \dots + a_1p + a_0} \equiv (m+1) \binom{n}{m+1} \binom{p^s}{a_{s-1}p^{s-1} + \dots + a_1p + a_0} \pmod{p^{s+1}}.$$

Remark 10. If we put $a = a_{s-1}p^{s-1} + \dots + a_1p + a_0$, then the congruence (28) can be written as

$$(29) \quad \binom{np^s}{mp^s + a} \equiv (m+1) \binom{n}{m+1} \binom{p^s}{a} \pmod{p^{s+1}},$$

where a is a positive integer less than p^s which is not divisible by p . \square

Using a multiple application of Lucas' theorem, in 2012 the author of this article [98, Theorem 1.1] proved the following similar congruence to (29):

$$(30) \quad \binom{np^s}{mp^s + a} \equiv (-1)^{a-1} a^{-1} (m+1) \binom{n}{m+1} p^s \pmod{p^{s+1}},$$

where p is a prime, n, m, s and a are nonnegative integers such that $n \geq m$, $s \geq 1$, $1 \leq a \leq p^s - 1$, and a is not divisible by p .

Remark 11. The congruence (29) is an immediate consequence of the congruence (30) (see [98, Corollary 1.2 and its proof]). \square

In 1990 D.F. Bailey [10, Theorem 3] (cf. [97, Theorem with $k = 2$]) proved the following result: *If p is a prime, n, m, n_0 and m_0 are nonnegative integers, and n_0 and m_0 are both less than p , then*

$$(31) \quad \binom{np^2 + n_0}{mp^2 + m_0} \equiv \binom{n}{m} \binom{n_0}{m_0} \pmod{p^2}.$$

Furthermore, in the same paper Bailey [10, Theorem 5] (cf. [97, Theorem with $k = 3$]) extended the above result as follows: *If p is a prime greater*

than 3 and n, m, n_0 and m_0 are nonnegative integers such that n_0 and m_0 are less than p , then

$$(32) \quad \binom{np^3 + n_0}{mp^3 + m_0} \equiv \binom{n}{m} \binom{n_0}{m_0} \pmod{p^3}.$$

Kummer's theorem given in Section 1, is useful in situations where the binomial coefficient is divisible by a prime power. However, if the binomial coefficient is not congruent to zero modulo a prime, then the question remains for a way to simplify the expression. In 1995 A. Granville [52, Theorem 1] generalized Anton's congruence (4) modulo prime powers as follows. *For a given integer k define $(k!)_p$ to be the product of all integers less than or equal to k , which are not divisible by p . Suppose that prime power p^f and positive integers n and m are given with $r := n - m \geq 0$. Write $n = n_0 + n_1p + \cdots + n_sp^s$ in base p , and let N_j be the least positive residue of $\lfloor n/p^j \rfloor \pmod{p^f}$ for each $j \geq 0$ (so that $N_j = n_j + n_{j+1}p + \cdots + n_{j+f-1}p^{f-1}$); also make the corresponding definitions for m_j, M_j, r_j, R_j . Let e_j be the number of indices $i \geq j$ for which $n_i < m_i$ (that is, the number of "carries" when adding m and r in base p , on or beyond the j th digit). Then*

$$(33) \quad \frac{1}{p^{e_0}} \binom{n}{m} \equiv (\pm 1)^{e_{f-1}} \frac{(N_0!)_p}{(M_0!)_p (R_0!)_p} \cdot \frac{(N_1!)_p}{(M_1!)_p (R_1!)_p} \cdots \frac{(N_s!)_p}{(M_s!)_p (R_s!)_p} \pmod{p^f},$$

where (± 1) is (-1) except if $p = 2$ and $f \geq 3$.

Here, as usually in the sequel, we will consider the congruence relation modulo a prime power p^l extended to the ring of rational numbers with denominators not divisible by p . For such fractions we put $m/n \equiv r/s \pmod{p^l}$ if and only if $ms \equiv nr \pmod{p^l}$, and the residue class of m/n is the residue class of mn' where n' is the inverse of n modulo p^l .

A result which gives readily an extension of Lucas' theorem in the form of the congruence to prime power moduli is given in 1992 by A. Granville [51, Proposition 2] as follows: *For each positive integer j , define n_j to be the least nonnegative residue of an integer n modulo p^j . If p is a prime that does not divide $\binom{n}{m}$, then*

$$(34) \quad \binom{n}{m} \equiv \binom{\lfloor n/p \rfloor}{\lfloor m/p \rfloor} \binom{n_f}{m_f} \bigg/ \binom{\lfloor n_f/p \rfloor}{\lfloor m_f/p \rfloor} \pmod{p^f},$$

for any positive integer f .

In particular, if $\binom{n}{m}$ is not divisible by p and $m \equiv n \pmod{p^f}$, then by (34) (also see [103, the congruence 7.1.16])

$$(35) \quad \binom{n}{m} \equiv \binom{\lfloor n/p \rfloor}{\lfloor m/p \rfloor} \pmod{p^f}.$$

As observed in 1998 by D. Berend and J.E. Harmse [15, p. 34, congruence (2.2)], if a prime p does not divide $\binom{n}{m}$ and $n = n_0 + n_1p + \dots + n_sp^s$, $m = m_0 + m_1p + \dots + m_sp^s$ are the p -adic expansions of n and m , then iterating the congruence (34), we find that

$$(36) \quad \binom{n}{m} \equiv \frac{P}{Q} \pmod{p^f},$$

where

$$P = \prod_{i=0}^{k-f+1} \binom{n_i + n_{i+1}p + \dots + n_{i+f-1}p^{f-1}}{m_i + m_{i+1}p + \dots + m_{i+f-1}p^{f-1}}$$

and

$$Q = \prod_{i=1}^{k-f+1} \binom{n_i + n_{i+1}p + \dots + n_{i+f-2}p^{f-2}}{m_i + m_{i+1}p + \dots + m_{i+f-2}p^{f-2}}.$$

The congruence (36) was established in 1991 independently by K. Davis and W. Webb [29, Theorem 3] (also see [85, p. 88, Theorem 5.1.2]), which is there formulated as follows: If $n = n_0 + n_1p + \dots + n_sp^s$, $m = m_0 + m_1p + \dots + m_sp^s$ are the p -adic expansions of n and m , and $l < s$, then

$$(37) \quad \begin{aligned} \binom{n}{m} &\equiv \binom{n_0 + n_1p + \dots + n_{s-1}p^{s-1} + n_sp^s}{m_0 + m_1p + \dots + m_{s-1}p^{s-1} + m_sp^s} \\ &\equiv \frac{\binom{n_{s-l} + \dots + n_sp^{s-l}}{m_{s-l} + \dots + m_sp^{s-l}} \dots \binom{n_0 + \dots + n_lp^{s-l}}{m_0 + \dots + m_lp^{s-l}}}{\binom{n_{s-l+1} + \dots + n_{s-1}p^{s-l-1}}{m_{s-l+1} + \dots + m_{s-1}p^{s-l-1}} \dots \binom{n_0 + \dots + n_{l-1}p^{s-l-1}}{m_0 + \dots + m_{l-1}p^{s-l-1}}} \pmod{p^l}. \end{aligned}$$

If $a = a_0 + a_1p + \dots + a_{k-1}p^{k-1} + a_kp^k$ and $b = b_0 + b_1p + \dots + b_{k-1}p^{k-1} + b_kp^k$ are the p -adic expansions of a and b such that $b_k > a_k$, then we define

$$\binom{a_0 + a_1p + \dots + a_{k-1}p^{k-1} + a_kp^k}{b_0 + b_1p + \dots + b_{k-1}p^{k-1} + b_kp^k} = p \binom{a_0 + a_1p + \dots + a_{k-1}p^{k-1}}{b_0 + b_1p + \dots + b_{k-1}p^{k-1}}.$$

Remark 12. For help in understanding the above result concerning the congruence (37), we offer the following example [85, p. 88]:

$$\begin{aligned} \binom{386}{154} &= \binom{3 \cdot 11^2 + 2 \cdot 11 + 1}{11^2 + 3 \cdot 11} \equiv \frac{\binom{3 \cdot 11 + 2}{11+3} \binom{2 \cdot 11 + 1}{3 \cdot 11}}{\binom{2}{3}} \pmod{11^2} \\ &\equiv \binom{3 \cdot 11 + 2}{11+3} \binom{1}{0} \equiv \binom{35}{14} \pmod{11^2}. \quad \square \end{aligned}$$

In 2005 A.D. Loveless [85, p. 88] noticed that the above result concerning the congruence (37) can be used to simplify general classes of congruences modulo prime powers involving binomial coefficients. In particular,

Loveless [85, p. 88, Theorem 5.1.3]) proved that *if p is a prime, s and n are positive integers with $n \leq p^s$, then*

$$(38) \quad \binom{p^s}{n} \equiv \begin{cases} 0 & (\text{mod } p^s) \quad \text{if } n \not\equiv 0 \pmod{p} \\ \binom{p^{s-1}}{n/p} & (\text{mod } p^s) \quad \text{if } p \mid n. \end{cases}$$

A similar result was earlier directly proved in 1980 by P.W. Haggard and J.O. Kiltinen [54, p. 398, Theorem]. This result asserts that *if p is a prime, l and f are positive integers with $f \geq l - 1$ and $0 \leq n \leq p^f$, then*

$$(39) \quad \binom{p^f}{n} \equiv \begin{cases} 0 & (\text{mod } p^l) \quad \text{if } n \not\equiv 0 \pmod{p^{f-l+1}} \\ \binom{p^{l-1}}{i} & (\text{mod } p^l) \quad \text{if } n = i \cdot p^{f-l+1}. \end{cases}$$

Using the congruence (37), in 1993 K. Davis and W. Webb [30] generalized Bailey's results concerning the congruences (31) and (32) for any modulus p^k with $p \geq 5$ and $k \geq 1$. They proved [30, Theorem 3] that *if p is any prime, k, n, m, a, b and s are positive integers such that $0 < a, b < p^s$, then*

$$(40) \quad \binom{np^{k+s} + a}{mp^{k+s} + b} \equiv \binom{np^k}{mp^k} \binom{a}{b} \pmod{p^{k+1}}.$$

Remark 13. Notice that under the same assumption preceding the congruence (40), and if $\binom{np^{k+s} + a}{mp^{k+s}} \not\equiv 0 \pmod{p}$, then the congruence (40) can be obtained by iterating s times the Granville's congruence (34). Notice also that the condition $\binom{np^{k+s} + a}{mp^{k+s}} \not\equiv 0 \pmod{p}$ is by Lucas' theorem equivalent to the following two conditions: $\binom{n}{m} \not\equiv 0 \pmod{p}$ and $\binom{a}{b} \not\equiv 0 \pmod{p}$. \square

Further, by repeated application of the congruence (40), and using Ljunggren's congruence (22), we find that *under the same assumptions preceding the congruence (40) [30, Corollary 1] for any prime $p > 3$,*

$$(41) \quad \binom{np^{k+s} + a}{mp^{k+s} + b} \equiv \binom{np^{\lfloor k/3 \rfloor}}{mp^{\lfloor k/3 \rfloor}} \binom{a}{b} \pmod{p^{k+1}}.$$

In particular, the congruence (41) with $s = 1$ and $k - 1 \geq 0$ instead of k implies that *for each prime $p \geq 5$ and for all integers $k \geq 1$, $n \geq 0$, a and b with $0 \leq a, b < p$*

$$(42) \quad \binom{np^k + a}{mp^k + b} \equiv \binom{np^{\lfloor (k-1)/3 \rfloor}}{mp^{\lfloor (k-1)/3 \rfloor}} \binom{a}{b} \pmod{p^k}.$$

Furthermore, *the congruence (42) with $\lfloor k/2 \rfloor$ instead of $\lfloor (k-1)/3 \rfloor$ is satisfied for $p = 2$, and the congruence (42) with $\lfloor (k-1)/2 \rfloor$ instead of $\lfloor (k-1)/3 \rfloor$ is also satisfied for $p = 3$.*

Remark 14. As noticed above, a proof of the congruence (41) given by Davis and Webb is based on their earlier result from [29] given by the congruence (41). However, this result together with related proof is slightly more complicated. In 2012 the author of this article [97, Theorem] gave a simple induction proof of the congruence (42) which uses only the usual properties of binomial coefficients. \square

Adapting Fine's method [39], in 1988 R.A. Macleod [88, Theorem 2] proved the following variation of Lucas' theorem: *Let p be a prime, let r be a positive integer, and let*

$$M = \sum_{i=0}^k M_i p^{ir}, \quad \text{with } 0 \leq M_i < p^r \quad \text{for all } i = 0, 1, \dots, k.$$

Then for every nonnegative integer N such that $0 \leq N \leq M$

$$(43) \quad \binom{M}{N} \equiv \sum \binom{p^{r-1}M_0}{N_0} \binom{p^{r-1}M_1}{N_1} \cdots \binom{p^{r-1}M_k}{N_k} \pmod{p^r},$$

where the summation ranges over all $k+1$ -tuples (N_0, N_1, \dots, N_k) such that

$$p^{r-1}N = \sum_{i=0}^k N_i p^{ir}, \quad \text{with } 0 \leq N_i < p^{r-1}M_i \quad \text{for all } i = 0, 1, \dots, k.$$

Quite recently, in 2014 E. Rowland and R. Yassawi [115, Section 5, Theorem 5.3] established a new generalization of Lucas' theorem to prime powers as follows: *Let p be a prime, let f be a positive integer and let $D = \{0, 1, \dots, p^f - p^{f-1}\}$. If $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^s$ are the p -adic expansions of nonnegative integers n and m , then*

$$(44) \quad \binom{n}{m} \equiv \sum_{\substack{(i_0, \dots, i_l) \in D^{l+1} \\ (j_0, \dots, j_l) \in D^{l+1}}} (-1)^{n-i+\sum_{h=0}^l i_h} \binom{p^{f-1}-1}{n-i} \binom{n-i}{m-j} \\ \times \prod_{h=0}^l \binom{p^f - p^{f-1}}{i_h} \binom{i_h}{j_h} \pmod{p^f},$$

where $i = \sum_{h=0}^l i_h p^h$ and $j = \sum_{h=0}^l j_h p^h$.

Remark 15. Note that $i = \sum_{h=0}^l i_h p^h$ and $j = \sum_{h=0}^l j_h p^h$ are representations of integers i and j in base p with an enlarged digit set D rather than the standard digit set $\{0, 1, \dots, p-1\}$. \square

Remark 16. E. Rowland and R. Yassawi [115, Section 5] showed that a broad range of multidimensional sequences possess "Lucas products" modulo a prime p . Furthermore, in 2009 K. Samol and D. van Straten

[117, Proposition 4.1] established the Lucas type congruence for a sequence whose terms are constant terms of $P(x)^n$ for certain Laurent polynomials $P(x)$. \square

3.3. Characterizations of Wolstenholme primes. A prime p is said to be a *Wolstenholme prime* if it satisfies the congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4},$$

or equivalently,

$$(45) \quad \binom{2p}{p} \equiv 2 \pmod{p^4}.$$

The two known such primes are 16843 and 2124679, and R.J. McIntosh and E.L. Roettger reported in [91] that these primes are only two Wolstenholme primes less than 10^9 . However, McIntosh in [90] conjectured that there are infinitely many Wolstenholme primes (for more information see [94]). By the well known result of J.W.L. Glaisher in 1900 [49, p. 323] (also see [95, the congruence (1.2)]),

$$(46) \quad \binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}p^3 B_{p-3} \pmod{p^4},$$

where B_k ($k = 0, 1, 2, \dots$) are Bernoulli numbers defined by the generating function [71]

$$\sum_{k=0}^{\infty} B_k \frac{x^k}{k!} = \frac{x}{e^x - 1}.$$

The congruence (46) shows that a prime p is a Wolstenholme prime if and only if p divides the numerator of B_{p-3} , the $(p-3)$ rd Bernoulli number.

