CONGRUENCES FOR CERTAIN LACUNARY SUMS OF PRODUCTS OF BINOMIAL COEFFICIENTS

René Gy
rene.gy@numericable.com

Received: 5/21/20, Accepted: 12/22/20, Published: 1/4/21

Abstract

We show that the following congruences

$$\sum_{i\geq \ell+1}(-1)^{m-i}\binom{m}{i}\binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)}\equiv 0 \bmod p$$

$$\sum_{i\geq 0}(-1)^{m-i}\binom{m}{i}\binom{\ell+ip}{m+s-1}\equiv 0 \bmod p^m$$

$$\sum_{j,i\geq \ell}(-1)^{j-i}\binom{m}{j}\binom{j}{i}\binom{j+s-1+i(p-1)}{j+s-1+\ell(p-1)}\equiv 0 \bmod p^{m-\ell}$$

are valid for any prime p and any natural numbers ℓ, m, and s such that $0<s<p$. The corresponding quotients involve Adelberg polynomials which can be computed explicitly, providing closed-form expressions for these sums, valid even if p is not prime, when the congruences do not necessarily hold.

1. Introduction, Notation, and Preliminaries

There exist many congruences involving binomial coefficients. Apart from their classical arithmetic properties like the famous Kummer, Lucas and Wolstenholme theorems, to name a few, other congruences involving lacunary sums or lacunary sums of products of binomial coefficients have also been known for a long time. These kinds of results can be found for instance in the introduction of [3] where advanced arithmetic properties of binomial coefficients are presented. They have been further investigated and generalized in [6] and [7]. We recall two old examples taken from [3] and two more recent examples from [6] and [7]:

$$\sum_{i\ge 0}\binom{s+\ell(p-1)}{h+i(p-1)} \equiv \binom{s}{h} \pmod p \quad \text{(Glaisher, 1899)},$$

$$\sum_{i\ge 0}(-1)^{ip}\binom{s+q(p-1)}{h+ip} \equiv 0 \pmod{p^q} \quad \text{(Fleck, 1913)},$$

$$\sum_{i\ge 0}(-1)^{ip}\binom{i}{\ell}\binom{\ell p+s+q(p-1)}{h+ip} \equiv 0 \pmod{p^q} \quad \text{(Wan, 2005)},$$

$$\sum_{i,j\ge 0}(-1)^{j+i(p-1)}\binom{q}{j}\binom{h+j(p-1)}{s+i(p-1)} \equiv 0 \pmod{p^q} \quad \text{(Sun, Tauraso, 2007)},$$

which are valid for prime p, non-negative integers ℓ, q and integers s, h such that $0 < s < p$ and $0 \le h < p$. Note that the aforementioned congruences are written here differently from how they read in the quoted papers, for an easier comparison in between them and with our own results. Also note that the last one is just a particular case from a vast generalization ([7], Theorem 1.2).

The purpose of the present paper is to establish three new congruences somewhat reminiscent of, but different from, the above congruences. Namely, we will show that, for any prime p and any natural numbers ℓ, m and s such that $0 < s < p$, it holds that

$$\sum_{i\ge \ell+1}(-1)^{m-i}\binom{m}{i}\binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)} \equiv 0 \pmod p,$$

$$\sum_{i\ge 0}(-1)^{m-i}\binom{m}{i}\binom{\ell+ip}{m+s-1} \equiv 0 \pmod{p^m},$$

$$\sum_{j,i\ge \ell}(-1)^{j-i}\binom{m}{j}\binom{j}{i}\binom{j+s-1+i(p-1)}{j+s-1+\ell(p-1)} \equiv 0 \pmod{p^{m-\ell}},$$

and we will show how to effectively obtain the corresponding quotients.

In the following, $[[x^n]]f(x)$ denotes the coefficient of x^n in $f(x)$, where f is a formal power series with the argument x and $\partial f(x)$ is the derivative of $f(x)$ with respect to x. If x is a real number, we denote by $\lfloor x \rfloor$ the largest integer smaller or equal to x. We also use the Iverson bracket notation: $[\mathfrak{P}] = 1$ when proposition $\mathfrak{P}$ is true, and $[\mathfrak{P}] = 0$ otherwise. We recall some basic properties of the binomial coefficients and Stirling numbers, which can be found for instance in [2]. The binomial coefficients $\binom{n}{k}$ are defined by $\sum_k \binom{n}{k}x^k = (1+x)^n$, whatever the sign of the integer n. They obviously vanish when $k < 0$. They are easily obtained by the basic recurrence relation $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, they satisfy the Vandermonde convolution $\sum_{j=0}^{m}\binom{n}{j}\binom{k}{m-j} = \binom{n+k}{m}$ and when $n > 0$, we have $\binom{-n}{k} = (-1)^k\binom{n+k-1}{n-1}$. The cycle Stirling numbers (or Stirling numbers of the first kind) $\left[{n \atop k}\right]$, $n \ge 0$, may be defined by the horizontal generating function

$$\sum_k \begin{bmatrix} n \\ k \end{bmatrix} x^k = \prod_{j=0}^{n-1} (x+j), \tag{1.1}$$

where an empty product is meant to be 1. Alternatively, they have the exponential generating function

$$\sum_n \begin{bmatrix} n \\ k \end{bmatrix} \frac{x^n}{n!} = \frac{(-1)^k \big(\ln(1-x)\big)^k}{k!}. \tag{1.2}$$

They obviously vanish when $k < 0$ and $k > n$. They are easily obtained by the basic recurrence $\left[{n \atop k}\right] = (n-1)\left[{n-1 \atop k}\right] + \left[{n-1 \atop k-1}\right]$, valid for $n \geq 1$, with $\left[{0 \atop k}\right] = [k = 0]$. We let $\left\{{n \atop k}\right\}$, $n \geq 0$, be the partition Stirling numbers (or Stirling numbers of the second kind). They also vanish when $k < 0$ and $k > n$. Their basic recurrence is $\left\{{n \atop k}\right\} = k\left\{{n-1 \atop k}\right\} + \left\{{n-1 \atop k-1}\right\}$ for $n \geq 1$, with $\left\{{0 \atop k}\right\} = [k = 0]$. They have the following exponential generating function

$$\sum_n \begin{Bmatrix} n \\ k \end{Bmatrix} \frac{x^n}{n!} = \frac{(e^x - 1)^k}{k!} \tag{1.3}$$

and the following explicit expression

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = \frac{(-1)^k}{k!} \sum_{j \geq 0} (-1)^j \binom{k}{j} j^n. \tag{1.4}$$

We will also need the following knowm lemmas, for which we include a short proof.

