LUCAS' THEOREM MODULO p^2

ERIC ROWLAND

ABSTRACT. Lucas' theorem describes how to reduce a binomial coefficient $\binom{a}{b}$ modulo p by breaking off the least significant digits of a and b in base p. We characterize the pairs of these digits for which Lucas' theorem holds modulo p^2. This characterization is naturally expressed using symmetries of Pascal's triangle.

1. Introduction

In 1878, Lucas [10] discovered a formula for computing the residue of a binomial coefficient modulo p, where p is a prime. Namely, if a and b are non-negative integers and $r, s \in \{0, 1, \dots, p-1\}$, then

$$\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p. \tag{1}$$

This congruence can also be written in terms of base-p representations. Let the base-p representations of a and b be $a_\ell \cdots a_1 a_0$ and $b_\ell \cdots b_1 b_0$, where we have made them the same length by padding the shorter representation with 0s if necessary. Iterating Congruence (1) gives

$$\binom{a}{b} \equiv \binom{a_\ell}{b_\ell} \cdots \binom{a_1}{b_1}\binom{a_0}{b_0} \mod p.$$

Several variants and generalizations of Lucas' theorem are known. Meštrović [12] gives an excellent survey. In particular, it is natural to ask for Lucas-type congruences modulo higher powers of p. We refer to a congruence of the form

$$\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p^\alpha \tag{2}$$

where $r, s \in \{0, 1, \dots, p-1\}$ as a *Lucas congruence*. Even prior to Lucas' work, Babbage [1] in 1819 showed that

$$\binom{2p-1}{p-1} \equiv 1 \mod p^2 \tag{3}$$

for all $p \geq 3$; this is a Lucas congruence where $a = 1$, $b = 0$, and $r = s = p-1$. In 1862, Wolstenholme [15] showed that Babbage's congruence holds modulo p^3 if $p \geq 5$. This was generalized by Glaisher [7, page 323] in 1900 to the Lucas congruence

$$\binom{pa-1}{p-1} \equiv 1 \mod p^3 \tag{4}$$

Date: June 20, 2020.

for all $a \geq 1$, again for $p \geq 5$. Since $a\binom{pa-1}{p-1} = \binom{pa}{p}$, this implies the Lucas congruence $\binom{pa}{p} \equiv a \mod p^3$, which itself can be generalized to

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p^3 \tag{5}$$

for $a \geq 0$, $b \geq 0$, and $p \geq 5$. Congruence (5) has been rediscovered several times. Granville [8] attributes it to Ljunggren [3]. Kazandzidis [9] and Bailey [2] also gave proofs. For $p = 2$ and $p = 3$, Congruence (5) does not hold modulo p^3 in general but does hold modulo p^2.

Each of the Lucas congruences (3)–(5) is uses a single pair (r, s) of digits. Some results of Bailey [2] allow the digits to be general. For every prime p, Bailey proved that

$$\binom{p^2a + r}{p^2b + s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$$

for all $r, s \in \{0, 1, \ldots, p-1\}$, $a \geq 0$, and $b \geq 0$. The equivalent form $\binom{p(pa)+r}{p(pb)+s} \equiv \binom{pa}{pb}\binom{r}{s} \mod p^2$ is a Lucas congruence. For $p \geq 5$, Bailey also proved

$$\binom{p^3a + r}{p^3b + s} \equiv \binom{a}{b}\binom{r}{s} \mod p^3.$$

These exponents 3 were subsequently increased by Davis and Webb [5]. A further extension was found by Zhao [16], and both Granville [8] and Davis and Webb [4] gave generalizations of Lucas' theorem modulo p^α, although these results depart from the form of Congruence (2).

In this article we address the following question. For which pairs (r, s) of base-p digits does the Lucas congruence

$$\binom{pa + r}{pb + s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$$

hold for all $a \geq 0$ and $b \geq 0$? The set of such pairs is our primary object of interest.