As an application of the congruences (42) with $k = 4$ and Jacobsthal's congruence (23), we can obtain the following characterization of Wolstenholme primes given in 2012 by the author of this article [97, Proposition]: *The following statements about a prime $p \geq 5$ are equivalent.*

- (i) p is a Wolstenholme prime;
- (ii) for all nonnegative integers n and m the congruence

$$(47) \quad \binom{np}{mp} \equiv \binom{n}{m} \pmod{p^4}$$

holds;

- (iii) for all nonnegative integers n, m, n_0 and m_0 such that n_0 and m_0 are less than p ,

$$(48) \quad \binom{np^4 + n_0}{mp^4 + m_0} \equiv \binom{n}{m} \binom{n_0}{m_0} \pmod{p^4}.$$

4. THE LUCAS PROPERTY AND THE p -LUCAS PROPERTY

4.1. The Lucas property and the double Lucas property. In 1992 R.J. McIntosh [89] proposed the following definition:

Definition. The integer sequence $(a_n)_{n \geq 0}$ has the *Lucas property* if $a_0 = 1$, and for every prime p , every $n \geq 0$, and every $j \in \{0, 1, \dots, p-1\}$ the congruence

$$(49) \quad a_{pn+j} \equiv a_n a_j \pmod{p}$$

holds. \square

Remark 17. (cf. [1, p. 152, Remark 6.1]). Taking $n = j = 0$ in the congruence (49) gives $a_0 \equiv a_0^2 \pmod{p}$. This yields that either $a_0 \equiv 0 \pmod{p}$ or $a_0 \equiv 1 \pmod{p}$. In the first case, taking $n = 0$ and $j \in \{0, 1, \dots, p-1\}$ gives $a_j \equiv 0 \pmod{p}$; hence $a_{pn+j} \equiv a_n a_j \equiv 0 \pmod{p}$ for all n 's and j 's. This means that a_n is a zero sequence modulo p . What precedes implies that such a sequence either satisfies $a_n = 0$ for all $n \geq 0$ or $a_0 = 1$. \square

An analogous definition of double Lucas property is given also by McIntosh [89] as follows:

Definition. The function $L : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$ has the *double Lucas property* if $L(n, m) = 0$ for all $n < m$, and for every prime p , every $n, m \geq 0$, and every r, s with $0 \leq r, s \leq p-1$ the congruence

$$(50) \quad L(np + r, mp + s) \equiv L(n, m)L(r, s) \pmod{p}$$

holds. \square

Notice that Lucas' theorem (the congruence (3)) and the congruence (14) show that both functions $C(n, m), B(n, m) : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$ defined as $C(n, m) = \binom{n}{m}$ and $B(n, m) = \binom{n+m}{m}$ have the double Lucas property. McIntosh [89] presents various properties of the function $L(n, k)$ and their connection with the Lucas property. A typical result is as follows: *If $L(n, m)$ has the double Lucas property, then the function $F(n) = \sum_{m=0}^n L(n, m)$ has the Lucas property.*

In 1999 J.-P. Allouche [1, Proposition 7.1] proved the following result: *Let m be a positive integer; let $e_1 = 2, e_2, \dots, e_m$ be integers such that $e_j \leq e_{j+1} \leq 2e_j$ for $j = 1, 2, \dots, m-1$, and let r_1, r_2, \dots, r_m be positive integers. Then the sequence $(u_n)_{n \geq 0}$ defined by*

$$(51) \quad u_n = \binom{2n}{n}^{r_1} \binom{e_2 n}{2n}^{r_2} \binom{e_3 n}{e_2 n}^{r_3} \cdots \binom{e_m n}{e_{m-1} n}^{r_m}$$

has the Lucas property.

In particular, if $e_{j+1} - e_j = 1$ for all $j = 1, 2, \dots, m-1$, and r_1, r_2, \dots, r_m are positive integers, then the above result implies that the sequence $(u_n)_{n \geq 0}$

defined as

$$u_n = \binom{2n}{n}^{r_1} \binom{3n}{n}^{r_2} \cdots \binom{(m+1)n}{n}^{r_m}$$

has the Lucas property (see [89]).

The Apéry numbers $A_1(n)$ and $A_2(n)$ defined as

$$A_1(n) = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2, A_2(n) = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}, \quad n = 0, 1, \dots,$$

arose in Apéry's proof in 1979 of the irrationality of $\zeta(3)$ [8]. $(A_1(n))_{n \geq 0}$ and $(A_2(n))_{n \geq 0}$ are Sloane's sequences A005259 and A005258 in [124], respectively.

The Apéry numbers modulo a prime were studied in 1982 by I. Gessel who proved [47, Theorem 1] the following result: *If $n = n_0 + n_1p + \cdots + n_sp^s$ is the p -adic expansion of n , then*

$$(52) \quad A_1(n) \equiv \prod_{i=0}^s A_1(n_i) \pmod{p}.$$

In other words, the sequence $(A_1(n))_{n \geq 1}$ has the Lucas property.

Similarly, the sequence $(A_2(n))_{n \geq 0}$ satisfies the Lucas property (see [31]).

In 2008 Y. Jin, Z-J. Lu and A.L. Schmidt [72, (ii) of Lemma 2] proved that the sums of powers of binomial coefficients have the Lucas property, that is: *For a positive integer s , let $(a_n^{(s)})_{n \geq 0}$ be a sequence defined as*

$$a_n^{(s)} = \sum_{k=0}^n \binom{n}{k}^s, \quad n = 0, 1, 2, \dots$$

Then for every prime p , every $n \geq 0$, and every $j \in \{0, 1, \dots, p-1\}$ the congruence

$$(53) \quad a_{pn+j}^{(s)} \equiv a_n^{(s)} a_j^{(s)} \pmod{p}$$

holds.

Remark 18. The above result implies that the residues of Pascal's triangle modulo p have a self-similar structure (see, e.g., [42], [52, Section 5] and [141]). \square

For a prime p and a positive integer k , in 1994 M. Razpet [111] considered the $p^k \times p^k$ matrix $A(k, p) = [a_{i,j}(k, p)]_{0 \leq i, j \leq p^k-1}^{0 \leq j \leq p^k-1}$, whose the entry $a_{i,j}(k, p)$ is defined as the remainder of the division of $\binom{i}{j}$ by p . In particular, for $k = 1$ we write $A(p) = A(1, p) = [a_{i,j}(p)]_{0 \leq i, j \leq p-1}^{0 \leq j \leq p-1}$. M. Razpet [111] noticed that for every $k \geq 1$ and every prime p , the matrix $A(k, p)$ is the k -fold tensor (or Kronecker) product of the matrix $A(p)$ by itself in the

field \mathbb{Z}_p , that is, $A(k, p) = \underbrace{A(p) \otimes A(p) \cdots \otimes A(p)}_k = A(p)^{\otimes k}$. Note that matrix indices start at index pair $(0, 0)$. This is an algebraic and “square” representation of the oft-noted self-similarity structure of Pascal’s triangle (see, e.g., [58] and [141]).

Furthermore, as noticed in [111, p. 378], by Lucas’ theorem we have

$$(54) \quad a_{i,j}(k, p) \equiv a_{i_0,j_0}(p) a_{i_1,j_1}(p) \cdots a_{i_{k-1},j_{k-1}}(p) \pmod{p},$$

where $0 \leq i, j \leq p^k - 1$, $i = i_0 + i_1p + \cdots + i_{k-1}p^{k-1}$ and $j = j_0 + j_1p + \cdots + j_{k-1}p^{k-1}$ with $0 \leq i_l, j_l \leq p - 1$ for all $l = 0, 1, \dots, k - 1$.

Remark 19. In [109] M. Prunescu pointed out that Pascal’s triangle modulo p^k is not a limit of tensor powers of matrices if $k \geq 2$. However, Pascal’s triangle modulo p^k are p -automatic, and consequently can be produced by matrix substitution and are projections of double sequences produced by two-dimensional morphisms (see [4]). \square

In 2003 D. Berend and N. Kriger [14, Theorem 5] proved that *there exist uncountably many infinite matrices $A = [a_{i,j}]_{m,n=0}^\infty$ satisfying the double Lucas property, that is the congruences*

$$(55) \quad a_{m,n} \equiv \prod_{i=0}^k a_{m_i,n_i} \pmod{p}$$

are satisfied for every prime p and all nonnegative integers m and n with p -adic expansions $m = \sum_{i=0}^k m_i p^i$ and $n = \sum_{i=0}^k n_i p^i$.

In 1998 N.J. Calkin [21] investigated divisibility properties for sums of powers of binomial coefficients $f_{n,a}$ defined as

$$f_{n,a} = \sum_{k=0}^n \binom{n}{k}^a,$$

where n and a are nonnegative integers. Then $f_{n,0} = n + 1$, $f_{n,1} = 2^n$ and $f_{n,2} = \binom{2n}{n}$. The sequences $(f_{n,a})_{n \geq 0}$ for $a = 3, 4, 5, 6$ are Sloane’s sequences A000172 (Franel numbers), A005260, A005261, A069865 in [124], respectively. Calkin [21, Lemma 4] proved that *for every positive integer a , the sequence $(f_{n,a})_{n \geq 0}$ has the Lucas property. This means that if p is a prime and if $n = n_0 + n_1p + \cdots + n_s p^s$ is the p -adic expansion of n , then*

$$(56) \quad f_{n,a} \equiv \prod_{i=0}^s f_{n_i,a} \pmod{p}.$$

Calkin [21, p. 21] also noticed that *for any $a \in \{1, 2, \dots\}$ the sequence $(h_{n,a})_{n \geq 0}$ defined as*

$$h_{n,a} = \sum_{k=0}^n (-1)^k \binom{2n}{k}^a,$$

also has the Lucas property.

For a positive integer n the central trinomial coefficient T_n is the largest coefficient in the expansion $(1 + x + x^2)^n$ (Sloane's sequence A002426 in [124]). It is easy to express T_n in terms of trinomial coefficients as

$$T_n = \sum_{k \geq 0} \binom{n}{k, k, n-2k},$$

where we use the convention that if any multinomial coefficient has a negative number on the bottom then the coefficient is zero. In 2006 E. Deutsch and B.E. Sagan [33] proved that the sequence $(T_n)_{n \geq 0}$ has the Lucas property. Namely, by [33, Theorem 4.7] if p is a prime and $n = n_0 + n_1p + \dots + n_sp^s$ is a positive integer with $0 \leq n_i \leq p-1$ for all $i = 0, 1, \dots, s$, then

$$(57) \quad T_n \equiv \prod_{i=0}^s T_{n_i} \pmod{p}.$$

Furthermore, E. Deutsch and B.E. Sagan [33, Theorem 4.4] proved the following result for central binomial coefficients $\binom{2n}{n}$ (Sloane's sequence A000984 in [124]): *Let p be a prime and let $n = n_0 + n_1p + \dots + n_sp^s$ be a positive integer with $0 \leq n_i \leq p-1$ for all $i = 0, 1, \dots, s$. For every $j \in \{0, 1, \dots, p-1\}$ let $\delta_{p,j}(n)$ be the number of elements of the set $\{n_0, n_1, \dots, n_s\}$ equal to j . Then*

$$(58) \quad \binom{2n}{n} \equiv \begin{cases} \prod_j \binom{2j}{j}^{\delta_{p,j}(n)} \pmod{p} & \text{if } n_i \leq p/2 \text{ for all } i = 0, 1, \dots, s, \\ 0 \pmod{p} & \text{otherwise,} \end{cases},$$

where the summation ranges over all $j \in \{0, 1, \dots, p-1\}$ such that $\delta_{p,j}(n) > 0$.

In 2009 M. Chamberland and K. Dilcher [25] studied the divisibility properties of the sums $u(n)$ defined as

$$u(n) = \sum_{k=0}^n (-1)^k \binom{n}{k} \binom{2n}{k}, \quad n = 0, 1, 2, \dots$$

Under this notation, the authors proved [25, Theorem 2.2] *that for every prime $p \geq 3$ and all integers $m \geq 0$ and r such that $0 \leq r \leq (p-1)/2$ we*

have

$$(59) \quad u(mp + r) \equiv u(m)u(r) \pmod{p}.$$

As an application, the authors proved [25, Corollary 2.1] that *for every prime $p \geq 3$ and every integer $n = n_0 + n_1p + \cdots + n_sp^s$ with $0 \leq n_i \leq (p-1)/2$ for each $i = 0, 1, \dots, s$, we have*

$$(60) \quad u(n) \equiv u(n_0)u(n_1) \cdots u(n_s) \pmod{p}.$$

Similarly, if the sums $w(n)$ are defined as

$$w(n) = \sum_{k=0}^{n-1} (-1)^k \binom{2n-1}{k} \binom{n-1}{k}, \quad n = 0, 1, 2, \dots,$$

then by [25, Corollary 2.2], *for all primes $p \geq 3$ and positive integers m and r with $(p+1)/2 \leq r \leq p-1$*

$$(61) \quad u(mp + r) \equiv w(m+1)u(r) \pmod{p}.$$

Remark 20. We point out that the Lucas property holds for a general family of sequences considered in 2006 by T.D. Noe [102]. \square

For all nonnegative integers i and j let $w(i, j|a, b, c)$ denote the number of all paths in the plane from $(0, 0)$ to (i, j) with steps $(1, 0)$, $(0, 1)$, $(1, 1)$, and with positive integer weights a, b, c , respectively. The explicit formula for $w(i, j|a, b, c)$ was obtained by several authors by using combinatorial arguments (see, e.g., [43]):

$$w(i, j|a, b, c) = \sum_{k \geq 0} \binom{k}{i} \binom{i}{k-j} a^{k-j} b^{k-i} c^{i+j-k}.$$

Actually, k in the above sum runs from $\max\{i, j\}$ to $i+j$. In the case $a = b = c = 1$, we have even the *Delannoy numbers* which count the usual, unweighted lattice paths from the point $(0, 0)$ to the point (i, j) with steps along the vectors $(1, 0)$, $(0, 1)$ and $(1, 1)$. If $i = j = n$, then the numbers $w(n, n|1, 1, 1)$, $n = 0, 1, 2, \dots$ are called the *central Delannoy numbers* (Sloane's sequence A001850 in [124]).

In 2002 M. Razpet [112, Theorem 1] proved the following double Lucas property of $w(i, j|a, b, c)$: *Let p be a prime and let $\alpha, \beta, \gamma, \delta$ be nonnegative integers where $0 \leq \beta < p$ and $0 \leq \delta < p$. Then the congruence*

$$(62) \quad w(\alpha p + \beta, \gamma p + \delta|a, b, c) \equiv w(\alpha, \gamma|a, b, c)w(\beta, \delta|a, b, c) \pmod{p}$$

holds for all positive integers a, b, c .