Lemma 1.1. *Let $f(w)$ be a formal power series, and α a natural number. We have* $[[w^n]]\frac{f(w)^\alpha}{\alpha} = [[w^{n-1}]]\frac{f(w)^{\alpha-1}\partial f(w)}{n}$.

Proof. This is clear, since $[[w^n]]f(w) = \frac{[[w^{n-1}]]\partial f(w)}{n}$. □

Lemma 1.2. *For any natural number n, $n > 0$, we have*

$$\begin{Bmatrix} n \\ p-1 \end{Bmatrix} \equiv \big[p - 1 \text{ divides } n\big] \pmod{p}. \tag{1.5}$$

Proof. We recall the Wilson theorem which states that $(p-1)! \equiv -1 \bmod p$ for any prime p, and two other well-known congruences, valid for any prime p:

$$\binom{p-1}{j} \equiv (-1)^j \big[0 \leq j \leq p-1\big] \pmod{p},$$

$$\sum_{p-1 \geq j \geq 1} j^k \equiv -\big[p - 1 \text{ divides } k\big] \pmod{p},$$

so that the claim readily follows from Equation (1.4). □

2. The p-Congruence for Stirling Numbers of the First Kind

The following known [4] p-congruence for the Stirling numbers of the first kind will be essential to our argument in Section 4.

Theorem 2.1. *Let p be a prime number and n, k non-negative integers such that $0 \leq k \leq n$, let r (respectively q) be the residue (respectively the quotient) of the Euclidean division of n by p and let ρ be the residue of the Euclidean division of $k-q$ by $p-1$. Let $j = \rho + [\rho = 0][r = p-1](p-1)$. We have*

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv (-1)^{q - \frac{k-q-j}{p-1}} \begin{bmatrix} r \\ j \end{bmatrix} \binom{q}{\frac{k-q-j}{p-1}} \pmod{p}. \tag{2.1}$$

Proof. For the sake of self-containment, we reproduce the proof from [4]. Let p be a prime number. We consider $\prod_{j=0}^{p-1}(x+j) = \sum_k \left[\begin{smallmatrix} p \\ k \end{smallmatrix}\right] x^k$ as an element of the ring of polynomials of $\mathbb{Z}/p\mathbb{Z}$. In that ring, we have $\sum_k \left[\begin{smallmatrix} p \\ k \end{smallmatrix}\right] x^k = x^p - x$, since the polynomials on both sides have the same degree p, the same coefficient for x^p and the same roots: $0, -1, -2, \cdots, -(p-1)$. In particular, for k such that $1 < k \leq p-1$, we have $\left[\begin{smallmatrix} p \\ k \end{smallmatrix}\right] \equiv 0 \bmod p$. Let n be a non-negative integer and r (respectively q) be the residue (respectively the quotient) of the Euclidean division of n by p, such that $n = qp + r$, with $0 \leq r \leq p-1$. We may explicitly write and regroup the factors of $\prod_{j=0}^{n-1}(x+j)$ so that

$$\prod_{j=0}^{n-1}(x+j) = \prod_{t=0}^{q-1}\left((x+tp)(x+tp+1)\cdots(x+tp+(p-1))\right)\prod_{u=0}^{r-1}(x+q+u),$$

with the convention that when $q = 0$ or $r = 0$ the empty products are meant to be equal to 1. Then, reducing modulo p, we have

$$\begin{aligned}
\sum_k \begin{bmatrix} n \\ k \end{bmatrix} x^k &\equiv \prod_{t=0}^{q-1}\left(x(x+1)\cdots(x+(p-1))\right)\prod_{u=0}^{r-1}(x+qp+u) \pmod{p} \\
&\equiv \left(x(x+1)\cdots(x+(p-1))\right)^q \prod_{u=0}^{r-1}(x+u) \pmod{p} \\
&\equiv (x^p - x)^q \prod_{u=0}^{r-1}(x+u) \pmod{p} \\
&\equiv x^q \left(x^{p-1} - 1\right)^q \prod_{u=0}^{r-1}(x+u) \pmod{p} \\
&\equiv x^q \sum_{m=0}^{q} (-1)^{q-m} \binom{q}{m} x^{m(p-1)} \prod_{u=0}^{r-1}(x+u) \pmod{p} \\
&\equiv \left(\sum_{m=0}^{q} (-1)^{q-m} \binom{q}{m} x^{m(p-1)}\right)\left(\sum_{\ell=0}^{r} \begin{bmatrix} r \\ \ell \end{bmatrix} x^{\ell}\right) \pmod{p}.
\end{aligned}$$

That is

$$\sum_k \begin{bmatrix} n \\ k \end{bmatrix} x^{k-q} \equiv \sum_k \sum_{\substack{m,l \\ m(p-1)+\ell=k-q}} (-1)^{q-m} \binom{q}{m} \begin{bmatrix} r \\ \ell \end{bmatrix} x^{k-q} \pmod p.$$

Hence

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv \sum_{\substack{m,l \\ m(p-1)+\ell=k-q}} (-1)^{q-m} \binom{q}{m} \begin{bmatrix} r \\ \ell \end{bmatrix} \pmod p. \tag{2.2}$$