Notation. For each prime p, let

$$D(p) = \left\{(r, s) \in \{0, 1, \ldots, p-1\}^2 : \binom{pa + r}{pb + s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2 \text{ for all } a \geq 0, b \geq 0\right\}.$$

2. Description of the set $D(p)$

Congruence (5) implies that $D(p)$ is non-empty for each prime $p \geq 5$, since $(0, 0) \in D(p)$. Computer experiments suggest that $D(p)$ contains additional pairs as well. For example, we will show that $D(3) = \{(0, 0), (2, 0), (2, 2)\}$ and $D(7) = \{(0, 0), (4, 2), (6, 0), (6, 6)\}$. Plotting the elements of $D(p)$ as points in the plane reveals some structure. For example, the elements of $D(7)$ are highlighted in the following table of $\binom{r}{s}$ for $r, s \in \{0, 1, \ldots, 6\}$.

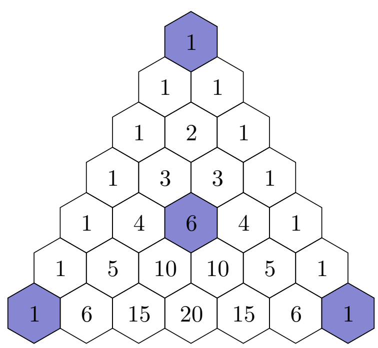
1	0	0	0	0	0	0
1	1	0	0	0	0	0
1	2	1	0	0	0	0
1	3	3	1	0	0	0
1	4	6	4	1	0	0
1	5	10	10	5	1	0
1	6	15	20	15	6	1

Our first result is that the zeros in this table do not correspond to points in $D(p)$.

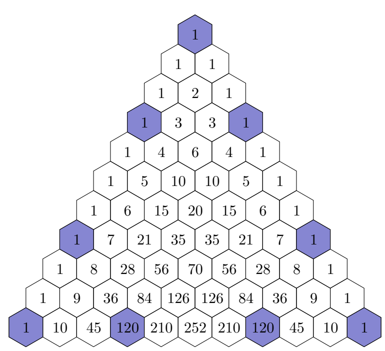
Proposition 1. *Let p be a prime. If $s > r$, then $(r, s) \notin D(p)$.*

Proof. Let $a = 1$ and $b = 0$. The binomial coefficient $\binom{pa+r}{pb+s} = \binom{p+r}{s} = \frac{(p+r)!}{s!(p+r-s)!}$ is divisible by p but not p^2. On the other hand, $\binom{a}{b}\binom{r}{s} = \binom{r}{s} = 0$ is divisible by p^2. Therefore $\binom{pa+r}{pb+s} \not\equiv \binom{a}{b}\binom{r}{s} \mod p^2$. □

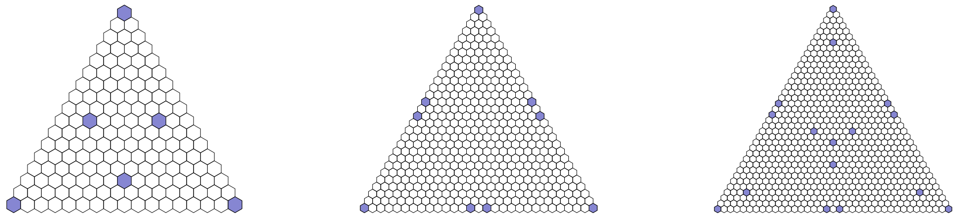
In light of Proposition 1, we omit points (r, s) where $s > r$ from the previous table. Then we shear the remaining triangle. This shows the symmetry of $D(7)$ more clearly.



For $p = 11$, the set $D(11)$ contains 9 pairs of digits, arranged as follows.



For $p = 17$, $p = 29$, and $p = 37$ the pairs in $D(p)$ appear in the following locations.

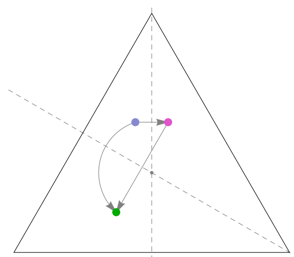


$p = 17$ $p = 29$ $p = 37$

These pictures suggest that $D(p)$ possesses the symmetries of the equilateral triangle!

Reflection symmetry about the vertical axis might have been expected, since Pascal's triangle also exhibits this symmetry. We establish this in Section 4. However, the rotational symmetry of $D(p)$ is less expected.