Remark 21. Razpet [112] notice that the congruence (62) is particularly true for the *Delannoy numbers* $D(i, j) := w(i, j|1, 1, 1)$ as proven in another way in 1990 by M. Razpet [110] and by M. Sved and R.J. Clarke [132] (see also [33] and [37]). \square

In 2004 H. Pan [106, Theorem 1] proved the following result: *Suppose $\lambda(x_1, \dots, x_n) = \sum_{\Phi \neq I \subseteq \{1, \dots, n\}} \alpha_I \prod_{i \in I} X_i$, $\alpha_I \in \mathbb{F}$, is a polynomial over the finite field \mathbb{F} with q elements. Let $w_\lambda(k_1, \dots, k_n)$ be the coefficient of $\prod_{i=1}^n X_i^{k_i}$ in the formal power series $\frac{1}{1-\lambda(x_1, \dots, x_n)}$. Then w_λ satisfies the double Lucas property, i.e., for any nonnegative integers a_1, \dots, a_n and $0 \leq b_1, \dots, b_n < q$,*

$$(63) \quad w_\lambda(a_1q + b_1, \dots, a_nq + b_n) = w_\lambda(a_1, \dots, a_n)w_\lambda(b_1, \dots, b_n).$$

Remark 22. If p is a prime and \mathbb{F} is the field $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, then the equality “=” in (63) becomes $\equiv 0 \pmod{p}$. \square

4.2. Further Lucas type congruences. For nonnegative integers n and k Stirling numbers of the second kind $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ (Sloane's sequence A008277 in [124]) are recursively defined as:

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \begin{cases} 1 & \text{if } n = 0, k = 0, \\ 0 & \text{if } n > 0, k = 0, \\ 0 & \text{if } n = 0, k > 0, \\ k \left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\} & \text{if } n > 0, k > 0. \end{cases}$$

$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ presents the number of ways of partitioning a set of n elements into k nonempty sets (i.e., k set blocks). They (as well as Stirling numbers of the first kind defined below) are named after James Stirling, who introduced them in 1730 [127].

In 1988 M. Sved [131, p. 61, Theorem] showed the following result: *Let n and m be nonnegative integers, and let p be an odd prime such that p does not divide m . Put*

$$n' = \left\lfloor \frac{pn - p \lfloor m/p \rfloor - 1}{p-1} \right\rfloor,$$

and let $n' = \sum_{i=0}^h n'_i p^i$ and $m = \sum_{i=0}^h m_i p^i$ be the expansions of n' and m to base p . Then

$$(64) \quad \left\{ \begin{smallmatrix} n \\ m \end{smallmatrix} \right\} \equiv \left\{ \begin{smallmatrix} n'_0 \\ m_0 \end{smallmatrix} \right\} \prod_{j=1}^h \binom{n'_j}{m_j}.$$

In 2000 R. Sánchez-Peregrino [118, Proposition 3.1] proved that *if n, m, r and s are nonnegative integers such that $0 \leq s \leq r \leq p-1$ and $m \leq n \leq p-1$, then*

$$(65) \quad \left\{ \begin{smallmatrix} np+r \\ mp+s \end{smallmatrix} \right\} \equiv \left\{ \begin{smallmatrix} n-m+r \\ s \end{smallmatrix} \right\} \binom{n}{m} + \left\{ \begin{smallmatrix} n-m+r+1 \\ s+p \end{smallmatrix} \right\} \binom{n}{m-1} \pmod{p}.$$

Notice also that under the hypothesis that $r + n - m + 1 < s + p$, the congruence (65) reduces to

$$(66) \quad \left\{ \begin{matrix} np + r \\ mp + s \end{matrix} \right\} \equiv \left\{ \begin{matrix} n - m + r \\ s \end{matrix} \right\} \binom{n}{m} \pmod{p}.$$

Furthermore, by [118, Proposition 4.1], if r, s, a and f are nonnegative integers, then

$$(67) \quad \left\{ \begin{matrix} ap^f + r \\ s \end{matrix} \right\} \equiv \sum_{i_0 + i_1 + \dots + i_f} \binom{a}{i_0, i_1, \dots, i_f} \left\{ \begin{matrix} r + i_0 \\ s - \sum_{l=1}^f i_l p^f \end{matrix} \right\} \pmod{p}.$$

Remark 23. As noticed in [118, Remark 3.1], in the case $r < p$ the congruence (65) gives the formulas (4.17) and (4.18) of F.T. Howard [67] from 1990. \square

For nonnegative integers n and k *Stirling numbers of the first kind* $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ (Sloane's sequence A008275 in [124]) are defined by the recurrence relation

$$\left[\begin{matrix} n \\ k \end{matrix} \right] = \begin{cases} 1 & \text{if } n = 0, k = 0, \\ 0 & \text{if } n > 0, k = 0, \\ 0 & \text{if } n = 0, k > 0, \\ (n-1) \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right] + \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right] & \text{if } n > 0, k > 0. \end{cases}$$

The absolute value of $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ (Sloane's sequence A094638 in [124]) denotes, as usual, the number of permutations of n elements which contain exactly k permutation cycles.

In 1993 R. Peele, A.J. Radcliffe and H.S. Wilf [107, Proposition 2.1] proved the following analogue of Lucas' theorem for the numbers $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$: *Let p be a prime and let n and k be integers with $1 \leq k \leq n$. Let $n' = \lfloor n/p \rfloor$ and $n_0 = n - n'p$. Further, define integers i and j as follows:*

$$k - n' = j(p-1) + i \quad \text{with } 0 \leq i < p-1 \text{ if } n_0 = 0; \quad 0 < i \leq p-1 \text{ if } n_0 > 0.$$

Then

$$(68) \quad \left[\begin{matrix} n \\ k \end{matrix} \right] \equiv (-1)^{n'-j} \binom{n'}{j} \left[\begin{matrix} n_0 \\ i \end{matrix} \right] \pmod{p}.$$

For a nonnegative integer k let $J_k(z)$ be the —it Bessel function of the first kind. Put

$$f_k(z) = \frac{J_k(2\sqrt{z})}{z^{k/2}} = \sum_{i=0}^{\infty} \frac{(-1)^i z^i}{i!(i+k)!}.$$

Furthermore, define the polynomial $u_i(k; x)$ by means of

$$\frac{k! f_k(xz)}{f_k(z)} = \sum_{i=0}^{\infty} u_i(k; x) \frac{z^i}{i!(i+k)!}.$$

Certain Lucas type congruences for $w_i(x) = u_i(0; x)$ and the integers $w_i = w_i(0)$ with $i = 0, 1, 2, \dots$, were derived by L. Carlitz [22] in 1955, and an interesting application was presented ($(w_n)_{n \geq 0}$ is Sloane's sequence A000275). In 1987 F.T. Howard [66, Theorem 1] proved a more general result as follows: *Let k, n and s be nonnegative integers, and let p be a prime such that $p \geq 2k$ and $s < p - 2k$. Then the numbers $u_i(k) := u_i(k; 0)$ are integral $(\text{mod } p)$ for all $i = 0, 1, 2, \dots$; in particular, $u_n(0)$ and $u_n(1)$ are positive integers for all $n = 0, 1, 2, \dots$. Furthermore, for any fixed $k \geq 0$ and every prime p the congruence*

$$(69) \quad u_{np+s}(k) \equiv u_s(k) \cdot w_n \pmod{p}$$

holds for all $n \geq 0$ and $0 \leq s \leq n - 1$.

With the assumptions of the above statement, if m is a nonnegative integer with the expansion $m = \sum_{i=0}^s m_i p^i$ to base p satisfying $m_0 < p - 2k$, then the congruence (70) with $k = 0$ implies Carlitz's result [22] from 1955 which asserts that the sequence $(w_n)_{n \geq 0}$ has the Lucas property, i.e.,

$$(70) \quad w_m \equiv \prod_{i=0}^s w_{m_i} \pmod{p},$$

Furthermore, the following two congruences are satisfied [66, p. 306, Corollary and Theorem 2]:

$$(71) \quad u_m(k) \equiv u_{m_0}(k) \prod_{i=1}^s w_{m_i}(0) \pmod{p},$$

and

$$(72) \quad u_{np-k}(k) \equiv (-1)^k u_0(k) \cdot w_n(0) \pmod{p}.$$

Let p be a prime and let n, r, l and a be positive integers. Following Z.-W. Sun and D. Wan [130], the *normalized cyclotomic ψ -coefficient* is defined as

$$(73) \quad \left\{ \begin{matrix} n \\ r \end{matrix} \right\}_{l, p^a} := p^{-\left\lfloor \frac{n - p^{a-1} - lp^a}{\varphi(p^a)} \right\rfloor} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k} \binom{(k-r)/p^a}{l}.$$

In 2008 Z.-W. Sun and D. Wan [130, Theorem 1.1] proved that if p is any prime, r is an integer and a, l, n, s, t are positive integers with $a \geq 2$ and

$s, t < p$, then

$$(74) \quad \left\{ \begin{matrix} pn + s \\ pr + t \end{matrix} \right\}_{l, p^{a+1}} \equiv (-1)^t \binom{s}{t} \left\{ \begin{matrix} n \\ r \end{matrix} \right\}_{l, p^a} \pmod{p}.$$

It is noticed in [130, Remark 1.1] that in the case $l = 0$ the congruence (74) is equivalent to Theorem 1.7 in [129] due to Z.-W. Sun and D.M. Davis in 2007. Under the same conditions preceeding the congruence (74), Sun and Davis [129, Theorem 1.7] proved the following congruence of Lucas' type:

$$(75) \quad \frac{1}{[n/p^{a-1}]!} \sum_{k \equiv r \pmod{p^a}} (-1)^{pk} \binom{pn + s}{pk + t} \left(\frac{k - r}{p^{a-1}} \right)^l \\ \equiv \frac{1}{[n/p^{a-1}]!} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k} \binom{s}{t} \left(\frac{k - r}{p^{a-1}} \right)^l \pmod{p}.$$

J. Boulanger and J.-L. Chabert [18] have extended Lucas' theorem to Linear Algebra and Even Topology. Their result can be briefly exposed as follows. Let V be a discrete valuation domain with finite residue field. Denote by K the quotient field of V , by v the corresponding valuation of K , by \mathfrak{m} the maximal ideal of V , and by q the cardinality of the residue field V/\mathfrak{m} . We denote by \widehat{K} , \widehat{V} and $\widehat{\mathfrak{m}}$ the completions of K , V and \mathfrak{m} , respectively, with respect to the \mathfrak{m} -adic topology and we still denote by v the extension of v to \widehat{K} . Consider the ring $\text{Int}(V)$ of integer-valued polynomials on V , that is,

$$\text{Int}(V) = \{f \in K[X] : f(V) \subseteq V\}.$$

A basis $C_n(X)$ of the V -module $\text{Int}(V)$ can be constructed as follows [20, Chapter II, §2]. We choose a generator t of \mathfrak{m} and a set $U = \{u_0 = 0, u_1, \dots, u_{q-1}\}$ of representatives of V modulo \mathfrak{m} . It is known that each element x of \widehat{V} has a unique t -adic expansion

$$x = \sum_{j=0}^{\infty} x_j t^j \quad \text{with } x_j \in U \text{ for each } j \in \mathbb{N}.$$

We now construct a sequence $(u_n)_{n \geq 0}$ of elements of V which will replace the sequence of nonnegative integers. Taking q as the basis of the numeration, that is, writing every positive integer n in the form $n = \sum_{i=0}^k n_i q^i$ with $0 \leq n_i < q$ for each $i = 0, 1, \dots, k$, we extend the sequence $(u_j)_{0 \leq j < k}$ in the following way:

$$u_n = u_{n_0} + u_{n_1} t + u_{n_2} t^2 + \dots + u_{n_k} t^k.$$

We then replace the binomial polynomials

$$\binom{X}{n} = \frac{X(X-1)(X-2)\cdots(X-n+1)}{n!}$$

(which form a basis of the \mathbb{Z} -module $\text{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] : f(\mathbb{Z}) \subseteq \mathbb{Z}\}$ of integer-valued polynomials on \mathbb{Z}) by the polynomials defined as

$$C_n(X) = \prod_{k=0}^{n-1} \frac{X - u_k}{u_n - u_k}, \quad n = 1, 2, \dots, \text{ and } C_0 = 1.$$

Then by [20, Theorem II.2.7], the sequence of polynomials $(C_n(X))_{n \geq 0}$ form a basis of the V -module $\text{Int}(V)$. In 2001 J. Boulanger and J.-L. Chabert [18, Theorem 2.2] proved the following “generalized Lucas’ theorem”: *If*

$$n = n_0 + n_1q + \dots + n_kq^k$$

is the q -adic expansion of a positive integer n , and if

$$x = x_0 + x_1t + \dots + x_jt^j + \dots$$

is the t -adic expansion of an element x of \widehat{V} , then

$$(76) \quad C_n(x) \equiv C_{n_0}(x_0)C_{n_1}(x_1)\cdots C_{n_k}(x_k) \pmod{\widehat{\mathfrak{m}}}.$$

Remark 24. Notice also that in 1993 N. Zaheer [144] generalized Lucas’ theorem to vector-valued abstract polynomials in vector spaces. \square

5. LUCAS TYPE THEOREMS FOR SOME GENERALIZED BINOMIAL COEFFICIENTS

5.1. Generalized binomial coefficients and related Lucas type congruences. Let A and B be nonzero integers. The *Lucas sequence* u_0, u_1, u_2, \dots is defined recursively as

$$(77) \quad u_0 = 0, u_1 = 1 \quad \text{and} \quad u_{n+1} = Au_n - Bu_{n-1} \quad \text{for } n = 1, 2, 3, \dots$$

The companion sequence of Lucas sequence $(u_n)_{n \geq 0}$ is the sequence $(v_n)_{n \geq 0}$ recursively defined as

$$(78) \quad v_0 = 2, v_1 = A \quad \text{and} \quad v_{n+1} = Av_n - Bv_{n-1} \quad \text{for } n = 1, 2, 3, \dots$$

It is well known that for all $n = 0, 1, 2, \dots$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n,$$

where

$$\alpha = \frac{A + \sqrt{\Delta}}{2}, \beta = \frac{A - \sqrt{\Delta}}{2} \quad \text{and} \quad \Delta = A^2 - 4B.$$

In fact, α and β are roots of the characteristic equation $x^2 - Ax + B = 0$. Note that for $A = 1, B = -1$ the terms of the sequence $(u_n)_{n \geq 0}$ defined by (77) are the well-known *Fibonacci numbers* F_n defined recursively as $F_0 = 0, F_1 = 1$ and

$$F_{n+1} = F_n + F_{n-1} \quad \text{for } n \geq 1.$$

Fibonacci numbers are in fact the Lucas sequence $(u_n)_{n \geq 0}$ given by (77) with $u_0 = 0$ and $u_1 = 1$.

Similarly, the *Lucas numbers* L_n are defined by $L_0 = 2, L_1 = 1$ and

$$L_{n+1} = L_n + L_{n-1} \quad \text{for } n \geq 1.$$

Fibonacci numbers F_n and Lucas numbers L_n are given as Sloane's sequences A000045 and A000032 in [124], respectively.