Now if p divides n, we have $r = 0$, and there exists only one possible solution in non-negative integers ℓ, m to the equation $m(p-1) + \ell = k - q$ with a non-zero contribution to the sum on the right-hand side of the above congruence: this is when $p - 1$ divides $k - \frac{n}{p}$ and the solution is $\ell = 0$ and $m = \frac{k-q}{p-1}$. Otherwise, $1 \leq r < p$ and since $\ell \leq r$ and $r < p$, we have $\ell < p$. But we also have $\ell > 0$, since $\begin{bmatrix} r \\ 0 \end{bmatrix} = 0$, since $r > 0$. Then, there exists at most one solution in non-negative integers ℓ, m to the equation $m(p-1) + \ell = k - q$. Indeed, let ρ be the residue of the Euclidean division of $k - q$ by $p - 1$. We have $0 \leq \rho < p - 1$. If $\rho = 0$, then the unique solution is $\ell = p - 1$ and $m = \frac{k-q}{p-1} - 1$. If $0 < \rho \leq r$, then the unique solution is $\ell = \rho$ and $m = \frac{k-q-\rho}{p-1}$. And finally, if $r < \rho < p - 1$, there is no solution. Putting everything together, we obtain the claimed p-congruence for the Stirling numbers of the first kind. □

Corollary 2.1.1. *Let p be a prime number and i, m and s be three natural numbers. We have*

$$\begin{bmatrix} m + s + m(p-1) \\ m + s + i(p-1) \end{bmatrix} \equiv (-1)^{m-i} \binom{m + \lfloor \frac{s}{p} \rfloor}{i + \lfloor \frac{s}{p} \rfloor} \pmod p. \tag{2.3}$$

Proof. We apply Theorem 2.1 with $n = mp + s$ and $k = m + s + i(p-1)$. We have $q = m + \lfloor \frac{s}{p} \rfloor$ and $k - q = s + i(p-1) - \lfloor \frac{s}{p} \rfloor = (i + \lfloor \frac{s}{p} \rfloor)(p-1) + r$. Then, when $s - p\lfloor \frac{s}{p} \rfloor = r < p - 1$ we have $r = \rho < p - 1$ and then $j = r$ and then Congruence (3.1) reduces to Congruence (2.3). Otherwise $s - p\lfloor \frac{s}{p} \rfloor = r = p - 1$ and then $\rho = 0$ and then $j = p - 1$ and then Congruence (3.1) also reduces to Congruence (2.3). □

3. An Identity Involving Stirling Numbers

In the following theorem, we present an identity involving binomial coefficients and Stirling numbers of both kinds which we believe is new.

Theorem 3.1. *Let p be a positive integer and n, k non-negative integers. We have*

$$(-1)^{p-1} \binom{n-1}{p-1} \begin{bmatrix} n-p+1 \\ k \end{bmatrix} = \sum_i (-1)^i \binom{k-1+i}{i} \begin{Bmatrix} i \\ p-1 \end{Bmatrix} \begin{bmatrix} n \\ i+k \end{bmatrix}. \tag{3.1}$$

Remark. It is interesting to compare Equation (3.1) to the identity (6.28) in [2]. The latter is also a three parameters identity, but involving only the second kind of Stirling numbers, which is rather easily obtained from their exponential generating function. We reproduce it hereafter: under the condition that $\ell, m, n \geq 0$, we have

$$\binom{\ell+m}{\ell}\left\{ {n \atop \ell+m} \right\} = \sum_k \left\{ {k \atop \ell} \right\}\left\{ {n-k \atop m} \right\}\binom{n}{k}. \tag{3.2}$$

If we replace m by $-m$ and n by $-n$ in Equation (3.2), taking into account that $\binom{-n}{k} = (-1)^k\binom{n+k-1}{k}$ and the known duality $\left\{ {-a \atop -b} \right\} = \left[{b \atop a} \right]$, see [2], we obtain our Equation (3.1) with $p-1=\ell$. This shows that Equation (3.2) holds under the only condition $\ell \geq 0$ and that the conditions $m, n \geq 0$ given in [2] are actually not needed.

Proof of Theorem 3.1. The following proof, using the coefficient extractor method and the generating functions Equation (1.2) and Equation (1.3) is due to Marko Riedel [5]. Let S be the right-hand side of Equation (3.1). We have

$$\begin{aligned} S &= \sum_{i=p-1}^{n-k} (-1)^i \binom{k-1+i}{i} \left\{ {i \atop p-1} \right\} \left[{n \atop i+k} \right] \\ &= \sum_{i=p-1}^{n-k} (-1)^i \binom{k-1+i}{i} i![[z^i]]\frac{(e^z-1)^{p-1}}{(p-1)!} n![[w^n]]\frac{\left(\log\frac{1}{1-w}\right)^{i+k}}{(i+k)!} \\ &= \frac{n!}{(p-1)!(k-1)!}[[w^n]] \sum_{i=p-1}^{n-k} (-1)^i [[z^i]](e^z-1)^{p-1} \frac{\left(\log\frac{1}{1-w}\right)^{i+k}}{(i+k)}. \end{aligned}$$

Then we make use of Lemma 1.1 and we have

$$\begin{aligned} S &= \frac{(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w} \sum_{i=p-1}^{n-k} (-1)^i [[z^i]](e^z-1)^{p-1} \left(\log\frac{1}{1-w}\right)^{i+k-1} \\ &= \frac{(-1)^{k-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w} \sum_{i=p+k-2}^{n-1} (-1)^i [[z^i]]z^{k-1}(e^z-1)^{p-1} \left(\log\frac{1}{1-w}\right)^{i} \\ &= \frac{(-1)^{k-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w} \sum_{i\geq p+k-2} \left(-\log\frac{1}{1-w}\right)^{i} [[z^i]]z^{k-1}(e^z-1)^{p-1}. \end{aligned}$$

