Fleck's binomial congruence using circulant matrices

Darij Grinberg

July 14, 2019

Contents

1. Fleck's congruence

Definition 1.1. Let $\mathbb{N}$ denote the set $\{0, 1, 2, \ldots\}$.

The following elementary theorem appears, e.g., in [SchWal12] and in [Granvi05, (12)]:

Theorem 1.2. Let p be a prime. Let $j \in \mathbb{Z}$, $n \in \mathbb{N}$ and $q \in \mathbb{N}$ be such that $q \leq \dfrac{n-1}{p-1}$. Then,

$$\sum_{\substack{m \in \mathbb{N}; \\ m \equiv j \bmod p}} (-1)^m \binom{n}{m} \equiv 0 \bmod p^q.$$

(The sum on the left hand side of this congruence is well-defined, because every $m > n$ satisfies $\dbinom{n}{m} = 0$.)

Theorem 1.2 was found in A. Fleck in 1913. In [Granvi05], it is proven using cyclotomic integers. Here, we shall instead give a proof using nothing more advanced than polynomials and matrix multiplication. The tactic used in the following proof is similar to that used in [Grinbe15] (viz., proving congruences of integers by interpreting them as single-entry pieces of matrix-valued congruences in commutative subrings of matrix rings), and is probably helpful more often.

2. Preliminaries: Iverson brackets and circulant matrices

We now start preparing for the proof of Theorem 1.2. Let us first agree on some notations.

Definition 2.1. We shall use the *Iverson bracket notation*: If $\mathcal{S}$ is a logical statement, then $[\mathcal{S}]$ will mean the integer $\begin{cases} 1, & \text{if } \mathcal{S} \text{ is true;} \\ 0, & \text{if } \mathcal{S} \text{ is false} \end{cases}$.

The Iverson bracket can be used for counting (or, rather, for neatly writing up counting arguments), via the following simple result:

Proposition 2.2. Let $\mathbf{K}$ be a set. For each $k \in \mathbf{K}$, let $\mathcal{A}(k)$ be some logical statement. Then,

$$\sum_{k \in \mathbf{K}} [\mathcal{A}(k)] = (\text{the number of all } k \in \mathbf{K} \text{ satisfying } \mathcal{A}(k)).$$

Proof of Proposition 2.2. We have

$$\begin{aligned}
\sum_{k \in \mathbf{K}} [\mathcal{A}(k)] &= \sum_{\substack{k \in \mathbf{K}; \\ \mathcal{A}(k) \text{ is true}}} \underbrace{[\mathcal{A}(k)]}_{\substack{=1 \\ (\text{since } \mathcal{A}(k) \text{ is true})}} + \sum_{\substack{k \in \mathbf{K}; \\ \mathcal{A}(k) \text{ is false}}} \underbrace{[\mathcal{A}(k)]}_{\substack{=0 \\ (\text{since } \mathcal{A}(k) \text{ is false})}} \\
&= \sum_{\substack{k \in \mathbf{K}; \\ \mathcal{A}(k) \text{ is true}}} 1 + \underbrace{\sum_{\substack{k \in \mathbf{K}; \\ \mathcal{A}(k) \text{ is false}}} 0}_{=0} = \sum_{\substack{k \in \mathbf{K}; \\ \mathcal{A}(k) \text{ is true}}} 1 \\
&= (\text{the number of all } k \in \mathbf{K} \text{ for which } \mathcal{A}(k) \text{ is true}) \cdot 1 \\
&= (\text{the number of all } k \in \mathbf{K} \text{ for which } \mathcal{A}(k) \text{ is true}) \\
&= (\text{the number of all } k \in \mathbf{K} \text{ satisfying } \mathcal{A}(k)).
\end{aligned}$$

This proves Proposition 2.2. □

Definition 2.3. In the following, all matrices are understood to have integer entries.

Definition 2.4. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

(a) If S is an $n \times m$-matrix, and if $(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}$, then we will denote the (i,j)-th entry of S by $S_{i,j}$.

(b) If $a_{i,j}$ is an integer for every $i \in \{1,2,\ldots,n\}$ and $j \in \{1,2,\ldots,m\}$, then we let $\left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ denote the $n \times m$-matrix whose (i,j)-th entry is $a_{i,j}$ for all $(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}$.