Let $a := (a_n)_{n \geq 0}$ be a sequence of real or complex numbers such that $a_n \neq 0$ for all $n \geq 1$. The *a-nomial coefficients* (or the *generalized binomial coefficients*) (associated to the sequence a) are defined by

$$\begin{bmatrix} n \\ k \end{bmatrix}_a = \frac{a_n a_{n-1} \cdots a_1}{(a_k a_{k-1} \cdots a_1)(a_{n-k} a_{n-k-1} \cdots a_1)} \quad \text{for } n \geq 2 \text{ and } 1 \leq k \leq n-1,$$

and

$$\begin{bmatrix} n \\ 0 \end{bmatrix}_a = \begin{bmatrix} n \\ n \end{bmatrix}_a = 1 \quad \text{for } n \geq 0.$$

This definition was suggested in 1915 by Georges Fontené in his one-page note [41]. A number of authors have considered different classes of generalized binomial coefficients $\begin{bmatrix} n \\ k \end{bmatrix}_a$ (usually, when $a := (a_n)_{n \geq 0}$ is an integer sequence). Related investigations were done in 1913 by R.D. Carmichael [24], in 1936 by M. Ward, [136], in 1967 by R.D. Fray [42] and V.E. Hoggatt [59], in 1969 by H.W. Gould [50], and later by several authors ([61], [62], [77], [79], [102], [134] and [135]). For example, in 1989 D.E. Knuth and H.S. Wilf [79, Proposition 3] generalized Kummer's theorem for the *a-nomial coefficients* $\begin{bmatrix} m+k \\ m \end{bmatrix}_a$, where $a = (a_n)_{n \geq 1}$ is a sequence of positive integers. Consequently, they obtained [79, Theorems 1 and 2] Kummer's theorem for the Gaussian *q-nomial coefficients* $\begin{bmatrix} m+k \\ m \end{bmatrix}_q$ where $q > 1$ is an integer and for the Fibonomial coefficients $\begin{bmatrix} m+k \\ m \end{bmatrix}_{\mathcal{F}}$ defined below, respectively.

In general, even if the all terms of a sequence $a = (a_n)_{n \geq 0}$ are integers, $\begin{bmatrix} n \\ k \end{bmatrix}_a$ may not be integers. In 1913 R.D. Carmichael [24, page 40] proved that *if the sequence $a := (a_n)_{n \geq 1}$ of positive integers is defined recursively as*

$$a_1 = a_2 = 1, \quad \text{and} \quad a_{n+1} = ca_n + da_{n-1} \quad \text{for } n = 2, 3, 4, \dots,$$

where c and d are integers, then the all a -nomial coefficients are integers. For a more general result see Remark 28.

If $u := (u_n)_{n \geq 0}$ is the Lucas sequence defined by (77), and if $A \neq \pm 1$ or $B \neq 1$, then u_1, u_2, \dots are nonzero (see, e.g., [69]), and so are $v_1 = u_2/u_1$, $v_2 = u_4/u_2, \dots$, where $v := (v_n)_{n \geq 0}$ is the companion sequence of the sequence $(u_n)_{n \geq 0}$ given by (78). In the case when $A^2 = B = 1$, then as noticed in [69] $u_n = 0$ if and only if $3 \mid n$. If $v_n = 0$, then $u_{2n} = u_n v_n = 0$; hence $3 \mid n$ and $u_n = 0$, which is impossible since $v_n^2 - \Delta u_n^2 = 4B^n$ (cf. [68]). Thus v_0, v_1, v_2, \dots are all nonzero.

If $A \neq \pm 1$ or $B \neq 1$ the *Lucas u -nomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_u$ with $1 \leq k \leq n$ is the generalized binomial coefficient associated to the Lucas sequence $u := (u_n)_{n \geq 0}$ defined by (77), that is,

$$\begin{bmatrix} n \\ k \end{bmatrix}_u = \frac{u_n u_{n-1} \cdots u_1}{(u_k u_{k-1} \cdots u_1)(u_{n-k} u_{n-k-1} \cdots u_1)} \quad \text{for } n \geq 2 \text{ and } 1 \leq k \leq n-1,$$

and $\begin{bmatrix} n \\ 0 \end{bmatrix}_u = \begin{bmatrix} n \\ n \end{bmatrix}_u = 1$ for all $n \geq 0$.

In the sam way we define the *v -nomial generalized binomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_v$, where $v := (v_n)_{n \geq 0}$ is the companion sequence of the Lucas sequence $(u_n)_{n \geq 0}$ defined by (78).

Remark 25. In the case $A = 2$ and $B = 1$, (77) yields $u_n = n$ for all $n = 0, 1, 2, \dots$, and hence $\begin{bmatrix} n \\ k \end{bmatrix}_u$ is exactly the binomial coefficient $\binom{n}{k}$. \square

Similarly, the *Fibonomial coefficients* (or *Fibonacci coefficients*) are defined as the generalized binomial coefficients associated to the sequence $(F_n)_{n \geq 0}$ of Fibonacci numbers, that is,

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\mathcal{F}} = \frac{F_n F_{n-1} \cdots F_1}{(F_k F_{k-1} \cdots F_1)(F_{n-k} F_{n-k-1} \cdots F_1)} \quad \text{for } n \geq 2 \text{ and } 1 \leq k \leq n-1,$$

and $\begin{bmatrix} n \\ 0 \end{bmatrix}_{\mathcal{F}} = \begin{bmatrix} n \\ n \end{bmatrix}_{\mathcal{F}} = 1$ for all $n \geq 0$.

The Fibonomial coefficients and the Lucas u -nomial coefficients were introduced in 1878 by É. Lucas [87, §9], and later they have been studied by several authors (see [50], [59], [60], [139], [69] and [68]).

The triangle of Fibonomial coefficients is given as Sloane's sequence A010048 in [124]. It is known (see, e.g., [59, the equality (D), page 386]) that

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\mathcal{F}} = F_{k+1} \begin{bmatrix} n-1 \\ k \end{bmatrix}_{\mathcal{F}} + F_{n-k-1} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_{\mathcal{F}}, \quad \text{for } 0 \leq k \leq n-1,$$

whence by induction immediately follows that the all Fibonomial coefficients are integers.

When $A = q+1$ and $B = q$ related to the sequence defined by (77), where q is an integer such that $|q| > 1$, $\begin{bmatrix} n \\ k \end{bmatrix}_u$, then it coincides with the *Gaussian*

q -nomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ because $u_j = (q^j - 1)/(q - 1)$ for $j = 1, 2, \dots$, and hence,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

The numbers $\begin{bmatrix} n \\ k \end{bmatrix}_q$ were introduced in 1808 by Gauss [46, §5]. It is well known that these numbers satisfy the recursion formula

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q, \text{ for } 0 \leq k \leq n-1.$$

The triangles of Gaussian q -nomial coefficients for $q = -2, 2, 3, 4, 5, 6, 7, 8, 9$ are given as Sloane's sequences A015109, A022166, A022167, A022168, A022169, A022170, A022171, A022172 and A022173 in [124], respectively.

It is easy to see that if $0 \leq m \leq n$, then

$$\lim_{q \rightarrow 1} \begin{bmatrix} n \\ m \end{bmatrix}_q = \binom{n}{m},$$

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \begin{bmatrix} n \\ n-m \end{bmatrix}_q \quad (\text{symmetry})$$

and

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q + q^m \begin{bmatrix} n-1 \\ m \end{bmatrix}_q,$$

whence easily follows by induction that if q is any positive integer, then $\begin{bmatrix} n \\ m \end{bmatrix}_q$ are also integers for all n and m . \square

Remark 26. An analogy to the Lucas u -nomial coefficients $\begin{bmatrix} n \\ k \end{bmatrix}_u$ was obtained in 1995 by W.A. Kimball and W.A. Webb [77] and in 1998 by B. Wilson [140] in some special cases, and in 2001 by H. Hu and Z.-W. Sun [69] for the general case (see Subsection 5.2). \square

It is known (see, e.g., [84], [139]) that the generalized base for the Fibonacci sequence is

$$\mathcal{P} = \{r_0, r_1, r_2, r_3, r_4, \dots\} = \{1, 3, 6, 6, 12, \dots\}$$

in the sense that any positive integer n can be uniquely expressed as

$$n = (n_s n_{s-1} \dots n_1 n_0)_{\mathcal{P}} := n_0 + n_1 r_1 + \dots + n_{s-1} r_{s-1} + n_s r_s,$$

where $0 \leq n_i < r_{i+1}/r_i$ for each $i = 0, 1, \dots, s-1$.

Under the above notations, in 1994 D.L. Wells [139, Theorem 2] proved that

$$(79) \quad \begin{bmatrix} n \\ k \end{bmatrix}_{\mathcal{F}} \equiv \begin{bmatrix} n_0 \\ k_0 \end{bmatrix}_{\mathcal{F}} \cdot \prod_{i \geq 1} \binom{n_i}{k_i} \pmod{2}.$$

In 1988 M. Sved [131] established that the geometry of the binomial arrays of Pascal's triangle modulo p gives a simple interpretation of Lucas' theorem. Moreover, as noticed in [131, p. 58], this interpretation can be extended to arrays of other combinatorial functions; in particular, Lucas' theorem can be generalized to the Gaussian q -nomial coefficients as follows. *Let p be a prime, $q > 1$ a positive integer not divisible by p , and let $a \neq 1$ be the minimal exponent for which $q^a \equiv 1 \pmod{p}$; then by Fermat little theorem it follows that $a \mid (p-1)$. Further, if $n = Na + n_0$, $m = Ma + m_0$ with $0 \leq n_0 < a$ and $0 \leq m_0 < a$, then [131, p. 60]*

$$(80) \quad \begin{bmatrix} n \\ m \end{bmatrix}_q \equiv \binom{N}{M} \begin{bmatrix} n_0 \\ m_0 \end{bmatrix}_q \pmod{p}.$$

Remark 27. In the same area of research A. Bès [16] generalized Lucas' theorem. This accomplishment obviously serves to improve the security of cryptographic applications modulo prime powers [16]. \square

Definition. For a positive integer d , the *rank of apparition* $r = r(d)$ with respect to the integer sequence $(a_n)_{n \geq 0}$ is the least index n for which d divides a_n , that is, $r(d) = \min\{n \in \mathbb{N} : d \mid a_n\}$ (if d does not divide any a_n , then $r(d) = \infty$). \square

Remark 28. Let $a = (a_n)_{n \geq 0}$ be an integer sequence. In order to guarantee that the all a -nomial coefficients $\begin{bmatrix} n \\ k \end{bmatrix}_a = 0$ are integers, it is usually required that the sequence $a = (a_n)_{n \geq 0}$ be *regularly divisible*, that is, $p^i \mid a_j$ if and only if $r(p^i) \mid j$ for all $i \geq 1$, $j \geq 1$, and all primes p . Here $r(p^i)$ denotes the rank of apparition of p^i as defined above. The principal class of sequences which are known to be regularly divisible are the Lucas sequences given by (77) for which $\gcd(A, B) = 1$ (see [63]). \square

In 2000 J.M. Holte [61, Theorem 1] proved the following result: *Let p be a prime and let m and n be nonnegative integers. Let r be the rank of apparition of p with respect to the Lucas sequence $u = (u_n)$, let τ be the period of (u_n) modulo p , and let $t = \tau/r$ (t is necessarily a positive integer). Furthermore, for $i, j \geq 0$ and for $0 \leq k, l < r$, let $A_{i,j}(k, l)$ denote the solution of the modulo p recurrence relation*

$$A_{i,j}(k, l) \equiv u_{ir+k+1}A_{i,j}(k, l-1) + bu_{jr+l-1}A_{i,j}(k-1, l) \pmod{p},$$

and let $H_{i,j}(k, l) = u_{r+1}^{rij}A_{i,j}(k, l)$. Set $n_0 = n \pmod{r}$, $m_0 = m \pmod{r}$, $n' = n + r$, $m' = m + r$, $n'' = n' \pmod{t}$, and $m'' = m' \pmod{t}$. Then

$$(81) \quad \begin{bmatrix} m+n \\ n \end{bmatrix}_u \equiv \binom{m'+n'}{n'} H_{m'',n''}(m_0, n_0) \pmod{p}.$$

Using the above result, with the same notations as above, Holte [61, Theorem 3] also proved the following result: *Let (u_n) be the Lucas sequence defined by (77), let p be a prime such that B is not divisible by p . Set $\lambda = \max\{0, m'' + n'' - (p - 1)\}$, $n^* = n(\bmod t)$ and $m^* = m(\bmod t)$. Then*

$$(82) \quad \begin{bmatrix} m + n \\ n \end{bmatrix}_u \equiv \begin{pmatrix} m' + n' \\ n' \end{pmatrix} \begin{pmatrix} m'' + n'' + \lambda t \\ n'' + \lambda t \end{pmatrix}^{-1} \begin{bmatrix} m^* \\ n^* + \lambda \tau \end{bmatrix}_u \pmod{p}.$$

Thus, except when $s = p - 1$ and $m'' + n'' \geq p$, then

$$(83) \quad \begin{bmatrix} m + n \\ n \end{bmatrix}_u \equiv \begin{pmatrix} m' + n' \\ n' \end{pmatrix} \begin{pmatrix} m'' + n'' + \lambda t \\ n'' \end{pmatrix}^{-1} \begin{bmatrix} m^* \\ n^* \end{bmatrix}_u \pmod{p}.$$

Holte [61, Section 7] noticed that by means of a bit of translation, the congruence (82) may be transformed into the following result obtained in 1992 by D. Wells [137] (also see [138]): *Let $N = n + m$, and correspondingly, $N_0 = N(\bmod r)$, $N' = \lfloor N/r \rfloor$, and $N'' = N'(\bmod s)$. Let $N' = \sum_{j=0}^l N_j p^j$ and $m' = \sum_{j=0}^l m_j p^j$ be the p -adic expansions of N' and m' . If p is a prime such that B is not divisible by p , then under the same definitions of B and t as above, for $N'' \geq m''$,*

$$(84) \quad \begin{bmatrix} N \\ m \end{bmatrix}_u \equiv \begin{pmatrix} N'' \\ m'' \end{pmatrix}^{-1} \prod_{j=0}^l \begin{pmatrix} N_j \\ m_j \end{pmatrix} \begin{bmatrix} Nr + N_0 \\ m''r + m_0 \end{bmatrix}_u \pmod{p},$$

and for $N'' < m''$,

$$(85) \quad \begin{bmatrix} N \\ m \end{bmatrix}_u \equiv \begin{cases} \begin{pmatrix} s + N'' \\ m'' \end{pmatrix}^{-1} \prod_{j=0}^l \begin{pmatrix} N_j \\ m_j \end{pmatrix} \begin{bmatrix} t + N''r + N_0 \\ m''r + m_0 \end{bmatrix}_u \pmod{p} & \text{if } s < p - 1 \\ \begin{pmatrix} s \\ m'' \end{pmatrix}^{-1} \prod_{j=0}^l \begin{pmatrix} N_j \\ m_j \end{pmatrix} \begin{bmatrix} (N'' + 1)t + N''r + N_0 \\ m''r + m_0 \end{bmatrix}_u \pmod{p} & \text{if } s = p - 1. \end{cases}$$

Remark 29. In 2002 E.R. Tou [135, Theorem 4] generalized the congruence (82) modulo product of a finite number of distinct primes. \square