Counterclockwise rotation by $120°$ about the center of an equilateral triangle is equivalent to the composition of two reflections:



The first is reflection through the vertical altitude of the triangle. This reflection maps the point (r, s) to $(r, r - s)$. The second is reflection through the altitude passing through the lower right vertex. This reflection maps (r, s) to $(p-1-r+s, s)$, as can be seen by shearing so that this altitude is horizontal. Composing these reflections shows that the rotation maps (r, s) to $(p - 1 - s, r - s)$. Therefore the three binomial coefficients visited by the orbit of (r, s) under rotation by $120°$ are

$$\binom{r}{s}, \binom{p-1-s}{r-s}, \binom{p-1-r+s}{p-1-r},$$

the third of which is equal to $\binom{p-1-r+s}{s}$.

In general, these three binomial coefficients are not equal, nor are they congruent modulo p. However, we will show in Corollary 7 that they are congruent modulo p if we include the correct signs. In other words, binomial coefficients modulo p exhibit a rotational symmetry up to sign. Furthermore, the elements of $D(p)$ can be characterized as the pairs (r, s) for which this symmetry holds not just modulo p but modulo p^2 for the three binomial coefficients in the orbit of (r, s).

Theorem 2. *Let p be a prime, and let $r, s \in \{0, 1, \ldots, p - 1\}$. The congruence*

$$\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$$

holds for all $a \geq 0$ and $b \geq 0$ if and only if $s \leq r$ and

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \equiv (-1)^{s}\binom{p-1-r+s}{s} \mod p^2. \tag{6}$$

In particular, if $p \equiv 1 \mod 3$ then the geometric center of the triangle has integer coordinates, namely $r = \frac{2}{3}(p-1)$ and $s = \frac{1}{3}(p-1)$. In fact $p \equiv 1 \mod 6$ in this case, so the coordinates r and s are even, and $1 = (-1)^{r-s} = (-1)^s$. Since the center is invariant under rotation about itself, the point (r, s) satisfies Congruence (6). Consequently, $(r, s) \in D(p)$ and we obtain the following congruence.

Corollary 3. *If $p \equiv 1 \mod 3$, then*

$$\binom{pa + \frac{2}{3}(p-1)}{pb + \frac{1}{3}(p-1)} \equiv \binom{a}{b}\binom{\frac{2}{3}(p-1)}{\frac{1}{3}(p-1)} \mod p^2$$

for all $a \geq 0$ and $b \geq 0$.

We can iterate Corollary 3 for the particular numbers $a = \frac{2}{3}(p-1)\sum_{i=0}^{\ell-1} p^i = \frac{2}{3}(p^\ell - 1)$ and $b = \frac{1}{3}(p^\ell - 1)$ whose base-p representations consist of ℓ copies of the digits $\frac{2}{3}(p-1)$ and $\frac{1}{3}(p-1)$ respectively. Namely, if $p \equiv 1 \mod 3$ and $\ell \geq 0$, then

$$\binom{\frac{2}{3}(p^\ell - 1)}{\frac{1}{3}(p^\ell - 1)} \equiv \binom{\frac{2}{3}(p-1)}{\frac{1}{3}(p-1)}^\ell \mod p^2.$$

An interesting question, which we do not address here, is whether anything more can be said about the size of $D(p)$ as a function of p. The following table gives the set $D(p)$ for the first ten primes.

p	$D(p)$
2	$\{(0,0)\}$
3	$\{(0,0),(2,0),(2,2)\}$
5	$\{(0,0),(4,0),(4,4)\}$
7	$\{(0,0),(4,2),(6,0),(6,6)\}$
11	$\{(0,0),(3,0),(3,3),(7,0),(7,7),(10,0),(10,3),(10,7),(10,10)\}$
13	$\{(0,0),(8,4),(12,0),(12,12)\}$
17	$\{(0,0),(9,2),(9,7),(14,7),(16,0),(16,16)\}$
19	$\{(0,0),(12,6),(18,0),(18,18)\}$
23	$\{(0,0),(22,0),(22,22)\}$
29	$\{(0,0),(13,0),(13,13),(15,0),(15,15),(28,0),(28,13),(28,15),(28,28)\}$