Thus, any $n \times m$-matrix S satisfies $S = \left(S_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$. Moreover, the definition of the product of two matrices can be stated as follows: For any $n \in \mathbb{N}$, any $m \in \mathbb{N}$, any $\ell \in \mathbb{N}$, any $n \times m$-matrix $\left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ and any $m \times \ell$-matrix $\left(b_{i,j}\right)_{1 \leq i \leq m,\ 1 \leq j \leq \ell}$, we have

$$\left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m} \left(b_{i,j}\right)_{1 \leq i \leq m,\ 1 \leq j \leq \ell} = \left(\sum_{k=1}^{m} a_{i,k} b_{k,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq \ell}. \tag{1}$$

Definition 2.5. Let p be a positive integer. Let S_p be the $p \times p$-matrix $\left([j \equiv i+1 \bmod p]\right)_{1 \leq i \leq p,\ 1 \leq j \leq p}$. Let I_p denote the $p \times p$ identity matrix.

For example, $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $S_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

Roughly speaking, the $p \times p$-matrix S_p can be viewed as the result of "moving I_p one column to the right" in a cyclic way (i.e., each column apart from the last one moves one unit to the right, whereas the last one moves to the front). More formally, S_p is the permutation matrix of a cyclic permutation. From this point of view, the following proposition should be rather obvious:

Proposition 2.6. Let p be a positive integer. Let $k \in \mathbb{N}$. Then,

$$\left(S_p\right)^k = \left([j \equiv i+k \bmod p]\right)_{1 \leq i \leq p,\ 1 \leq j \leq p}.$$

For the sake of completeness, let me give a formal proof of this proposition:

Proof of Proposition 2.6. We shall prove Proposition 2.6 by induction over k:

Induction base: The definition of the identity matrix I_p yields $I_p = \left([i=j]\right)_{1 \leq i \leq p,\ 1 \leq j \leq p}$. But if i and j are two elements of $\{1,2,\ldots,p\}$, then $[j \equiv i+0 \bmod p] = [i=j]$ [1].

[1] *Proof.* Let i and j be two elements of $\{1,2,\ldots,p\}$. Then, $i \equiv j \bmod p$ holds if and only if $i=j$ (because no two distinct elements of $\{1,2,\ldots,p\}$ are congruent to each other modulo

Hence, $\left(\underbrace{[j \equiv i+0 \bmod p]}_{=[i=j]} \right)_{1 \leq i \leq p,\ 1 \leq j \leq p} = ([i=j])_{1 \leq i \leq p,\ 1 \leq j \leq p}$. Comparing this with $\left(S_p\right)^0 = I_p = ([i=j])_{1 \leq i \leq p,\ 1 \leq j \leq p}$, we obtain $\left(S_p\right)^0 = ([j \equiv i+0 \bmod p])_{1 \leq i \leq p,\ 1 \leq j \leq p}$. In other words, Proposition 2.6 holds for $k=0$. This completes the induction base.

Induction step: Let $K \in \mathbb{N}$. Assume that Proposition 2.6 holds for $k=K$. We now must prove that Proposition 2.6 holds for $k=K+1$.

We have assumed that Proposition 2.6 holds for $k=K$. In other words, we have

$$\left(S_p\right)^K = ([j \equiv i+K \bmod p])_{1 \leq i \leq p,\ 1 \leq j \leq p}. \tag{2}$$

For every $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,p\}$, we have

$$\begin{aligned} &[k \equiv i+K \bmod p]\,[j \equiv k+1 \bmod p] \\ &= [k \equiv i+K \bmod p]\,[j \equiv i+(K+1) \bmod p]. \end{aligned} \tag{3}$$

[*Proof of (3):* Let $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,p\}$. We must prove the equality (3). We are in one of the following two cases:

Case 1: We have $k \equiv i+K \bmod p$.

Case 2: We don't have $k \equiv i+K \bmod p$.

Let us first consider Case 1. In this case, we have $k \equiv i+K \bmod p$. Thus, $\underbrace{k}_{\equiv i+K \bmod p} +1 \equiv i+K+1 = i+(K+1) \bmod p$. Therefore, we have $j \equiv k+1 \bmod p$ if and only if $j \equiv i+(K+1) \bmod p$. Therefore, $[j \equiv k+1 \bmod p] = [j \equiv i+(K+1) \bmod p]$. Now,

$$\begin{aligned} &[k \equiv i+K \bmod p]\,\underbrace{[j \equiv k+1 \bmod p]}_{=[j \equiv i+(K+1) \bmod p]} \\ &= [k \equiv i+K \bmod p]\,[j \equiv i+(K+1) \bmod p]. \end{aligned}$$

Hence, (3) is proven in Case 1.

Let us now consider Case 2. In this case, we don't have $k \equiv i+K \bmod p$. Thus, $[k \equiv i+K \bmod p] = 0$. Since $[k \equiv i+K \bmod p]$ appears as a factor on both sides of (3), this shows that both sides of (3) are 0. Thus, (3) is proven in Case 2.