Indeed, since w^i is the lowest term in the power expansion of $\left(\log\frac{1}{1-w}\right)^i$, the coefficient of w^{n-1} in the sum is unaffected when we let the index i run unbounded above $n-1$. Similarly, since $(e^z-1)^{p-1} = z^{p-1} + \cdot\cdot$, the lowest power of z in the power expansion of $z^{k-1}(e^z-1)^{p-1}$ is z^{p+k-2}, and then

$$\begin{aligned} S &= \frac{(-1)^{k-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w}\sum_{i\geq 0}\left(-\log\frac{1}{1-w}\right)^i [[z^i]]z^{k-1}(e^z-1)^{p-1} \\ &= \frac{(-1)^{k-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w}\left(-\log\frac{1}{1-w}\right)^{k-1}(e^{-\log\frac{1}{1-w}}-1)^{p-1} \\ &= \frac{(-1)^{k-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w}\left(-\log\frac{1}{1-w}\right)^{k-1}(-w)^{p-1} \\ &= \frac{(-1)^{p-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-1}]]\frac{1}{1-w}\left(\log\frac{1}{1-w}\right)^{k-1}w^{p-1} \\ &= \frac{(-1)^{p-1}(n-1)!}{(p-1)!(k-1)!}[[w^{n-p}]]\frac{1}{1-w}\left(\log\frac{1}{1-w}\right)^{k-1} \\ &= \frac{(-1)^{p-1}(n-1)!}{(p-1)!(k-1)!}(n-p+1)[[w^{n-p}]]\frac{1}{1-w}\frac{\left(\log\frac{1}{1-w}\right)^{k-1}}{n-p+1}. \end{aligned}$$

Then, we use again Lemma 1.1 and we have

$$\begin{aligned} S &= \frac{(-1)^{p-1}(n-1)!}{(p-1)!(k-1)!}(n-p+1)[[w^{n-p+1}]]\frac{\left(\log\frac{1}{1-w}\right)^{k}}{k} \\ &= \frac{(-1)^{p-1}(n-1)!}{(p-1)!(n-p)!}(n-p+1)![[w^{n-p+1}]]\frac{\left(\log\frac{1}{1-w}\right)^{k}}{k!} \\ &= (-1)^{p-1}\binom{n-1}{p-1}\begin{bmatrix} n-p+1 \\ k \end{bmatrix}. \end{aligned}$$

□

As corollary, we have a new congruence involving Stirling numbers of the first kind.

Corollary 3.1.1. *Let p be a prime number, and let n, k be non-negative integers. The following congruence holds:*

$$\sum_{\substack{i>0 \\ p-1|i}}\binom{k-1+i}{k-1}\begin{bmatrix} n \\ i+k \end{bmatrix} \equiv [p \text{ divides } n]\begin{bmatrix} n-p+1 \\ k \end{bmatrix} \pmod p. \tag{3.3}$$

Proof. Consider Equation (3.1) when p is prime. When $i=0$, we have $\left\{ {i \atop p-1} \right\} = 0$, and when $i>0$, by Lemma 1.2, we have $\left\{ {i \atop p-1} \right\} \equiv [p-1 \text{ divides } i] \bmod p$. Moreover, $(-1)^{p-1} \equiv 1 \bmod p$, and hence, modulo p, the right-hand side of Equation (3.1) is

$$\sum_{\substack{i>0 \\ p-1|i}}\binom{k-1+i}{k-1}\begin{bmatrix} n \\ i+k \end{bmatrix}.$$

Now, for the left-hand side of Equation (3.1), when p does not divide n, we have $n-p \not\equiv 0 \bmod p$, and by Kummer's theorem, $\binom{n-1}{p-1} \equiv 0 \pmod{p}$, since in this case the addition $(n-p)+(p-1)$ in base p has at least one carry (at the lowest digit). Otherwise, when p divides n, we have $\binom{n-1}{p-1} \equiv \binom{-1}{p-1} = (-1)^{p-1} \equiv 1 \pmod{p}$. □

4. The First Congruence

We can now prove our first claim from the introduction. Actually, we have an even stronger theorem.

Theorem 4.1. *Let p be a prime number, and m, ℓ and s three natural numbers such that $m > \ell$. We have*

$$\sum_{i \geq \ell+1} (-1)^{m-i} \binom{m + \lfloor \frac{s}{p} \rfloor}{i + \lfloor \frac{s}{p} \rfloor} \binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)}$$

$$\equiv \big[p \text{ divides } s\big] (-1)^{m-1-\ell} \binom{m-1+\frac{s}{p}}{\ell + \frac{s}{p}} \pmod{p}. \tag{4.1}$$

Proof. If we substitute $m+s+\ell(p-1)$ for k and $mp+s$ for n, Congruence (3.3) becomes

$$\sum_{\substack{i>0 \\ p-1 \mid i}} \binom{m+s-1+\ell(p-1)+i}{m+s-1+\ell(p-1)} \begin{bmatrix} mp+s \\ i+m+s+\ell(p-1) \end{bmatrix}$$

$$\equiv \big[p \text{ divides } s\big] \begin{bmatrix} (m-1)p+s+1 \\ m+s+\ell(p-1) \end{bmatrix} \pmod{p},$$

which, by the appropriate index change, is

$$\sum_{i \geq \ell+1} \binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)} \begin{bmatrix} mp+s \\ m+s+i(p-1) \end{bmatrix}$$

$$\equiv \big[p \text{ divides } s\big] \begin{bmatrix} (m-1)p+s+1 \\ m+s+\ell(p-1) \end{bmatrix} \pmod{p}.$$

To complete the proof, we make use of Corollary 2.1.1 and we have

$$\sum_{i \geq \ell+1} \binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)} (-1)^{m-i} \binom{m + \lfloor \frac{s}{p} \rfloor}{i + \lfloor \frac{s}{p} \rfloor}$$

$$\equiv \big[p \text{ divides } s\big] (-1)^{m-1-\ell} \binom{m-1+\lfloor \frac{s+1}{p} \rfloor}{\ell + \lfloor \frac{s+1}{p} \rfloor} \pmod{p},$$

which is the claim, since when p divides s, we have $\lfloor \frac{s+1}{p} \rfloor = \frac{s}{p}$. □

Remark. Clearly, when $s = 0$, we obtain

$$\sum_{i \geq \ell+1} (-1)^i \binom{m}{i} \binom{m-1+i(p-1)}{m-1+\ell(p-1)} + (-1)^\ell \binom{m-1}{\ell} \equiv 0 \pmod{p}, \tag{4.2}$$

and whenever $0 < s < p$, we have

$$\sum_{i \geq \ell+1} (-1)^{m-i} \binom{m}{i} \binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)} \equiv 0 \pmod{p}, \tag{4.3}$$

which is our first claim from the introduction.