Theorem 2 was suggested by an analogous result for the Apéry numbers, which are defined by $A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$. Gessel [6] showed that the Apéry numbers satisfy the Lucas congruence $A(pn+r) \equiv A(n)A(r) \mod p$ for all $r \in \{0, 1, \ldots, p-1\}$ and all $n \geq 0$. For certain values of r, this congruence is known to also hold modulo p^2. Gessel noticed that $A(3n + r) \equiv A(n)A(r) \mod 9$ for all $r \in \{0, 1, 2\}$. By computing an automaton for the Apéry numbers modulo 25, Rowland and Yassawi [13, Theorem 3.31] showed that $A(5n + r) \equiv A(n)A(r) \mod 25$ if $r \in \{0, 2, 4\}$. This was recently generalized to all primes [14]. Namely, the digits $r \in \{0, 1, \ldots, p-1\}$ for which all $n \geq 0$ satisfy

$$A(pn + r) \equiv A(n)A(r) \mod p^2$$

are precisely the digits for which $A(r) \equiv A(p-1-r) \mod p^2$. The reflection symmetry $A(p-1-r) \equiv A(r) \mod p$ was established by Malik and Straub [11, Lemma 6.2] for all $r \in \{0, 1, \ldots, p-1\}$. Therefore, the elements of both $D(p)$ and the analogous set for the Apéry numbers can be characterized as those for which a certain symmetry modulo p in fact holds modulo p^2.

3. A general congruence

To prove Theorem 2, we first prove a general congruence for $\binom{pa+r}{pb+s}$ modulo p^2. Similar results have been used by Jacobsthal [3] and others. Let $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ be the nth harmonic number. (In particular, the 0th harmonic number is the empty sum $H_0 = 0$.) For $r \in \{0, 1, \dots, p-1\}$, the denominator of H_r is not divisible by p, so we can interpret H_n modulo p and modulo p^2.

Theorem 4. *Let p be a prime. If $0 \le s \le r \le p-1$, $a \ge 0$, and $b \ge 0$, then*

$$\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s}\left(1 + pa\left(H_r - H_{r-s}\right) + pb\left(H_{r-s} - H_s\right)\right) \mod p^2.$$

Proof. If $b > a$, then $\binom{pa+r}{pb+s} = 0 = \binom{a}{b}$, so the congruence holds. Assume $b \le a$. By breaking a factorial into two products, we obtain

$$\begin{aligned}\binom{pa+r}{pb+s} &= \frac{(pa+r)!}{(pb+s)!(pa-pb+r-s)!} \\ &= \frac{(pa)!}{(pb)!(pa-pb)!}\frac{\prod_{i=1}^{r}(pa+i)}{\prod_{i=1}^{s}(pb+i)\prod_{i=1}^{r-s}(pa-pb+i)}.\end{aligned}$$

The first factor is $\binom{pa}{ba} \equiv \binom{a}{b} \mod p^2$; this is a special case of Congruence (5). For the three products, we expand each and collect terms by like powers of p. For example, $\prod_{i=1}^{r}(pa+i) \equiv r! + pa\sum_{i=1}^{r}\frac{r!}{i} \mod p^2$. This gives

$$\begin{aligned}\binom{pa+r}{pb+s} &\equiv \binom{a}{b}\frac{r!}{s!(r-s)!}\frac{1+paH_r}{(1+pbH_s)(1+p(a-b)H_{r-s})} \mod p^2 \\ &\equiv \binom{a}{b}\binom{r}{s}(1+paH_r)(1-pbH_s)(1-p(a-b)H_{r-s}) \mod p^2 \\ &\equiv \binom{a}{b}\binom{r}{s}\left(1 + pa\left(H_r - H_{r-s}\right) + pb\left(H_{r-s} - H_s\right)\right) \mod p^2\end{aligned}$$

as desired. □

4. Symmetries of $D(p)$

In this section we establish that $D(p)$ possesses the symmetries of the equilateral triangle. In particular, we prove Theorem 2. The reflection symmetry $\binom{a}{b} = \binom{a}{a-b}$ of Pascal's triangle is familiar. Next we show that $D(p)$ also exhibits this symmetry.