5.2. Lucas type congruences for some classes of Lucas u -nomial coefficients. In 2001 H. Hu and Z.-W. Sun [69, Theorem] proved the following result for the Lucas u -nomial coefficients: *Let $u = (u_n)_{n \geq 0}$ be a Lucas sequence defined by (77). Suppose that $\gcd(A, B) = 1$, and $A \neq \pm 1$ or $B \neq \pm 1$. Then $u_k \neq 0$ for every $k \geq 1$. Let q be a positive integer, let m and n be nonnegative integers, and let $R(q) = \{0, 1, \dots, q - 1\}$. If $s, t \in R(q)$ then*

$$(86) \quad \begin{bmatrix} mq + s \\ nq + t \end{bmatrix}_u \equiv \begin{pmatrix} m \\ n \end{pmatrix} \begin{bmatrix} s \\ t \end{bmatrix}_u u_{q+1}^{(nq+t)(m-n)+n(s-t)} \pmod{w_q},$$

where w_q is the largest divisor of u_q relatively prime to u_1, \dots, u_{q-1} . If q or $m(n+t) + n(s+1)$ is even, then

$$(87) \quad \begin{bmatrix} mq+s \\ nq+t \end{bmatrix}_u \equiv \binom{m}{n} \begin{bmatrix} s \\ t \end{bmatrix}_u (-1)^{(mt-ns)(q-1)} B^{\frac{q}{2}((nq+t)(m-n)+n(s-t))} \pmod{w_q}.$$

Remark 30. ([69, Remark 1]) When $A = 2$ and $B = 1$, we have $u_k = k$ for each nonnegative integer k , and if in addition we assume that $q = p$ is a prime, then $w_p = p$, and hence the congruence (86) becomes

$$\begin{pmatrix} mp+s \\ np+t \end{pmatrix} \equiv \binom{m}{n} \binom{s}{t} \pmod{p},$$

which is in fact, Lucas' theorem. \square

In 2002 H. Hu [68, p. 291, Theorem] proved the following result: *Let q be a positive integer, and let m and n be even nonnegative integers with $n \leq m$. Let s and t be nonnegative integers such that $t \leq s < q$, and let v_q^* be the largest divisor of v_q relatively prime to v_0, \dots, v_{q-1} . Then*

$$(88) \quad \begin{pmatrix} m/2 \\ n/2 \end{pmatrix} \begin{bmatrix} mq+s \\ nq+t \end{bmatrix}_u \equiv \binom{m}{n} \begin{bmatrix} s \\ t \end{bmatrix}_u (-B^q)^{\frac{m-n}{2}(nq+t)+\frac{n}{2}(s-t)} \pmod{v_q^*}.$$

Lucas type congruences modulo p^2 and p^3 (p is a prime > 3) for Lucas u -nomial coefficients and Fibonomial coefficients are established in [76], [77] and [120]. Namely, in 1993 W.A. Kimball and W.A. Webb [76] (also see [120, p. 1029]) proved the following two results: *Let p be an odd prime and let m and n be nonnegative integers. Suppose that τ is the period of the Fibonacci sequence $(F_n)_{n \geq 0}$ modulo p , r is the rank of apparition of p (that is, r is the least index k for which p divides F_k), and $t = \tau/r$ is an integer. In [134] it is shown that $t \in \{1, 2, 4\}$. The number ε is defined as follows: $\varepsilon = 1$ if $\tau = r$; $\varepsilon = -1$ if $\tau = 2r$; and $\varepsilon^2 \equiv -1 \pmod{p^2}$ if $\tau = 4r$; in this case $p \equiv 1 \pmod{4}$. Then*

$$(89) \quad \begin{bmatrix} m\tau \\ n\tau \end{bmatrix}_{\mathcal{F}} \equiv \begin{pmatrix} mt \\ nt \end{pmatrix} \pmod{p^2}$$

and

$$(90) \quad \begin{bmatrix} mr \\ nr \end{bmatrix}_{\mathcal{F}} \equiv \varepsilon^{(m-n)nr} \begin{bmatrix} m \\ n \end{bmatrix}_{\mathcal{F}} \pmod{p^2}.$$

In 1995 Kimball and Webb [77, Theorems 1 and 3] proved the following results: *Let $(u_n)_{n \geq 0}$ and $(v_n)_{n \geq 0}$ be the sequences defined by (77) and (78), respectively, where A and B are nonzero integers such that $\gcd(A, B) = 1$. Let p be an odd prime, let τ be the period of the sequence $(u_n)_{n \geq 0}$ modulo*

p , and let r be the rank of apparition of p . Then for all nonnegative integers m and n such that $n \leq m$ there holds

$$(91) \quad \left[\begin{matrix} mr \\ nr \end{matrix} \right]_u \equiv \left(\frac{v_r}{2} \right)^{(m-n)nr} \binom{m}{n} \pmod{p^2}$$

and

$$(92) \quad \left[\begin{matrix} m\tau \\ n\tau \end{matrix} \right]_u \equiv \left(1 + \frac{1}{2}\tau(m-n)n((-B)^\tau - 1) \right) \binom{mt}{nt} \pmod{p^2}.$$

As a consequence of the congruence (91), it is proved in [77, Corollary 2] that

$$(93) \quad \left[\begin{matrix} m\tau \\ n\tau \end{matrix} \right]_u \equiv \left(1 + \tau(m-n)n \left(\left(\frac{v_r}{2} \right)^t - 1 \right) \right) \binom{mt}{nt} \pmod{p^2}.$$

Moreover, the congruence (92) immediately implies [77, Corollary 4] that if $B = \pm 1$, then

$$(94) \quad \left[\begin{matrix} m\tau \\ n\tau \end{matrix} \right]_u \equiv \binom{mt}{nt} \pmod{p^2}.$$

Kimball and Webb [77, Theorem 5] also proved the following congruences for the Gaussian q -nomial coefficients:

$$(95) \quad \begin{aligned} \left[\begin{matrix} mr \\ nr \end{matrix} \right]_q &\equiv \left(\frac{q^r + 1}{2} \right)^{(m-n)nr} \binom{m}{n} \pmod{p^2} \\ &\equiv \left(1 + \frac{1}{2}r(m-n)n(q^r - 1) \right) \binom{m}{n} \pmod{p^2}, \end{aligned}$$

where p is a prime, q is any p -integral rational number such that $q^2 - q$ is not divisible by p , and r is the rank of apparition of p .

In 1998 B. Wilson [140] proved the following result: *Let p be a prime such that $p \neq 2, 5$, and let r be the rank of apparition of p with respect to the Fibonacci sequence $(F_n)_{n \geq 0}$. Then for any nonnegative integers m, n, s and l such that $0 \leq s, l < r$*

$$(96) \quad \left[\begin{matrix} mr \\ nr \end{matrix} \right]_{\mathcal{F}} \equiv \left[\begin{matrix} m \\ n \end{matrix} \right]_{\mathcal{F}} F_{r+1}^{(m-n)nr} \pmod{p}$$

and

$$(97) \quad \left[\begin{matrix} mr + s \\ nr + l \end{matrix} \right]_{\mathcal{F}} \equiv \binom{m}{n} \left[\begin{matrix} s \\ l \end{matrix} \right]_{\mathcal{F}} F_{r+1}^{(nr+l)(m-n)+n(s-l)} \pmod{p}.$$

In 2007 L.-L. Shi [120] proved another congruence modulo p^2 (where $p > 3$ is a prime) for the Lucas u -nomial coefficients. Namely, in [120, Theorem 2] it is proved the following result: *Let $(u_n)_{n \geq 0}$ be the Lucas sequence defined by (77), where A and B are nonzero integers such that*

$\gcd(A, B) = 1$, and $A \neq \pm 1$ or $B \neq 1$. Let $p > 3$ be a prime not dividing B . If r is the rank of apparition of p with respect to $(u_n)_{n \geq 0}$, then for any nonnegative integers m, n, s and t such that $0 \leq s, l < r$, we have

(98)

$$\begin{bmatrix} mr + s \\ nr + l \end{bmatrix}_u \equiv \begin{cases} (-1)^{l-s-1} B^{-\binom{l-s}{2}} u_{(m-n)r} u_{l-s}^{-1} \\ \times u_{r+1}^{(m-n)(l-1)-n(l-s)} \begin{bmatrix} mr \\ nr \end{bmatrix}_u \left(\begin{bmatrix} l \\ s \end{bmatrix}_u \right)^{-1} \pmod{p^2} & \text{if } s < l \\ u_{r+1}^{ml+ns-2nl} \frac{S_{m,s}}{S_{n,l} S_{m-n,s-l}} \begin{bmatrix} mr \\ nr \end{bmatrix}_u \begin{bmatrix} s \\ l \end{bmatrix}_u \pmod{p^2} & \text{if } s \geq l, \end{cases}$$

where $S_{k,i} = 1 - (kBu_r)/u_{r+1} \sum_{j=1}^i (u_{j-1}/u_j)$.

If $\Delta := A^2 - 4B$ is not divisible by p , then $\begin{bmatrix} mr \\ nr \end{bmatrix}_u$ in (98) can be replaced by $(v_r/2)^{(m-n)nr} \binom{m}{n}$.

In 1995 Kimball and Webb [78, Theorem] and in 2007 L.-L. Shi [120] considered the *generalized Lucas u -nomial coefficients* and the *generalized Fibonomial coefficients* defined as follows. If $(u_n)_{n \geq 0}$ is the Lucas sequence defined by (77) such that $A \neq \pm 1$ or $B \neq 1$, and let $(F_n)_{n \geq 0}$ be the Fibonacci sequence. For any positive integer j we set

$$[n]_u^j = \prod_{k=1}^n u_{kj} \quad \text{and} \quad [n]_{\mathcal{F}}^j = \prod_{k=1}^n F_{kj},$$

for $n = 0, 1, 2, \dots$, and regard an empty product as value 1.

Then for $n, k = 0, 1, 2, \dots$ the *generalized Lucas u -nomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_u^j$ and the *generalized Fibonomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_{\mathcal{F}}^j$ are defined as follows:

$$\begin{bmatrix} n \\ k \end{bmatrix}_u^j = \begin{cases} \frac{[n]_u^j}{[k]_u^j [n-k]_u^j} & \text{if } 0 \leq k \leq n \\ 0 & \text{otherwise,} \end{cases}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\mathcal{F}}^j = \begin{cases} \frac{[n]_{\mathcal{F}}^j}{[k]_{\mathcal{F}}^j [n-k]_{\mathcal{F}}^j} & \text{if } 0 \leq k \leq n \\ 0 & \text{otherwise.} \end{cases}$$

where $(u_{ij}/u_j)_{i \geq 0}$ is also a Lucas sequence.

In 1995 Kimball and Webb [78, Theorem] extended the congruence (90) by showing that *if the rank r of apparition of p is $p+1$ or $p-1$, then for any prime $p > 3$ and any $m \geq n \geq 0$,*

$$(99) \quad \begin{bmatrix} mr \\ nr \end{bmatrix}_{\mathcal{F}} \equiv (\mp)^{(m-n)n} \begin{bmatrix} m \\ n \end{bmatrix}_{\mathcal{F}}^r \pmod{p^3}, \quad \text{respectively.}$$

In 2007 Shi [120] proved the congruence modulo p^3 (where $p > 3$ is a prime) for the generalized Lucas u -nomial coefficients. Namely, in [120, Theorem 1] it is proved the following result: *Let A and B be nonzero integers such that $\gcd(A, B) = 1$, and $A \neq \pm 1$ or $B \neq 1$. Let $p > 3$ be a prime not dividing B . If the rank r of apparition of p is $p+1$ or $p-1$ (and hence*

$r = p - \left(\frac{A^2 - 4B}{p}\right)$), where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, then for any nonnegative integers m and n we have

$$(100) \quad \begin{bmatrix} mr \\ nr \end{bmatrix}_u \equiv (-1)^{(m-n)n} B^{(m-n)n} \binom{r}{2} \begin{bmatrix} m \\ n \end{bmatrix}_u^r \pmod{p^3}.$$

Remark 31. In the case $A = -B = 1$ the congruence (100) yields the congruence (99) of Kimball and Webb [78]. \square

In 1965 G. Olive [104] (also see [105, Lemma 2.1]) proved the following result: *Suppose that d is a positive integer and a, b, h, l are integers such that $0 \leq b, l \leq d - 1$. Then*

$$(101) \quad \begin{bmatrix} ad + b \\ hd + l \end{bmatrix}_q \equiv \binom{a}{h} \begin{bmatrix} b \\ l \end{bmatrix}_q \pmod{\Phi_d(q)},$$

where $\Phi_d(q)$ is the d th cyclotomic polynomial.

Remark 32. As noticed in [119, Chapter 5, p. 506], the congruence (101) perhaps was known to Gauss and it is rediscovered in 1982 by J. Désarménien [32] and V. Strehl [128] whose proof uses combinatorial arguments. \square

Remark 33. Another different q -analogue of the congruence (101) was established in 1967 by R.D. Fray [42]. \square

Remark 34. Applying Lucas' theorem, in 2006 S.-P. Eu, S.-C. Liu and Y.-N. Yeh [37] established the congruences of several combinatorial numbers, including Delannoy numbers and a class of Apéry-like numbers, the numbers of noncrossing connected graphs (Sloane's sequence A007297), the numbers of total edges of all noncrossing connected graphs on n vertices (Sloane's sequence A045741), etc. \square

6. SOME APPLICATIONS OF LUCAS' THEOREM

Even today, Lucas' theorem is being studied widely, and has both extended and generalized, particularly in the area of divisibility of binomial coefficients. Numerous results on divisibility of binomial and multinomial coefficients by primes and prime powers and related historical notes are given in 1980 by D. Singmaster [122]. Furthermore, Lucas' theorem has numerous applications in Number Theory, Combinatorics, Cryptography and Probability. We also point out that this theorem has become ubiquitous in the Theory of cellular automata.

6.1. Lucas' theorem and the Pascal's triangle. Let $a_k(n)$ be the number of integers $0 \leq m \leq n$ such that $\binom{n}{m} \not\equiv 0 \pmod{k}$, that is, $a_k(n)$ is the number of nonzero entries on row n of Pascal's triangle modulo k . Let $|n|_w$ be the number of occurrences of the word w in $n_s n_{s-1} \cdots n_0$, where

$n = \sum_{i=0}^s n_i k^i$ is the base- k representation of n . In 1899 J.W.L. Glaisher [48, §14] initiated the study of counting entries on row n of Pascal's triangle modulo k by using Lucas' theorem to determine $a_2(n) = 2^{|n|_1}$. The proof is simple (cf. [114, p. 1]): In order that $\binom{n}{m}$ be odd, each term $\binom{n_i}{m_i}$ in the product must be 1, so if $n_i = 0$ then $m_i = 0$ and if $n_i = 1$ then m_i can be either 0 or 1. It was the first result on a thorny path of solution of this difficult problem. However, this topic was forgotten for almost a half-century.

In 1947 N.J. Fine [39] generalized Glaisher's result to an arbitrary prime. Fine's result follows from Lucas' theorem in the same way: *Let p be a prime, and let n be a nonnegative integer. The number of nonzero entries on row $n = \sum_{i=0}^s n_i p^i$ of Pascal's triangle modulo p is (cf. [114, p. 2])*

$$(102) \quad a_p(n) = \prod_{i=0}^s (n_i + 1).$$

Namely, the formula (102) immediately follows from the fact that by Lucas' theorem, the binomial coefficient $\binom{n}{m}$ with $m = \sum_{i=0}^s m_i p^i$ is not divisible by a prime p if and only if $0 \leq m_i \leq n_i$ for all $i = 0, 1, \dots, s$.