Finally, we also have the following corollary.

Corollary 4.1.1. *For any prime p and natural numbers ℓ, n such that p does not divide n, we have*

$$\sum_{i \geq \ell+1} (-1)^i \binom{n-r}{i} \binom{n-1+i(p-1)}{n-1+\ell(p-1)} \equiv 0 \pmod{p}, \tag{4.4}$$

where r is the non-zero residue of the Euclidean division of n by p.

Proof. Congruence (4.4) is obtained from Congruence (4.1) in which we let s be the residue of the Euclidean division of n by p and we replace m by $\lfloor \frac{n}{p} \rfloor p$. $\square$

5. Adelberg Polynomials

In this section we recall the definition and some properties of the *Adelberg polynomials.* Most of the content of this section is taken from [1]. We have the A-Adelberg polynomials and the B-Adelberg polynomials. By definition, the A-Adelberg polynomial $A_{s-1}(x, y, m)$ is

$$A_{s-1}(x, y, m) := \frac{1}{y^m} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \binom{x+ky}{m+s-1}. \tag{5.1}$$

It is the m-th *divided difference with increment* y of the function $f(x) := \binom{x}{m+s-1}$. That is

$$A_{s-1}(x, y, m) = \nabla_y^m \binom{x}{m+s-1}, \tag{5.2}$$

where $\nabla_y f(x) = \frac{f(x+y)-f(x)}{y}$. The B-Adelberg polynomial $B_{s-1}(y, m)$ is defined as

$$B_{s-1}(y, m) := A_{s-1}(0, y, m) = \frac{1}{y^m} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \binom{ky}{m+s-1}. \tag{5.3}$$

$A_{s-1}(x,y,m)$ and $B_{s-1}(y,m)$ are polynomials in x, y and, most interestingly, in m, of degree $s-1$. We shall re-prove this, after [1], for the sake of self-containment. This proof actually consists in deriving an explicit expression for $B_{s-1}(y,m)$ that will be the key to the proofs of our congruences in the next section. Note also that since the m-th difference of a polynomial of degree less than m is zero, we see from these definitions that both A_{s-1} and B_{s-1} vanish when $s<1$. Then, entering the Vandermonde convolution $\sum_{j=0}^{m+s-1}\binom{x}{j}\binom{ky}{m+s-1-j}=\binom{x+ky}{m+s-1}$ into the definition of $A_{s-1}(x,y,m)$ we obtain

$$A_{s-1}(x,y,m)=\sum_{j=0}^{s-1}\binom{x}{j}B_{s-1-j}(y,m). \tag{5.4}$$

Now, the explicit expression for $B_u(y,m)$ is given.

Theorem 5.1. *Let u be a positive integer. We have*

$$B_u(y,m)=\sum\binom{m}{t_u}\binom{m-t_u}{t_{u-1}}\cdot\cdot\binom{m-t_u-t_{u-1}\cdots-t_2}{t_1}\frac{\binom{y-1}{1}^{t_1}}{2^{t_1}}\frac{\binom{y-1}{2}^{t_2}}{3^{t_2}}\cdot\cdot\frac{\binom{y-1}{u}^{t_u}}{(u+1)^{t_u}},$$

where the sum is over all the partitions of the integer u, that is over all the u-uples of non negative integers $(t_1,t_2,\cdot\cdot t_u)$ such that $\sum_{i=1}^{u} it_i=u$.

This theorem has the following two corollaries.

Corollary 5.1.1. *The B-Adelberg polynomial $B_u(y,m)$ is a polynomial in both m and y of degree u and the A-Adelberg polynomial $A_u(x,y,m)$ is a polynomial of degree u in m, in x and in y. Moreover, $m=0$ and $y=1$ are roots of the polynomials $B_u(y,m)$ for all positive u.*

Proof. From the explicit expression of Theorem 5.1, $B_u(y,m)$ is clearly a polynomial of both y and m, and so is $A_u(x,y,m)$ after Equation (5.4). The degree of B_u is clearly u since $t_1+t_2+\cdot\cdot+t_u$ is less than or equal to u and the equality is reached for the partition made with 1s only. Then, from Equation (5.4), the degree of A_u is also u. Now when $u>0$, $y=1$ is clearly a root of B_u since no partition of the positive integer u has all the $t_j=0$. Also, provided that u is positive, for each partition of u, there is a maximal $j>0$ such that $t_j\neq 0$, so that $\binom{m}{t_j}$ factors out of the corresponding summand, and then m factors out of the whole sum. □

Corollary 5.1.2. *Let p be prime, let $m,x\in\mathbb{Z}$ and let s be an integer such that $0<s<p$. We have $B_{s-1}(p,m)\in\mathbb{Z}$ and $A_{s-1}(x,p,m)\in\mathbb{Z}$.*

Proof. We only need a proof for the B-polynomial, since the proof for the A-polynomial will then follow from Equation (5.4). In the explicit expression of $B_{s-1}(p,m)$ from Theorem 5.1, each factor $\frac{\binom{p-1}{j}}{j+1}=\frac{\binom{p}{j+1}}{p}$ is clearly an integer when $s-1<p-1$, since $j\leq s-1$. □

Proof of Theorem 5.1. This is the proof from [1]. Using the Vandermonde convolution again, the first divided difference with increment y of $\binom{x}{r}$ is

$$\nabla_y \binom{x}{r} = \frac{\binom{x+y}{r} - \binom{x}{r}}{y} = \frac{\sum_{j=0}^{r} \binom{x}{j}\binom{y}{r-j} - \binom{x}{r}}{y} = \frac{\sum_{j=0}^{r-1} \binom{x}{j}\binom{y}{r-j}}{y}.$$