Proposition 5. *Let p be a prime. If $(r, s) \in D(p)$, then $(r, r-s) \in D(p)$.*

Proof. Let $(r, s) \in D(p)$. By Proposition 1, $s \le r$. By assumption, $\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$ for all $a \ge 0$ and $b \ge 0$. Fix a and b. We would like to show $\binom{pa+r}{pb+r-s} \equiv \binom{a}{b}\binom{r}{r-s} \mod p^2$. There are two cases. If $b > a$, then $s < p \le p(b-a)$. It follows that $pa + r < pb + r - s$. Therefore $\binom{pa+r}{pb+r-s} = 0 = \binom{a}{b}\binom{r}{r-s}$, so the congruence holds. On the other hand, if $b \le a$, the reflection symmetry of Pascal's triangle gives

$$\binom{pa+r}{pb+r-s} = \binom{pa+r}{(pa+r)-(pb+r-s)} = \binom{pa+r}{p(a-b)+s}.$$

Since $(r,s) \in D(p)$, this implies

$$\begin{aligned}\binom{pa+r}{pb+r-s} &\equiv \binom{a}{a-b}\binom{r}{s} \mod p^2\\ &= \binom{a}{b}\binom{r}{r-s}\\ &\equiv \binom{pa}{pb}\binom{r}{r-s} \mod p^2,\end{aligned}$$

as desired. In both cases, $\binom{pa+r}{pb+r-s} \equiv \binom{a}{b}\binom{r}{r-s} \mod p^2$, so $(r, r-s) \in D(p)$. □

In addition to the reflection symmetry, the first p rows of Pascal's triangle also exhibit rotational symmetry modulo p. To see this, first we prove the following congruence modulo p^2.

Proposition 6. *Let p be a prime. If $0 \le s \le r \le p-1$, then*

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s}(1+pH_r-pH_s) \mod p^2. \tag{7}$$

Proof. We begin with $r!(p-1-r)!$. Similar to the proof of Theorem 4, we expand the product $(p-1-r)!$ and collect terms by like powers of p:

$$\begin{aligned}r!(p-1-r)! &= r!\prod_{i=r+1}^{p-1}(p-i)\\ &\equiv r!\left(\prod_{i=r+1}^{p-1}(-i) + p\,(-1)^{p-1-r}\frac{(p-1)!}{r!}\sum_{i=r+1}^{p-1}\frac{1}{-i}\right) \mod p^2\\ &= (-1)^{p-1-r}(p-1)!(1-p\,(H_{p-1}-H_r)).\end{aligned}$$

Therefore

$$\begin{aligned}\frac{r!(p-1-r)!}{s!(p-1-s)!} &\equiv (-1)^{r-s}\frac{1-p\,(H_{p-1}-H_r)}{1-p\,(H_{p-1}-H_s)} \mod p^2\\ &\equiv (-1)^{r-s}(1-p\,(H_{p-1}-H_r))(1+p\,(H_{p-1}-H_s)) \mod p^2\\ &\equiv (-1)^{r-s}(1+pH_r-pH_s) \mod p^2.\end{aligned}$$

This is equivalent to

$$\frac{r!}{s!} \equiv (-1)^{r-s}\frac{(p-1-s)!}{(p-1-r)!}(1+pH_r-pH_s) \mod p^2.$$

Dividing both sides by $(r-s)!$ produces Congruence (7). □

Modulo p, we obtain the following rotational symmetry.

Corollary 7. *Let p be a prime. If $0 \le s \le r \le p-1$, then*

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \mod p.$$

Theorem 2 follows from Theorem 4 and Proposition 6.

Theorem 2. *Let p be a prime. If $r, s \in \{0, 1, \ldots, p-1\}$, then $(r,s) \in D(p)$ if and only if $s \le r$ and*

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \equiv (-1)^{s}\binom{p-1-r+s}{s} \mod p^2. \tag{8}$$

Proof. By Proposition 1, if $(r,s) \notin D(p)$ then $s \leq r$. Therefore assume $s \leq r$. We show two equivalences.