Remark. 35. If $p = 2$, then the formula (102) presents the number of odd entries on row $n = \sum_{i=0}^s n_i 2^i$ of Pascal's triangle. Notice that the parity of binomial coefficients has played an important role in a paper from 1984 of J.P. Jones and Y.V. Matijasevič [73] in connection with Hilbert's tenth problem, Gödel's undecidability proposition and computational complexity. They base their Lemma on the Lucas' theorem given by the congruence (1) with $p = 2$ (cf. [74, Lemmas 3.9 and 3.10]). \square

As noticed in [114], one may generalize Glaisher's result in a different direction, namely to ask for the number $a_{k,r}$ of integers $0 \leq m \leq n$ such that $\binom{n}{m} \equiv r \pmod{k}$. In 2011 E. Rowland [114, Section 2, Theorem 1] generalized Fine's result to prime powers, obtaining a formula for the sum $a_{p^\alpha}(n) = \sum_{r=1}^{p^\alpha-1} a_{p,r}(n)$. Notice that in 1978 E. Hexel and H. Sachs [58, §5] determined a formula for $a_{p,r}(n)$ in terms of $(p-1)$ th roots of unity, where r is a primitive root modulo p . For some related results see also [5], [28], [44], [51] and [114, Theorem 2]).

The previous considerations can be generalized as follows. Let p be a prime. For nonnegative integers n and k consider the set

$$A_{n,k}^{(p)} = \{j \in \{0, 1, \dots, n\} : p^k \parallel \binom{n}{j}\},$$

where $p^k \parallel \binom{n}{j}$ denotes that $p^k \mid \binom{n}{j}$ and $\binom{n}{j} \not\equiv 0 \pmod{p^{k+1}}$. In particular, $A_{n,0}^{(p)}$ is a set of nonzero entries on row n of Pascal's triangle modulo k . Therefore, under the previous notation, for a prime p we have $a_p(n) =$

$|A_{n,0}^{(p)}|$ ($|S|$ denotes the cardinality of a set S), Notice that $|A_{n,0}^{(p)}|$ can be evaluated by Fine's formula (102). In 1967 L. Carlitz [23] solved a difficult problem for evaluation of $|A_{n,1}^{(p)}|$. In 1971 F.T. Howard [64], discovered the formula for $|A_{n,k}^{(2)}|$ for arbitrary k . In 1973 F.T. Howard [65] found a solution for $|A_{n,2}^{(p)}|$.

Further related results are given in [52], and in 1997 by J.G. Huard, B.K. Spearman and K.S. Williams [70]. Let n be a nonnegative integer. The n th row of Pascal's triangle consists of the following $n+1$ binomial coefficients:

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}.$$

We denote by $N_n(t, m)$ the number of those binomial coefficients which are congruent to t modulo m , where t and $m \geq 1$ are integers such that $0 \leq t \leq m-1$. Let p be a prime, and let n be a positive integer with the p -adic expansion $n = \sum_{i=0}^k n_i p^i$. We denote the number of r 's occurring among n_0, n_1, \dots, n_k by l_r ($r = 0, 1, \dots, p-1$). Set $\omega = e^{2\pi i/(p-1)}$ and let g denote a primitive root modulo p . Denote by $\text{ind}_g t$ the index of the integer $t \not\equiv 0 \pmod{p}$ with respect to g ; that is, $\text{ind}_g t$ is the unique integer j such that $t \equiv g^j \pmod{p}$. In 1978 E. Hexel and H. Sachs [58, Theorem 3] have shown that for $t = 1, 2, \dots, p-1$,

$$(103) \quad N_n(t, p) = \frac{1}{p-1} \sum_{s=0}^{p-2} \omega^{-s \text{ind}_g t} \prod_{r=1}^{p-1} B(r, s)^{l_r},$$

where

$$B(r, s) = \sum_{j=0}^r \omega^{s \text{ind}_g \binom{r}{j}}.$$

By using the formula (103), in 1997 J.G. Huard, B.K. Spearman and K.S. Williams proved the analogous formula for $N_n(tp, p^2)$ with $t = 1, 2, \dots, p-1$ [70, Theorem 1.1]. They proved that for $t = 1, 2, \dots, p-1$,

$$(104) \quad N_n(tp, p^2) = \frac{1}{p-1} \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} l_{ij} \sum_{s=0}^{p-2} \omega^{-s(\text{ind}_g t + \text{ind}_g(i+1) - \text{ind}_g j)} \\ \times B(p-2-i, -s) B(j-1, s) \prod_{r=1}^{p-1} B(r, s)^{l_r - \delta(r-i) - \delta(r-j)},$$

where

$$\delta(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0, \end{cases}$$

and l_{ij} denotes the number of occurrences of the pair ij in the string $n_0 n_1 \dots n_k$.

Let p be a prime, and let k be a positive integer. Let $A(k, p)$ be the matrix with entries $\binom{i}{j}_p := \binom{i}{j}(\bmod p)$, $0 \leq i < p^k$, $0 \leq j < p^k$ (actually, $\binom{i}{j}_p$ is the remainder of the division of $\binom{i}{j}$ by p). By using the Lucas property of the matrix $A(k, p)$ given by (54), in 1994 M. Razpet [111, p. 378] *proved that the number of all zero entries of the matrix $A(k, p)$ is equal to $p^{2n} - \binom{p+1}{2}^k$, and hence, the number of all nonzero entries of the matrix $A(k, p)$ is equal to $\binom{p+1}{2}^k$.*

Let p be a prime, and let n be a positive integer. For an integer r such that $0 \leq r \leq p-1$, let $b_r(n)$ be the number of binomial coefficients $\binom{i}{j}$ with $0 \leq j \leq i < n$ such that $\binom{i}{j} \equiv r(\bmod p)$. In 1957 J.B. Roberts [113] established systems of simultaneous linear difference equations with constant coefficients whose solutions would yield the quantities $b_r(n)$ explicitly. Namely, if $0 \leq c \leq p-1$, $1 \leq t \leq p^k$, $k > 0$, and if \bar{q} is the reciprocal of $q \in \{1, 3, \dots, p-1\}$ modulo p (i.e., $q\bar{q} \equiv 1(\bmod p)$), then by [113, Theorem 1],

$$(105) \quad b_r(cp^k + t) = b_r(cp^k) + \sum_{q=1}^{p-1} (b_{r\bar{q}}(c+1) - b_{r\bar{q}}(c))b_q(t).$$

Furthermore, if $b(n) = \sum_{r=1}^{p-1} b_r(n)$ and $n = \sum_{i=0}^k n_i p^i$ with $0 \leq n_i \leq p-1$ for all $i = 0, 1, \dots, k$, then by [113, Corollary 4],

$$(106) \quad b(n) = \frac{1}{2} \sum_{i=0}^k n_i ((n_i + 1) \cdots (n_k + 1)) \left(\frac{1}{2} p(p+1) \right)^i.$$

By using Lucas' theorem, in 1992 R. Garfield and H.S. Wilf [44, Theorem] proved the following result: *Let p be a prime, let a be a primitive root modulo p , and let n be a nonnegative integer with the p -adic expansion $n = \sum_{i=0}^s n_i p^i$. Denote by $l_j(n)$ the number of j 's occurring among n_0, n_1, \dots, n_s ($j = 0, 1, \dots, p-1$). Further, for each $i \in \{0, 1, \dots, p-2\}$ let $r_i(n)$ be the number of integers k with $0 \leq k \leq n$, for which $\binom{n}{k} \equiv a^i(\bmod p)$, and let $R_n(X) = \sum_{i=0}^{p-2} r_i(n) X^i$ be their generating function. Then*

$$(107) \quad R_n(X) \equiv \prod_{j=1}^{p-1} R_j(X)^{l_j(n)} \pmod{X^{p-1} - 1}.$$

In 1990 R. Bollinger and C. Burchard [17] considered the extended pascal's triangles which arise, by analogy with the ordinary Pascal's triangle as the (left-justified) arrays of the coefficients in the expansion $(1 + x + x^2 + \cdots + x^{k-1})^n$. That is, the array T_k has in row n , column m , the number

$C_k(n, m)$ defined for $k, n, m \geq 0$ by the expansion

$$(1 + x + x^2 + \cdots + x^{k-1})^n = \sum_{m=0}^{(k-1)n} C_k(n, m) x^m,$$

It is noticed in [17, the property d) on page 199] that

$$C_k(n, m) = \sum_j (-1)^j \binom{n}{j} \binom{n-1+m-kj}{n-1},$$

and hence, $C_2(n, m) = \binom{n}{m}$. Accordingly, T_2 is the Pascal's triangle.

R. Bollinger and C. Burchard [17, Theorem 1] applied Lucas' theorem to the Pascal's triangle, proving that *if p is a prime, and if $n = n_0 + n_1p + \cdots + n_sp^s$ and $m = m_0 + m_1p + \cdots + m_sp^l$ are the p -adic expansions of n and m , then*

$$(108) \quad C_k(n, m) \equiv \sum_{r_0, \dots, r_s} \prod_{i=0}^s C_k(n_i, r_i) \pmod{p},$$

where the sum is taken over all $(s+1)$ -tuples (r_0, r_1, \dots, r_s) such that *i) $m = r_0 + r_1p + \cdots + r_sp^s$ and ii) $0 \leq r_i \leq (k-1)n_i$ for each $i = 0, 1, \dots, s$; if m is not representable in this form, then certainly $C_k(n, m) \equiv 0 \pmod{p}$.*

6.2. Another applications of Lucas's theorem. By using Kummer's theorem and Lucas' theorem, in 2007 K. Dilcher [34, Theorem 2] derived an alternating sum analog to a special case to an 1876 congruence of Hermite [57] (also see [36, Chapter IX, p. 271]) as follows. *Let p be an odd prime and let q be a positive integer. Then*

$$(109) \quad \sum_{j=0}^{\lfloor q/2 \rfloor} \binom{q(p-1)}{2j(p-1)} \equiv \begin{cases} 1 \pmod{p} & \text{if } q \text{ is odd;} \\ 2 \pmod{p} & \text{if } q \text{ is even and } q \not\equiv 0 \pmod{p+1}; \\ \frac{3}{2} \pmod{p} & \text{if } p+1 \mid q. \end{cases}$$

By using Lucas' theorem, in 2009 the author of this article proved the following result [92, Theorem]. *If $d, q > 1$ are integers such that*

$$(110) \quad \binom{nd}{md} \equiv \binom{n}{m} \pmod{q}$$

for every pair of integers $n \geq m \geq 0$, then d and q are powers of the same prime p .

Remark 36. Observe that the above result may be considered as a partial converse theorem of the congruence (5) of Subsection 2.1. \square

In 2010 M.P. Saikia and J. Vogrinc [116, Theorem 2.1] (see also [81, Theorem 1.2 and its proof]) proved that *a positive integer $p > 1$ is a prime if and only if*

$$(111) \quad \binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p}$$

for every nonnegative integer n .

By using Lucas' theorem, in 2013 the author of this article [99, Theorem 1.1] generalized Babbage's criterion for primality given in 1819 by Babbage [9] (also see [52, Section 4]). Lucas' theorem is also applied in a recent author's note [101, Theorem 1] in order to prove the following result: *If $n > 1$ and $q > 1$ are integers such that*

$$\binom{n-1}{k} \equiv (-1)^k \pmod{q}$$

for every integer $k \in \{0, 1, \dots, n-1\}$, then q is a prime and n is a power of q .

Definition (see, e.g., [2]). Let p be a prime. We say that the sequence of rational numbers $(a_n)_{n \geq 0}$ has the *p -Lucas property* (or that the sequence $(a_n)_{n \geq 0}$ is *p -Lucas*) if the denominators of all the a_n 's are not divisible by p , and if for all $n \geq 0$ and for all $j \in \{0, 1, \dots, p-1\}$ it holds

$$(112) \quad a_{pn+j} \equiv a_n a_j \pmod{p}. \quad \square$$

Clearly, the sequence of rational numbers $(a_n)_{n \geq 0}$ has the p -Lucas property if and only if

$$(113) \quad a_n \equiv \prod_{i=0}^s a_{n_i} \pmod{p},$$

for every positive integer n with the p -adic expansion $n = n_0 + n_1 p + \dots + n_s p^s$ such that $0 \leq n_i \leq p-1$ for all $i = 0, 1, \dots, s$. Furthermore, the integer sequence $(a_n)_{n \geq 0}$ has the Lucas property if and only if $(a_n)_{n \geq 0}$ has the p -Lucas property for every prime p .

In what follows, we will consider sequences $(a_n)_{n \geq 0}$ having the p -Lucas property for infinitely many primes p . As noticed in [2, Remarks 1], such a sequence is either 0 or it satisfies $a_0 = 1$. \square

For a positive integer t consider *the formal power series*

$$\sum_{n=0}^{\infty} \binom{2n}{n}^t X^n.$$

It is known that the above formal power series is transcendental over $\mathbb{Q}(X)$ when $t \geq 2$. This is due in 1980 to Stanley [125], and independently in 1987 to Flajolet [40] and in 1989 to C.F. Woodcock and H. Sharif [143]. While

Stanley and Flajolet used analytic methods and studied the asymptotics of the coefficients of this series, Woodcock and Sharif gave a purely algebraic proof. Their basic idea is to reduce this series modulo a prime p , and to use the p -Lucas property for central binomial coefficients: if $n = \sum_{i=0}^s n_i$ is the base p expansion of a positive integer n , then ([89]; cf. (58) of Subsection 4.1)

$$(114) \quad \binom{2n}{n} \equiv \prod_{i=0}^s \binom{2n_i}{n_i} \pmod{p}.$$

Namely, a proof of Woodcock and Sharif [143] is based on the following congruence which follows from Lucas' theorem:

$$F_t^{p-1}(X) \equiv \left(\sum_{i=0}^{(p-1)/2} \binom{2i}{i} X^i \right)^{-1} \pmod{p}.$$

In 1998 J.-P. Allouche, D. Gouyou-Beauchamps and G. Skordev [2] generalized the method of Woodcock and Sharif to characterize all formal power series that have the p -Lucas property for “many” primes p , and that are furthermore algebraic over $\mathbb{Q}(X)$. Namely, they proved the following result [2, Theorem 1]: *Let s be an integer ≥ 2 . Define $s' = s$ if s is even, and $s' = 2s$ if s is odd. Let $F(X) = \sum_{n=0}^{\infty} a_n X^n$ be a nonzero formal power series with coefficients in \mathbb{Q} . Then the following conditions are equivalent:*

- (i) *The sequence $(a_n)_{n \geq 0}$ has the p -Lucas property for all large primes p such that $p \equiv 1 \pmod{s}$, and the formal power series $F(X)$ is algebraic over $\mathbb{Q}(X)$.*
- (ii) *There exists a polynomial $P(X)$ in $\mathbb{Q}[X]$ of degree at most s' , with $P(0) = 1$, such that $F(X) = (P(X))^{-1/s'}$.*

If s is odd, and if the number s' is replaced by s in the statement (ii), we still have (ii) implies (i), but the converse is not necessarily true.