Then, iterating the divided difference operator m times, we have

$$\begin{aligned}\nabla_y^m \binom{x}{r} &= \frac{1}{y^m} \sum_{j_1=0}^{r-1} \sum_{j_2=0}^{j_1-1} \cdot\cdot \sum_{j_m=0}^{j_{m-1}-1} \binom{x}{j_m}\binom{y}{j_{m-1}-j_m} \cdot\cdot \binom{y}{j_1-j_2}\binom{y}{r-j_1} \\ &= \frac{1}{y^m} \sum_{j=0}^{r-m} \binom{x}{j} \sum_{\substack{k_i>0 \\ k_1+k_2\cdot\cdot+k_m=r-j}} \binom{y}{k_m} \cdot\cdot \binom{y}{k_2}\binom{y}{k_1},\end{aligned}$$

where the inner sum in the last line is over all the m-uples of positive integers whose sum is $r-j$. Then by Equation (5.2), we have

$$\begin{aligned}A_u(x,y,m) &= \sum_{j=0}^{u} \binom{x}{j} \frac{1}{y^m} \sum_{\substack{k_i>0 \\ k_1+k_2\cdot\cdot+k_m=m+u-j}} \binom{y}{k_m} \cdot\cdot \binom{y}{k_2}\binom{y}{k_1} \\ &= \sum_{j=0}^{u} \binom{x}{j} \sum_{\substack{k_i>0 \\ k_1+k_2\cdot\cdot+k_m=m+u-j}} \frac{\binom{y-1}{k_m-1} \cdot\cdot \binom{y-1}{k_2-1}\binom{y-1}{k_1-1}}{k_m \cdot\cdot k_2 k_1} \\ &= \sum_{j=0}^{u} \binom{x}{j} \sum_{\substack{k_i\geq 0 \\ k_1+k_2\cdot\cdot+k_m=u-j}} \frac{\binom{y-1}{k_m} \cdot\cdot \binom{y-1}{k_2}\binom{y-1}{k_1}}{(k_m+1)\cdot\cdot(k_2+1)(k_1+1)}.\end{aligned}$$

Then, by comparison with Equation (5.4), we have

$$B_u(y,m) = \sum_{\substack{k_i\geq 0 \\ k_1+k_2\cdot\cdot+k_m=u}} \frac{\binom{y-1}{k_m} \cdot\cdot \binom{y-1}{k_2}\binom{y-1}{k_1}}{(k_m+1)\cdot\cdot(k_2+1)(k_1+1)}, \tag{5.5}$$

where the sum is over all the *weak compositions* of u with m non negative integers. But it is well known that there are $\binom{m}{t_0,t_1,\cdot\cdot,t_m} = \frac{m!}{t_0!t_1!\cdot\cdot t_m!}$ weak compositions of u which produce the same unique *partition* of u in $m-t_0$ summands, such that $u = 0\cdot t_0 + 1\cdot t_1 + \cdots + m\cdot t_m$ and $m = t_0 + t_1 + \cdot\cdot + t_m$. Then

$$B_u(y,m) = \sum_{\substack{t_1+2t_2\cdot\cdot+ut_u=u \\ t_1+t_2\cdot\cdot+t_{s-1}=m-t_0}} \frac{m!}{t_0!t_1!\cdot\cdot t_u!} \left(\frac{\binom{y-1}{0}}{1}\right)^{t_0} \cdot\cdot \left(\frac{\binom{y-1}{u}}{u+1}\right)^{t_u}. \tag{5.6}$$

Now, the multinomial coefficient $\frac{m!}{t_0!t_1!\cdot\cdot t_m!}$ can be expanded as a finite product of binomial coefficients, so that

$$B_u(y,m) = \sum \binom{m}{t_u}\binom{m-t_u}{t_{u-1}} \cdot\cdot \binom{m-t_u-t_{u-1}\cdots - t_2}{t_1} \frac{\binom{y-1}{1}^{t_1}}{2^{t_1}} \frac{\binom{y-1}{2}^{t_2}}{3^{t_2}} \cdot\cdot \frac{\binom{y-1}{u}^{t_u}}{(u+1)^{t_u}},$$

where the sum is over all the partitions of the integer u, that is over all the u-uples of non negative integers $(t_1, t_2, \cdots t_u)$ such that $\sum_{i=1}^{u} it_i = u$. □

From Equation (5.5), we see that $B_u(y,m)$ is the coefficient of z^u in the power series expansion of $\left(\sum_j \frac{\binom{y-1}{j}}{j+1} z^j\right)^m = \left(\frac{(1+z)^y-1}{yz}\right)^m$, so that we have the following generating functions for the Adelberg polynomials [1]:

$$\sum_{u\geq 0} B_u(y,m) z^u = \left(\frac{(1+z)^y - 1}{yz}\right)^m, \tag{5.7}$$

$$\sum_{u\geq 0} A_u(x,y,m) z^u = (1+z)^x \left(\frac{(1+z)^y - 1}{yz}\right)^m, \tag{5.8}$$

where the latter is obtained from the former after accounting for Equation (5.4).

Adelberg gives many *symetries* (or identities) for his polynomials. We will need the symetry (Sxvi) from [1]. It reads

$$\sum_{j\geq 0} \binom{m}{j} y^j A_u(x+j, y, j) = (y+1)^m A_u(x, y+1, j, m) \tag{5.9}$$

and is obtained with the generating function (5.8). As explained in [1], we just need to verify that $\sum_{j\geq 0} \binom{m}{j} y^j (1+z)^{x+j} \left(\frac{(1+z)^y-1}{yz}\right)^j = (y+1)^m (1+z)^x \left(\frac{(1+z)^{y+1}-1}{(y+1)z}\right)^m$, which is elementary.

6. The Second and Third Congruences

We are now ready for our second and third congruences.

Theorem 6.1. *Let p be prime and ℓ, m, s non-negative integers such that $0 < s < p$. We have*

$$\sum_{i\geq 0} (-1)^{m-i} \binom{m}{i} \binom{\ell + ip}{m+s-1} \equiv 0 \pmod{p^m} \tag{6.1}$$

and the quotient is an integer-valued polynomial function of m of degree $s-1$.