First we show that $\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$ for all $a \geq 0$ and $b \geq 0$ if and only if $H_r \equiv H_{r-s} \equiv H_s \mod p$. By Theorem 4,

$$\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s}\left(1 + pa\left(H_r - H_{r-s}\right) + pb\left(H_{r-s} - H_s\right)\right) \mod p^2.$$

Clearly if $H_r \equiv H_{r-s} \equiv H_s \mod p$ then $\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$ for all $a \geq 0$ and $b \geq 0$. Conversely, assume $\binom{pa+r}{pb+s} \equiv \binom{a}{b}\binom{r}{s} \mod p^2$ for all $a \geq 0$ and $b \geq 0$. Since $\binom{r}{s}$ is not divisible by p, this, along with Theorem 4, implies

$$\binom{a}{b} \equiv \binom{a}{b}\left(1 + pa\left(H_r - H_{r-s}\right) + pb\left(H_{r-s} - H_s\right)\right) \mod p^2.$$

Setting $a = 1$ and $b = 0$ shows that $H_r \equiv H_{r-s} \mod p$. Now setting $a = 1$ and $b = 1$ shows that $H_{r-s} \equiv H_s \mod p$.

Now we show that $H_r \equiv H_{r-s} \equiv H_s \mod p$ is equivalent to Congruence (8). We see from Proposition 6 that $H_r \equiv H_s \mod p$ if and only if

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \mod p^2.$$

Similarly, $H_r \equiv H_{r-s} \mod p$ if and only if

$$\binom{r}{r-s} \equiv (-1)^{s}\binom{p-1-r+s}{s} \mod p^2.$$

Since $\binom{r}{r-s} = \binom{r}{s}$, this implies that $H_r \equiv H_{r-s} \equiv H_s \mod p$ if and only if Congruence (8) holds. □

Theorem 2 and Proposition 5 imply that $D(p)$ is invariant under the symmetries of the equilateral triangle.

References

[1] Charles Babbage, Demonstration of a theorem relating to prime numbers, *The Edinburgh Philosophical Journal* **1** (1819) 46–49.

[2] D. F. Bailey, Two p^3 variations of Lucas' theorem, *Journal of Number Theory* **35** (1990) 208–215.

[3] 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, *Skandinaviske Matematikerkongress* **11** (1949) 42–54.

[4] Kenneth Davis and William Webb, Lucas' theorem for prime powers, *European Journal of Combinatorics* **11** (1990) 229–233.

[5] Kenneth Davis and William Webb, A binomial coefficient congruence modulo prime powers, *Journal of Number Theory* **43** (1993) 20–23.

[6] Ira Gessel, Some congruences for Apéry numbers, *Journal of Number Theory* **14** (1982) 362–368.

[7] 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, *The Quarterly Journal of Pure and Applied Mathematics* **31** (1900) 321–353.

[8] Andrew Granville, Binomial coefficients modulo prime powers, *Canadian Mathematical Society Conference Proceedings* **20** (1997) 253–275.

[9] G. S. Kazandzidis, Congruences on the binomial coefficients, *Bulletin of the Greek Mathematical Society* **9** (1968) 1–12.

[10] Édouard Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des functions trigonométriques, suivant un module premier, *Bulletin de la Société Mathématique de France* **6** (1878) 49–54.

[11] Amita Malik and Armin Straub, Divisibility properties of sporadic Apéry-like numbers, *Research in Number Theory* **2** (2016) Article 5.

[12] Romeo Meštrović, Lucas' theorem: its generalizations, extensions and applications (1878–2014), `https://arxiv.org/abs/1409.3820`.

[13] Eric Rowland and Reem Yassawi, Automatic congruences for diagonals of rational functions, *Journal de Théorie des Nombres de Bordeaux* **27** (2015) 245–288.

[14] Eric Rowland, Reem Yassawi, and Christian Krattenthaler, Lucas congruences for the Apéry numbers modulo p^2, `https://arxiv.org/abs/2005.04801`.

[15] Joseph Wolstenholme, On certain properties of prime numbers, *The Quarterly Journal of Pure and Applied Mathematics* **5** (1862) 35–39.

[16] Jianqiang Zhao, Bernoulli numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem, *Journal of Number Theory* **123** (2007) 18–26.

Department of Mathematics, Hofstra University, Hempstead, NY, USA