Furthermore, when the number s is equal to 2, in 1999 Allouche [1, Theorem 6.4] proved the following result (cf. [2, Theorem 2]): *Let $(a_n)_{n \geq 0}$ be a nonzero sequence of rational numbers. Then the following assertions are equivalent.*

- (i) *The sequence $(a_n)_{n \geq 0}$ has the p -Lucas property for all large primes p , and the series $F(X) = \sum_{n=0}^{\infty} a_n X^n$ is algebraic over $\mathbb{Q}(X)$.*
- (ii) *For all large primes p the sequence $(a_n)_{n \geq 0}$ has the p -Lucas property, and the degree d_p of the series $\sum_{n=0}^{\infty} (a_n \pmod{p}) X^n$ (that is necessarily algebraic over $\mathbb{F}_p(X)$ from the p -Lucas property) is bounded independently of p .*
- (iii) *There exists a polynomial $P(X)$ in $\mathbb{Q}[X]$ of degree at most 2, with $P(0) = 1$, such that $F(X) = \sum_{n=0}^{\infty} a_n X^n = (P(X))^{-1/2}$.*

Remark 37. In 2013 É. Delaygue [31, Subsection 1.2] considered the notion of p -Lucas property to a \mathbb{Z}_p -valued family $A = (A(\mathbf{n}))_{\mathbf{n} \in \mathbb{N}^d}$, where p is a prime, \mathbb{Z}_p is the ring of p -adic integers and d is a positive integer. We say that A satisfies the p -Lucas property if and only if, for all $\mathbf{v} \in \{0, 1, \dots, p-1\}^d$ and all $\mathbf{n} \in \mathbb{N}^d$, we have

$$A(\mathbf{v} + \mathbf{n}p) \equiv A(\mathbf{v})A(\mathbf{n}) \pmod{p\mathbb{Z}_p}.$$

Delaygue [31, Theorem 3] established an effective criterion for a sequence of factorial ratios to satisfy the p -Lucas property for almost all primes p . \square

REFERENCES

- [1] J.-P. Allouche, Transcendence of formal power series with rational coefficients, *Theoret. Comput. Sci.* **218** (1999), 143–160.
- [2] J.-P. Allouche, D. Gouyou-Beauchamps and G. Skordev, Transcendence of binomial and Lucas' formal power series, *J. Algebra* **210** (1998), 577–592.
- [3] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen and G. Skordev, *Discrete Appl. Math.* **66** (1996), 1–22.
- [4] J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, New York/Cambridge, 2003.
- [5] T. Amdeberhan and R. Stanley, Polynomial coefficient enumeration, <http://arXiv.org/abs/0811.3652v1>, 2008.
- [6] P.G. Anderson, A.T. Benjamin and J.A. Rouse, Combinatorial proofs of Fermat's, Lucas's, and Wilson's theorems, *Amer. Math. Monthly* **112** (2005), 266–268.
- [7] H. Anton, Die Elferprobe und die Proben für die Modul Neun, 9, 13 and 101, Dreizehn und Hunderteins. Für Volksund Mittelschulen, *Archiv Math. Physik* **49** (1869), 241–308.
- [8] R. Apéry, Irrationalité de $\zeta(2)$ and $\zeta(3)$, *Astérisque* **61** (1979), 11–13.
- [9] C. Babbage, Demonstration of a theorem relating to prime numbers, *Edinburgh Philosophical J.* **1** (1819), 46–49.
- [10] D.F. Bailey, Two p^3 variations of Lucas' theorem, *J. Number Theory* **35** (1990), 208–215.
- [11] D.F. Bailey, Some binomial coefficient congruences, *Appl. Math. Letters* **4**, No. 4 (1991), 1–5.
- [12] D.F. Bailey, More binomial coefficient congruences, *Fibonacci Quart.* **30**, No. 2 (1992), 121–125.
- [13] A.T. Benjamin and J.J. Quinn, *Proofs That Really Count, The Art of Combinatorial proofs*, Mathematical Association of America, Providence, 2003.
- [14] D. Berend and N. Kriger, On some questions of Razpet regarding binomial coefficients, *Discrete Math.* **260** (2003), 177–182.
- [15] D. Berend and J.E. Harmse, On some arithmetical properties of middle binomial coefficients, *Acta Arith.* **84** (1998), 31–41.
- [16] A. Bès, On Pascal triangles modulo a prime power, *Ann. Pure Appl. Logic* **89** (1997), 17–35.
- [17] R.C. Bollinger and C.L. Burchard, Lucas' theorem and some related results for extended Pascal triangles, *Amer. Math. Monthly* **97** (1990), 198–204.
- [18] J. Boulanger and J.-L. Chabert, An extension of the Lucas theorem, *Acta Arith.* **96** (2001), 303–312.

- [19] V. Brun, J.O. Stubban, J.E. Fjeldstad, R. Tambs Lyche, K.E. Aubert, W. Ljunggren and E. Jacobsthal, *On the divisibility of the difference between two binomial coefficients*. Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, 42–54. Johan Grundt Tanums Forlag, Oslo, 1952.
- [20] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys Monogr. **48**, Providence, 1997.
- [21] N.J. Calkin, Factors sums of powers of binomial coefficients, *Acta Arithmetica* **86** (1998), 17–26.
- [22] L. Carlitz, The coefficients of the reciprocal of $J_0(x)$, *Arch. Math.* **6** (1955), 121–127.
- [23] L. Carlitz, The number of binomial coefficients divisible by a fixed power of a prime, *Rend. Circ. Mat. Palermo* **16**, no. 2 (1967), 299–320.
- [24] R.D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913–1914), 30–70.
- [25] M. Chamberland and K. Dilcher, A binomial sum related to Wolstenholme's theorem, *J. Number Theory* **129** (2009), 2659–2672.
- [26] L.E. Clarke, Problem 4704, *Amer. Math. Monthly* **63** (1956), p. 584; Solution, *ibid* **64** (1957), 597–598.
- [27] H. Cohen, *Number Theory. Volume II: Analytic and Modern Tools*, Springer, 2007.
- [28] K.S. Davis and W.A. Webb, Pascal's triangle modulo 4, *Fibonacci Quart.* **29**, no. 1 (1991), 79–83.
- [29] K.S. Davis and W.A. Webb, Lucas' theorem for prime powers, *European J. Combin.* **11** (1990), 229–233.
- [30] K.S. Davis and W.A. Webb, A binomial coefficient congruence modulo prime powers, *J. Number Theory* **43** (1993), 20–23.
- [31] É. Delaygue, Arithmetic properties of Apéry-like numbers, [arXiv:1310.4131v1 \[math.NT\]](https://arxiv.org/abs/1310.4131v1), 2013.
- [32] J. Désarménien, Un analogue des congruences de Kummer pour les q -nombres d'Euler, *European J. Combin.* **3** (1982), 19–28.
- [33] E. Deutsch and B.E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, *J. Number Theory* **117** (2006), 191–215.
- [34] K. Dilcher, Congruences for a class of alternating lacunary sums of binomial coefficients, *J. Integer Sequences* **10** (2007), Article 07.10.1.
- [35] D. Djukić, V. Janković, I. Matić and N. Petrović, *The IMO compendium: A Collection of Problems Suggested for the International Mathematical Olympiads: 1959–2009*, Second edition, Springer-Verlag, New York, 2009.
- [36] L.E. Dickson, *The History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1966.
- [37] S.-P. Eu, S.-C. Liu and Y.-N. Yeh, On the congruences of some combinatorial numbers, *Stud. Appl. Math.* **116** (2006), 135–144.
- [38] T.J. Evans, On some generalizations of Fermat's, Lucas's and Wilson's theorem, *Ars Combinatoria* **79** (2005), 189–194.
- [39] N.J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (1947), 589–592.
- [40] P. Flajolet, Analytic models and ambiguity of context-free languages, *Theoret. Comput. Sci.* **49** (1987), 283–309.
- [41] G. Fontené, Généralisation d'une formule connue, *Nouvelles Annales de Mathématiques* **15**, no. 4 (1915), p. 112.

- [42] R.D. Fray, Congruence properties of ordinary and q -binomial coefficients, *Duke Math. J.* **34** (1967), 467–480.
- [43] R.D. Fray, D.P. Roselle, Weighted lattice paths, *Pacific J. Math.* **37**, no. 1 (1971), 85–96.
- [44] R. Garfield and H. Wilf, The distribution of the binomial coefficients modulo p , *J. Number Theory* **41** (1992), 1–5.
- [45] C.F. Gauss, *Disquisitiones Arithmeticae*, Fleischer, Leipzig, 1801.
- [46] C.F. Gauss, Summatio quarumdam serierum singularium, *Commentationes societatis regiae scientiarum Gottingensis recentiores* **1** (1808), 147–186. Reprinted in Gauss's *Werke* **2** (1863), 9–45.
- [47] I. Gessel, Some congruences for Apéry numbers, *J. Number Theory* **14** (1982), 362–368.
- [48] J.W.L. Glaisher, On the residues of a binomial-theorem coefficients, *Q. J. Pure Appl. Math.* **30** (1899), 150–156.
- [49] J.W.L. Glaisher, On the residues of the sums of products of the first $p - 1$ numbers, and their powers, to modulus p^2 or p^3 , *Q. J. Math.* **31** (1900), 321–353.
- [50] H.W. Gould, The Bracket function and Fonténe-Ward generalized binomial coefficients with applications to Fibonomial coefficients, *Fibonacci Quart.* **7**, no. 1 (1969), 23–40.
- [51] A. Granville, Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle, *Amer. Math. Monthly* **99** (1992), 318–331.
- [52] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, in Organic Mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, American Mathematical Society, Providence, RI, 1997, 253–275.
- [53] R.K. Guy, *Unsolved problems in Number Theory*, Third edition, Springer-Verlag, New York, 2004.
- [54] P.W. Haggard and J.O. Kiltinen, Binomial expansions modulo prime powers, *Internat. J. Math. & Math. Sci.* **3**, No. 2 (1980), 397–400.
- [55] M. Hausner, Applications of a simple of counting technique, *Amer. Math. Monthly* **90** (1983), 127–129.
- [56] C. Helou and G. Terjanian, On Wolstenholme's theorem and its converse, *J. Number Theory* **128** (2008), 475–499.
- [57] Ch. Hermite, Extrait d'une lettre à M. Borchardt, *J. Reine Angew. Math.* **81** (1876), 93–95.
- [58] E. Hexel and H. Sachs, Counting residues modulo a prime in Pascal's triangle, *Indian J. Math.* **20** (1978), 91–105.
- [59] V.E. Hoggatt, Fibonacci numbers and generalized binomial coefficients, *Fibonacci Quart.* **5**, no. 4 (1967), 383–400.
- [60] J.M. Holte, A Lucas-type theorem for Fibonomial-coefficient residues, *Fibonacci Quart.* **32**, no. 1 (1994), 60–68.
- [61] J.M. Holte, Residues of generalized binomial coefficients modulo a prime, *Fibonacci Quart.* **38**, no. 3 (2000), 227–238.
- [62] J.M. Holte, Fractal dimension of arithmetical structures of generalized binomial coefficients modulo a prime, *Fibonacci Quart.* **44**, no. 1 (2006), 46–58.
- [63] P. Horak and L. Skula, A characterization of the second-order strong divisibility sequences, *Fibonacci Quart.* **23**, no. 2 (1985), 126–132.
- [64] F.T. Howard, The number of binomial coefficients divisible by a fixed power of 2, *Proc. Amer. Math. Soc.* **29** (1971), 236–242.

- [65] F.T. Howard, The number of binomial coefficients divisible by a fixed power of a prime, *Proc. Amer. Math. Soc.* **37** (1973), 358–362.
- [66] F.T. Howard, The reciprocal of the Bessel function $J_k(z)$, *Fibonacci Quart.* **25**, no. 4 (1987), 304–311.
- [67] F.T. Howard, Congruences for the Stirling numbers and associated Stirling numbers, *Acta Arith.* **55** (1990), 29–41.
- [68] H. Hu, On Lucas v -triangles, *Fibonacci Quart.* **40**, no. 4 (2002), 290–294.
- [69] H. Hu and Z.-W. Sun, An extension of Lucas' theorem *Proc. Amer. Math. Soc.* **129** (2001), 3471–3478.
- [70] J.G. Huard, B.K. Spearman and K.S. Williams, On Pascal's triangle modulo p^2 , *Colloq. Mathem.* **74**, no. 1 (1997), 157–165.
- [71] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.
- [72] Y. Jin, Z.-J. Lu and A.L. Schmidt, On recurrences for sums of powers of binomial coefficients, *J. Number Theory* **128** (2008), 2784–2794.
- [73] J.P. Jones and Y.V. Matijasevič, Register machine proof of the theorem on exponential diophantine representation of enumerable sets, *J. Symbolic Logic* **49** (1984), 818–829.
- [74] J.P. Jones and Y.V. Matijasevič, Proof of recursive unsolvability of Hilbert's tenth problem, *Amer. Math. Monthly* **98**, no. 8 (1991), 689–709.
- [75] G.S. Kazandzidis, Congruences on the binomial coefficients, *Bull. Soc. Math. Grèce (N.S.)* **9** (fasc. 1) (1968), 1–12.
- [76] W.A. Kimball and W.A. Webb, Congruence properties of Fibonacci numbers and Fibonacci coefficients, in *Applications of Fibonacci numbers*, vol. 5, Kluwer, Dordrecht, 1993.
- [77] W.A. Kimball and W.A. Webb, Some congruences for generalized binomial coefficients, *Rocky Mountain J. Math.* **25** (1995), 1079–1085.
- [78] W.A. Kimball and W.A. Webb, A congruence for Fibonacci coefficients modulo p^3 , *Fibonacci Quart.* **33**, no. 4 (1995), 290–297.
- [79] D.E. Knuth and H.S. Wilf, The power of a prime that divides a generalized binomial coefficient, *J. Reine Angew. Math.* **396** (1989), 212–219.
- [80] E.E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146.
- [81] A. Laugier and M.P. Saikia, A characterization of a prime p from the binomial coefficient $\binom{n}{p}$ with $n > p + 1$ a natural number,
- [82] A. Laugier and M.P. Saikia, A new proof of Lucas' Theorem, *Notes on Number Theory and Discrete Mathematics* **18**, no. 4 (2012), 1–6; also available at [arXiv:1301.4250v1 \[math.NT\]](https://arxiv.org/abs/1301.4250v1), 2013.
- [83] S.-C. Liu and J.C.-C. Yeh, Catalan numbers modulo 2^k , *J. Integer Sequences* **13** (2010), Article 10.5.4.
- [84] C.T. Long and N. Woo, On bases for the set of integers, *Duke Math. J.* **38** (1971), 583–590.
- [85] A.D. Loveless, *Extensions in the Theory of Lucas and Lehmer Pseudoprimes*, Ph.D. Thesis, Washington State University, 2005, available at <http://www.dissertations.wsu.edu>.
- [86] É. Lucas, Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques, suivant un module premier, *Bull. Soc. Math. France* **6** (1877–1878), 49–54.