Proof. Everything has already been done in the previous section. By definition, the quotient is the Adelberg polynomial $A_{s-1}(\ell, p, m)$ which is integer-valued by Corollary 5.1.2. □

Our third congruence requires slightly more work, as we will need the following generalization of Corollary 5.1.2.

Theorem 6.2. *Let p be prime, ℓ, m non-negative integers and s an integer such that $0 < s < p$. We have $p^\ell B_{\ell(p-1)+s-1}(p,m) \in \mathbb{Z}$ and $p^\ell A_{\ell(p-1)+s-1}(s-1,p,m) \in \mathbb{Z}$. In other words, for any non negative integer u, r being the residue of the Euclidean division of u by $p-1$, we have $p^{\lfloor \frac{u}{p-1} \rfloor} B_u(p,m) \in \mathbb{Z}$ and $p^{\lfloor \frac{u}{p-1} \rfloor} A_u(r,p,m) \in \mathbb{Z}$.*

Proof. In the case where $y = p$ a prime number, we may rewrite the Equation (5.6) for $B_u(y,m)$ slightly differently:

$$B_u(p,m) = \sum_{t_1+2t_2 \cdot\cdot + ut_u = u} \frac{m!}{t_0! t_1! \cdot \cdot t_u!} \left(\frac{\binom{p}{2}}{p} \right)^{t_1} \cdot\cdot \left(\frac{\binom{p}{u+1}}{p} \right)^{t_u}.$$

The partitions of u for which there exist $j \geq p$ such that $t_j \neq 0$ do not contribute to the sum because when $j \geq p$, we have $\binom{p}{j+1} = 0$ and then

$$\begin{aligned} B_u(p,m) &= \sum_{t_1+2t_2 \cdot\cdot + (p-1)t_{p-1} = u} \frac{m!}{t_0! t_1! \cdot \cdot t_{p-1}!} \left(\frac{\binom{p}{2}}{p} \right)^{t_1} \cdot\cdot \left(\frac{\binom{p}{p}}{p} \right)^{t_{p-1}} \\ &= \sum_{t_1+2t_2 \cdot\cdot + (p-1)t_{p-1} = u} \frac{m!}{t_0! t_1! \cdot \cdot t_{p-1}!} \left(\frac{\binom{p}{2}}{p} \right)^{t_1} \cdot\cdot \left(\frac{\binom{p}{p-1}}{p} \right)^{t_{p-2}} \frac{1}{p^{t_{p-1}}}. \end{aligned}$$

Now, we let $u = \ell(p-1) + s - 1$ and we obtain

$$p^\ell B_{\ell(p-1)+s-1}(p,m) = \sum \frac{m!}{t_0! t_1! \cdot \cdot t_{p-1}!} \left(\frac{\binom{p}{2}}{p} \right)^{t_1} \cdot\cdot \left(\frac{\binom{p}{p-1}}{p} \right)^{t_{p-2}} p^{\ell - t_{p-1}},$$

where the sum is over all the $(p-1)$-uples of non-negative integers $(t_1, \cdot\cdot t_{p-1})$ such that $t_1 + 2t_2 \cdot\cdot + (p-1)t_{p-1} = \ell(p-1) + s - 1$. We see that $p^\ell B_{\ell(p-1)+s-1}(p,m) \in \mathbb{Z}$ because if $t_{p-1} \geq \ell + 1$, then we would have $\ell(p-1) + s - 1 \geq (p-1)t_{p-1} \geq \ell(p-1) + p - 1$, which is not possible since it is supposed that $s < p$. Now, it follows that $p^\ell A_{\ell(p-1)+s-1}(s-1,p,m)$ is integer because

$$\begin{aligned} p^\ell A_{\ell(p-1)+s-1}(s-1,p,m) &= \sum_{j=0}^{\ell(p-1)+s-1} \binom{s-1}{j} p^\ell B_{\ell(p-1)+s-1-j}(p,m) \\ &= \sum_{j=0}^{s-1} \binom{s-1}{j} p^\ell B_{\ell(p-1)+s-1-j}(p,m). \end{aligned}$$

□

Theorem 6.3. *Let p be prime and ℓ, m, s integers such that $0 < s < p$. We have*

$$\sum_{j,i \geq \ell} (-1)^{j-i} \binom{m}{j} \binom{j}{i} \binom{j+s-1+i(p-1)}{j+s-1+\ell(p-1)} \equiv 0 \pmod{p^{m-\ell}}.$$

The quotient is an integer-valued polynomial function of m of degree $s-1+\ell(p-1)$.

Proof. We start from Equation (5.9) where we let $y = p-1$ and $u = \ell(p-1)+s-1$. We replace the Adelberg polynomial on the right-hand side by its original definition, rearrange the sums and then we obtain

$$\sum_{j,i\geq \ell}(-1)^{j-i}\binom{m}{j}\binom{j}{i}\binom{j+s-1+i(p-1)}{j+s-1+\ell(p-1)} = p^m A_{\ell(p-1)+s-1}(s-1,p,m)$$
$$= p^{m-\ell}p^\ell A_{\ell(p-1)+s-1}(s-1,p,m).$$

The claim then follows from Theorem 6.2. □

Remark. When $0 \leq n < \ell$, it is clear that $A_{\ell(p-1)+s-1}(s-1,p,n) = 0$ and we have $p^\ell A_{\ell(p-1)+s-1}(s-1,p,\ell) = 1$. Let

$$s_{p,s,\ell}(m) := \sum_{i\geq \ell}(-1)^{m-i}\binom{m}{i}\binom{m+s-1+i(p-1)}{m+s-1+\ell(p-1)}.$$