- [87] É. Lucas, Théorie des fonctions numérique simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240.
- [88] R.A. Macleod, Generalization of a result of E. Lucas, *Canad. Math. Bull.* **31**, no. 1, 1988, 95–98.
- [89] R.J. McIntosh, A generalization of a congruential property of Lucas, *Amer. Math. Monthly* **99**, No.3 (1992), 231–238.
- [90] R.J. McIntosh, On the converse of Wolstenholme's Theorem, *Acta Arith.* **71** (1995), 381–389.
- [91] R.J. McIntosh and E.L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, *Math. Comp.* **76** (2007), 2087–2094.
- [92] R. Meštrović, A Note on the Congruence $\binom{nd}{md} \equiv \binom{n}{m}(\text{mod } q)$, *Amer. Math. Monthly* **116** (2009), 75–77.
- [93] R. Meštrović, Wolstenholme's theorem: its generalizations and extensions in the last hundred and fifty years (1862–2012); preprint arXiv:1111.3057v2 [math.NT], 2011.
- [94] R. Meštrović, Congruences for Wolstenholme primes, accepted for publication in *Czechoslovak Math. J.*; preprint arXiv:1108.4178v1 [math.NT], 2011.
- [95] R. Meštrović, On the mod p^7 determination of $\binom{2p-1}{p-1}$, *Rocky Mount. J. Math.* **44** (2014), 633–548; preprint arXiv:1108.1174v1 [math.NT], 2011.
- [96] R. Meštrović, A note on the congruence $\binom{np^k}{mp^k} \equiv \binom{n}{m}(\text{mod } p^r)$, *Czechoslovak Math. J.* **62** (2012), No. 1, 59–65.
- [97] R. Meštrović, Variations of Lucas' theorem modulo prime powers, 11 pages; preprint arXiv:1301.0252 [math.NT], 2012.
- [98] R. Meštrović, A Lucas' type theorem modulo prime powers, *Fibonacci Quart.* **51**, no. 2 (2013), 142–146; preprint arXiv:1301.0251 [math.NT], 2012.
- [99] R. Meštrović, An extension of Babbage's criterion for primality, *Math. Slovaca* **63**, no. 6 (2013), 1179–1182.
- [100] R. Meštrović, Some Wolstenholme type congruences, *Math. Appl.* **2** (2013), 35–42.
- [101] R. Meštrović, A primality criterion based on a Lucas' congruence, arXiv:1407.7894v1 [math.NT], 2014.
- [102] T.D. Noe, On the divisibility of generalized central trinomial coefficients, *J. Integer Sequences* **9** (2006), Article 06.2.7.
- [103] A. Nowicki, Podróże po Imperium Liczb. Część 11. Silnie i Symbole Newtona (Rozdział 7), University of Torun, Poland, 2011; also available at <http://www.mat.uni.torun.pl/~anow>.
- [104] G. Olive, Generalized powers, *Amer. Math. Monthly* **72** (1965), 619–627.
- [105] H. Pan, On divisibility of sums of Apéry polynomials; preprint arXiv:1108.1546v1 [math.NT], 2011.
- [106] H. Pan, A congruence of Lucas' type *Discrete Math.* **288** (2004), 173–175.
- [107] R. Peele, A.J. Radcliffe and H.S. Wilf, Congruence problems involving Stirling numbers of the first kind, *Fibonacci Quart.* **31**, no. 1 (1993), 27–34.
- [108] P.A. Piza, Solution of Problem 4704, *Amer. Math. Monthly* **64**, No. 8 (1957), 597–598.
- [109] M. Prunescu, Sign-reductions, p -adic valuations, binomial coefficients modulo p^k and triangular symmetries, available at <http://home.mathematik.uni-freiburg.de>.
- [110] M. Razpet, Divisibility properties of some number arrays, *Ars Combin.* **30** (1990), 308–318.

- [111] M. Razpet, On divisibility of binomial coefficients, *Discrete Math.* **135** (1994), 377–379.
- [112] M. Razpet, The Lucas property of a number array, *Discrete Math.* **248** (2002), 157–168.
- [113] J.B. Roberts, On binomial coefficient residues, *Canad. J. Math.* **9** (1957), 363–370.
- [114] E. Rowland, The number of nonzero binomial coefficients modulo p^α ; preprint [arXiv:1001.1783v3](https://arxiv.org/abs/1001.1783v3) [math.NT], 2011.
- [115] E. Rowland and R. Yassawi, Automatic congruences for diagonals of rational functions; preprint [arXiv:1310.8635v2](https://arxiv.org/abs/1310.8635v2) [math.NT], 2014.
- [116] M.P. Saikia and J. Vogrin, A simple number theoretic result, *J. Assam Academy of Math.* **3** (2010), 91–96.
- [117] K. Samol and D. van Straten, Dwork congruences and reflexive polytopes; preprint [arXiv:0911.0797](https://arxiv.org/abs/0911.0797) [math.NT], 2009.
- [118] R. Sánchez-Peregrino, The Lucas congruences for Stirling numbers of the second kind, *Acta Arith.* **94** (2000), 41–52.
- [119] J. Sándor and B. Crstici, *Handbook of Number Theory II*, Kluwer Academic Publisher, vol. 198, Dordrecht/Boston/London, 2004.
- [120] L.-L. Shi, Congruences for Lucas u -nomial coefficients modulo p^3 , *Rocky Mountain J. Math.* **37** (2007), 1027–1042.
- [121] D. Singmaster, Notes on binomial coefficients I- a generalization of Lucas' congruence *J. London Math. Soc.* **8**, no. 2 (1974), 545–548.
- [122] D. Singmaster, *Divisibility of binomial and multinomial coefficients by primes and prime powers*, 18th Anniversary Volume of the Fibonacci Association, pp. 98–113, 1980.
- [123] C.C. Siong, A simple proof of Ljunggren's binomial congruence, *Amer. Math. Monthly* **121**, No. 2 (2014), 162–164.
- [124] N.J.A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, <http://www.research.att.com/~njas/sequences/seis.html>.
- [125] R.P. Stanley, Differentiability finite power series, *European J. Combin.* **1** (1980), 175–188.
- [126] R.P. Stanley, *Enumerative Combinatorics*, Vol. I, Cambridge University Press, 1997.
- [127] J. Stirling, *Methodus differentialis, sive tractatus de summatione et interpolatione serierum infinitarum*, Londini, 1730.
- [128] V. Strehl, Zum q -Analogon der Kongruenz von Lucas, in *Séminaire Lotharingien de Combin.*, 5ème Session, 102–104, Strasbourg, 1982.
- [129] Z.W. Sun and D.M. Davis, Combinatorial congruences modulo prime powers, *Trans. Amer. Math. Soc.* **359** (2007), 5525–5553.
- [130] Z.-W. Sun and D. Wan, Lucas type congruences for cyclotomic ψ -coefficients, *Int. J. Number Theory* **4** (2008), no. 2, 155–170.
- [131] M. Sved, Divisibility-with visibility, *Math. Intelligencer* **10**, No. 2 (1988), 56–64.
- [132] M. Sved and R.J. Clarke, King's walk on the infinite chessboard, *Australasian J. Math.* **2** (1990), 191–215.
- [133] The William Lowell Putnam Mathematical Competition, Problem A-5, *Amer. Math. Monthly* **86** (1979), 171–173.
- [134] R.F. Torretto and J.A. Fuchs, Generalized binomial coefficients, *Fibonacci Quart.* **2** (1964), 296–302.
- [135] E.R. Tou, *Residues of generalized binomial coefficients modulo a product of primes*, senior thesis, Spring (2002), Department of Mathematics and

- Computer Science, Gustavus Adolphus College, St. Peter, MN; available at <http://sites.google.com/site/erikrtou/home>.
- [136] M. Ward, A Calculus of Sequences, *American J. Math.* **58** (1936), 255–266.
 - [137] D.L. Wells, *Lucas theorem for generalized binomial coefficients*, Ph.D. Thesis, Washington State University, 1992.
 - [138] D.L. Wells, Lucas' theorem for generalized binomial coefficients, *AMS Abstracts* **14** (1993), p. 32.
 - [139] D.L. Wells, The Fibonacci and Lucas triangles modulo 2, *Fibonacci Quart.* **32**, no. 2 (1994), 111–123.
 - [140] B. Wilson, Fibonacci triangles modulo p , *Fibonacci Quart.* **36**, no. 3 (1998), 194–203.
 - [141] S. Wolfram, Geometry of binomial coefficients, *Amer. Math. Monthly* **91** (1984), 566–571.
 - [142] J. Wolstenholme, On certain properties of prime numbers, *Quart. J. Pure Appl. Math.* **5** (1862), 35–39.
 - [143] C.F. Woodcock and H. Sharif, On the transcendence of certain series, *J. Algebra* **121** (1989), 364–369.
 - [144] N. Zaheer [144] A generalization of Lucas' theorem to vector spaces, *Int. J. Math. and Math. Sci.* **16** (1993), 267–276.
 - [145] J. Zhao, Bernoulli Numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem, *J. Number Theory* **123** (2007), 18–26.
 - [146] J. Zhao, Wolstenholme type theorem for multiple harmonic sum, *Int. J. of Number Theory* **4** (2008), 73–106.

APPENDIX

List of references and related Lucas type congruences from this article (arranged by year of publication)

- [9, 1819] Charles Babbage (also see [52, Introduction] or [36, page 271]) - (19), p. 10.
- [142, 1862] Joseph Wolstenholme - (20), p. 10.
- [7, 1869] H. Anton (also see [36, p. 271]) - (2), p. 5)
- [86, 1878], [87, 1878; Section XXI, pp. 229–230], É. Lucas (Lucas' theorem) - the congruences (1) and (3), p. 5.
- [49, 1900; p. 323] J.W.L. Glaisher (also see [103, the congruence 7.1.5] and [93, Section 6]) - (21), p. 10.
- [19, 1949] W. Ljunggren (also see [10, Theorem 4], [52], [126, Problem 1.6 (d)] and [123]) - (22), p. 11.
- [19, 1952] E. Jacobsthal (also see [52]) - (23), p. 11.
- [22, 1955] L. Carlitz - (70), p. 25.
- [26, 1956] L.E. Clarke and [108, 1957], P.A. Piza - (7), p. 8.
- [104, 1965] G. Olive (also see [119, Chapter 5, p. 506], [32], [128] [105, Lemma 2.1]) - (101), p. 36.
- [47, 1982; Theorem 1] I. Gessel - (52), p. 19.
- [66, 1987; Theorem 1] F.T. Howard - (69), p. 25.

- [66, 1987; p. 306, Corollary and Theorem 2] F.T. Howard - (71) and (72), p. 25.
- [88, 1988; Theorem 2], R.A. Macleod - (43), p. 16.
- [131, 1988; p. 61, Theorem] M. Sved - (64), p. 23.
- [131, 1988; p. 60, Theorem] M. Sved - (80), p. 31.
- [10, 1990; Theorem 3] D.F. Bailey - (31), p. 12.
- [10, 1990; Theorem 5] D.F. Bailey - (32), p. 13.
- [17, 1990; Theorem 1] R. Bollinger and C. Burchard - (108), p. 40.
- [11, 1991; Theorem 4] D.F. Bailey - (26), p. 11.
- [11, 1991; Theorem 5] D.F. Bailey - (27), p. 12.
- [29, 1991; Theorem 3] K. Davis and W. Webb (also see [85, p. 88, Theorem 5.1.2] and [15, p. 34, congruence (2.2)]) - (37), p. 14.
- [12, 1992; Theorem 5] D.F. Bailey (also see [98, Corollary 1.2]) - (28) and (29), p. 12.
- [51, 1992; Proposition 2] A. Granville - (34), p. 13.
- [89, 1992] R.J. McIntosh - (114), p. 42.
- [137, 1992; Theorem 2] (also see [138] and [61, Section 7]) D.L. Wells - (84) and (85), p. 32.
- [30, 1993; Theorem 3] K. Davis and W. Webb (also see [51, Proposition 2]) - (40), p. 15.
- [30, 1993; Corollary 1] K. Davis and W. Webb - (41), p. 15.
- [30, 1993; Corollary 1] K. Davis and W. Webb (also see [97, Theorem]) - (42), p. 15.
- [76, 1993] W.A. Kimball and W.A. Webb (also see [120, p. 1029]) - (89) and (90), p. 33.
- [107, 1993; Proposition 2.1] R. Peele, A.J. Radcliffe and H.S. Wilf - (68), p. 24.
- [60, 1994; p. 60] J.M. Holte (also see [61, 1994; p. 227]) - (14) and (15), p. 9.
- [111, 1994; p. 378] M. Razpet - (54), p. 20.
- [139, 1994; Theorem 2] D.L. Wells - (79), p. 30.
- [52, 1995; Section 6, the congruence (24)] A. Granville - (16), p. 9.
- [52, 1995; Theorem 1] A. Granville - (33), p. 13.
- [77, 1995; Theorems 1 and 3] W.A. Kimball and W.A. Webb - (91) and (92), p. 34.
- [77, 1995; Corollaries 2 and 4] W.A. Kimball and W.A. Webb - (93) and (94), p. 34.
- [77, 1995; Theorem 5] W.A. Kimball and W.A. Webb - (95), p. 34.
- [78, 1995; Theorem] W.A. Kimball and W.A. Webb - (99), p. 35.
- [21, 1998; Lemma 4] N.J. Calkin - (56), p. 20.
- [140, 1998] B. Wilson - (96) and (97), p. 34.
- [1, 1999; Proposition 7.1] J.-P. Allouche - (51), p. 18.
- [61, 2000; Theorem 1] J.M. Holte - (81), p. 31.
- [61, 2000; Theorem 3] J.M. Holte - (82) and (83), p. 32.
- [118, 2000; Proposition 3.1] R. Sánchez-Peregrino - (65) and (66), pp. 23–24.
- [118, 2000; Proposition 4.1] R. Sánchez-Peregrino - (67), p. 24.
- [18, 2001; Theorem 2.2] J. Boulanger and J.-L. Chabert - (76), p. 27.
- [69, 2001; Theorem] H. Hu and Z.-W. Sun - (86) and (87), pp. 32–33.

- [68, 2002; p. 291, Theorem] H. Hu - (88), p. 33.
- [112, 2002; Theorem 1] M. Razpet - (62), p. 22.
- [14, 2003; Theorem 5] D. Berend and N. Kriger - (55), p. 20.
- [106, 2004; Theorem 1] H. Pan - (63), p. 23.
- [38, 2005; Theorem 3] T.J. Evans - (17), p. 9.
- [33, 2006; Theorem 4.7] E. Deutsch and B.E. Sagan - (57), p. 21.
- [33, 2006; Theorem 4.4] E. Deutsch and B.E. Sagan - (58), p. 21.
- [120, 2007; Theorem 2] L.-L. Shi - (98), p. 35.
- [120, 2007; Theorem 1] L.-L. Shi - (100), p. 36.
- [129, 2007; Theorem 1.7] Z.-W. Sun and D.M. Davis - (75), p. 26.
- [56, 2008; the congruence (1) of Corollary on page 490] C. Helou and G. Terjanian (also see [27, Section 11.6, Corollary 11.6.22, p. 381]) - (24), p. 11.
- [72, 2008; (ii) of Lemma 2] Y. Jin, Z.-J. Lu and A.L. Schmidt - (53), p. 19.
- [130, 2008; Theorem 1.1] Z.-W. Sun and D. Wan - (74), p. 26.
- [25, 2009; Theorem 2.2] M. Chamberland and K. Dilcher - (59), p. 22.
- [25, 2009; Corollaries 2.1 and 2.2] M. Chamberland and K. Dilcher - (60) and (61), p. 22.
- [103, 2011; the congruences 7.3.1–7.33] A. Nowicki - (6), p. 7.
- [98, 2012; Theorem 1.1] R. Meštrović - (30), p. 12.
- [97, 2012; Theorem] R. Meštrović (also see [30, Corollary 1]) - (42), p. 15.
- [97, 2012; Proposition] R. Meštrović - (47) and (48), p. 17.
- [115, 2014; Section 5, Theorem 5.3] E. Rowland and R. Yassawi - (44), p. 16.

MARITIME FACULTY, UNIVERSITY OF MONTENEGRO, DOBROTA 36, 85330 KOTOR, MONTENEGRO

E-mail address: romeo@ac.me