We have

$$p^m A_{\ell(p-1)+s-1}(s-1,p,m) = \sum_j \binom{m}{j} s_{p,s,\ell}(j),$$

so that $p^m A_{\ell(p-1)+s-1}(s-1,p,m)$ is a *binomial transform* of $s_{p,s,\ell}(m)$ where we consider $s_{p,s,\ell}(m)$ as an integer sequence with index m. Equivalently, by binomial inversion, we have

$$\begin{aligned} s_{p,s,\ell}(m) &= \sum_j (-1)^{m-j}\binom{m}{j} p^j A_{\ell(p-1)+s-1}(s-1,p,j) \\ &= \sum_{j\geq \ell}(-1)^{m-j}\binom{m}{j} p^{j-\ell}p^\ell A_{\ell(p-1)+s-1}(s-1,p,j) \\ &= (-1)^{m-\ell}\binom{m}{\ell} + \sum_{j\geq 1} p^j (-1)^{m-j-\ell}\binom{m}{j+\ell} p^\ell A_{\ell(p-1)+s-1}(s-1,p,j+\ell). \end{aligned}$$

But the right-hand side of Congruence (4.3) is $s_{p,s,\ell}(m) - (-1)^{m-\ell}\binom{m}{\ell}$ and we see that our first congruence also follows from the above derivation.

7. Examples and Final Remarks

With appropriate changes of variables and index, the Adelberg polynomials are actually degenerate Bernoulli polynomials of arbitrary order [1]. But Adelberg writes that his polynomials have *a more combinatorial flavor* and *show more of the landscape*. His approach also provides an effective way to compute our lacunary sums of products of binomial coefficients, via Theorem 5.1 and Equation (5.4). The result of such computations for the first few Adelberg polynomials is displayed in the following tables.

u	$B_u(y,m)$
0	1
1	$\frac{1}{2}m(-1+y)$
2	$\frac{1}{24}m(-1+y)(-5-3m+y+3my)$
3	$\frac{1}{48}m(-1+y)(-2-m+my)(-3-m+y+my)$
4	$\frac{1}{5760}m(-1+y)(-502-485m-150m^2-15m^3+218y+655my+330m^2y+45m^3y$ $-2y^2-175my^2-210m^2y^2-45m^3y^2-2y^3+5my^3+30m^2y^3$ $+15m^3y^3)$

Table 1: The first five B-Adelberg polynomials.

u	$A_u(x,y,m)$
0	1
1	$\frac{1}{2}(-m+2x+my)$
2	$\frac{1}{24}(5m+3m^2-12x-12mx+12x^2-6my-6m^2y+12mxy+my^2+3m^2y^2)$
3	$\frac{(-2-m+2x+my)}{48}(3m+m^2-8x-4mx+4x^2-4my-2m^2y+4mxy+my^2+m^2y^2)$

Table 2: The first four A-Adelberg polynomials.

We can also write many impressive-looking binomial identities like, for instance:

$$\sum_{i\geq 0}(-1)^{m-i}\binom{m}{i}\binom{\ell+in}{m+2} = \frac{n^m}{24}\big(5m+3m^2-12\ell-12m\ell+12\ell^2-6mn-6m^2n + 12m\ell n+mn^2+3m^2n^2\big),$$

or

$$\sum_{j,i\geq 0}(-1)^{j-i}\binom{m}{j}\binom{j}{i}\binom{j+5+6i}{j+5} = 7^m\,\frac{(m+1)(81m^4+684m^3+1401m^2+434m+40)}{40}.$$

The polynomial part on the right-hand side of these identities is integer-valued when the number which is raised to the power m is a prime number larger than s.

We conclude the paper by a comparison of our *Adelberg*-congruences with the Fleck-like congruences reported in the introduction. They are similar by the fact that for both kinds of congruences, the most inner sum is indeed lacunary: one of the two indices of the binomial coefficient is from an arithmetic progression with a ratio larger than 1, but they differ by which index. In the Fleck-like congruences, the lower index of the binomial coefficient is lacunary, whereas the upper index is lacunary in our work.

Illustrating further this aspect, we rewrite Congruence (6.1) together with Wan congruence, but in a different form, highlighting the similarity and the difference. For p prime, and non-negative integers m, ℓ and r, we have

$$\sum_{k\equiv r \bmod p} (-1)^{\lfloor \frac{k}{p} \rfloor} \binom{\lfloor \frac{m}{p-1} \rfloor (p-1)}{\lfloor \frac{k}{p} \rfloor} \binom{k}{m} \equiv 0 \quad \bmod p^{\lfloor \frac{m}{p-1} \rfloor (p-1)},$$

$$\sum_{k\equiv r \bmod p} (-1)^{\lfloor \frac{k}{p} \rfloor} \binom{\lfloor \frac{k}{p} \rfloor}{\ell} \binom{m}{k} \equiv 0 \quad \bmod p^{\lfloor \frac{m-p\ell-1}{p-1} \rfloor}.$$

Note that, written in this form, the validity of the first one also requires the supplementary condition that $p-1$ does not divide m.

Acknowledgement. The author is indebted to Marko Riedel for the proof of Theorem 3.1.

References

[1] A. Adelberg, A finite difference approach to degenerate Bernoulli and Stirling polynomials *Discrete Math.* **140** (1995), 1-21.

[2] R.L. Graham, D.E. Knuth and O. Patashnik, *Concrete Mathematics*, Second Ed., Adison-Wesley Publishing Company, Reading, Massachusetts, 1994.

[3] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic mathematics*, Proceedings of the workshop, Simon Fraser University, Burnaby, Canada, December 12-14, 1997.

[4] R. Peele, A.J. Radcliffe and H.S. Wilf, Congruence problems involving Stirling numbers of the first kind, *Fibonacci Quart.* **31** (1993), 73-80.

[5] M. Riedel, A three-parameters identity involving Stirling numbers of both kinds, URL (version: 2020-03-24): https://math.stackexchange.com/q/3592354.

[6] Z.W. Sun, Polynomial extension of Fleck's congruence, *Acta Arith.* **122** (2006), 91-100.

[7] Z.W. Sun and R. Tauraso, Congruences for sums of binomial coefficients, *J. Number Theory* **126** (2007), 287-296.