---

p). Thus, we have $[i \equiv j \bmod p] = [i=j]$. Now,

$$\left[j \equiv \underbrace{i+0}_{=i} \bmod p \right] = \left[\underbrace{j \equiv i \bmod p}_{\substack{\text{this is equivalent to} \\ (i \equiv j \bmod p)}} \right] = [i \equiv j \bmod p] = [i=j].$$

Qed.

We now have proven (3) in each of the two Cases 1 and 2. Thus, (3) always holds. Qed.]

For every $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,p\}$, we have

$$\begin{aligned} &\sum_{k=1}^{p} [k \equiv i+K \bmod p]\,[j \equiv k+1 \bmod p] \\ &= [j \equiv i+(K+1) \bmod p] \end{aligned} \tag{4}$$

[2].

[2] *Proof of (4):* Let $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,p\}$.

The following fact is well-known: The integers $1,2,\ldots,p$ cover each of the remainder classes modulo p exactly once. In other words, for every integer N, there is exactly one $k \in \{1,2,\ldots,p\}$ satisfying $k \equiv N \bmod p$. In other words, for each integer N, we have

$$(\text{the number of all } k \in \{1,2,\ldots,p\} \text{ satisfying } k \equiv N \bmod p) = 1. \tag{5}$$

But

$$\begin{aligned} &\underbrace{\sum_{k=1}^{p}}_{=\sum_{k\in\{1,2,\ldots,p\}}} \underbrace{[k \equiv i+K \bmod p]\,[j \equiv k+1 \bmod p]}_{=[k\equiv i+K \bmod p]\,[j\equiv i+(K+1) \bmod p] \text{ (by (3))}} \\ &= \sum_{k\in\{1,2,\ldots,p\}} [k \equiv i+K \bmod p]\,[j \equiv i+(K+1) \bmod p] \\ &= [j \equiv i+(K+1) \bmod p] \cdot \underbrace{\sum_{k\in\{1,2,\ldots,p\}} [k \equiv i+K \bmod p]}_{=(\text{the number of all } k\in\{1,2,\ldots,p\} \text{ satisfying } k\equiv i+K \bmod p) \text{ (by Proposition 2.2 (applied to } \mathbf{K}=\{1,2,\ldots,p\} \text{ and } \mathcal{A}(k)=(\text{“}k\equiv i+K \bmod p\text{”}))} \\ &= [j \equiv i+(K+1) \bmod p] \cdot \underbrace{(\text{the number of all } k \in \{1,2,\ldots,p\} \text{ satisfying } k \equiv i+K \bmod p)}_{=1 \text{ (by (5) (applied to } N=i+K))} \\ &= [j \equiv i+(K+1) \bmod p]\,. \end{aligned}$$

This proves (4).

Now,

$$\begin{aligned}
\left(S_p\right)^{K+1} &= \underbrace{\left(S_p\right)^{K}}_{=([j\equiv i+K \bmod p])_{1\leq i\leq p,\ 1\leq j\leq p}} \underbrace{S_p}_{=([j\equiv i+1 \bmod p])_{1\leq i\leq p,\ 1\leq j\leq p}} \\
&= \left([j \equiv i+K \bmod p]\right)_{1\leq i\leq p,\ 1\leq j\leq p} \left([j \equiv i+1 \bmod p]\right)_{1\leq i\leq p,\ 1\leq j\leq p} \\
&= \left(\underbrace{\sum_{k=1}^{p} [k \equiv i+K \bmod p]\,[j \equiv k+1 \bmod p]}_{\substack{=[j\equiv i+(K+1) \bmod p] \\ \text{(by (4))}}} \right)_{1\leq i\leq p,\ 1\leq j\leq p} \\
&\qquad \left(\begin{array}{c} \text{by (1), applied to } n=p,\ m=p,\ \ell=p, \\ a_{i,j}=[j\equiv i+K \bmod p] \text{ and } b_{i,j}=[j\equiv i+1 \bmod p] \end{array} \right) \\
&= \left([j \equiv i+(K+1) \bmod p]\right)_{1\leq i\leq p,\ 1\leq j\leq p}.
\end{aligned}$$

In other words, Proposition 2.6 holds for $k = K+1$. This completes the induction step.

Thus, Proposition 2.6 is proven by induction. □

Corollary 2.7. Let p be a positive integer. Let $k \in \mathbb{N}$. Let $u \in \{1,2,\ldots,p\}$ and $v \in \{1,2,\ldots,p\}$. Then,

$$\left(\left(S_p\right)^k\right)_{u,v} = [v \equiv u+k \bmod p].$$

Proof of Corollary 2.7. Proposition 2.6 yields $\left(S_p\right)^k = \left([j \equiv i+k \bmod p]\right)_{1\leq i\leq p,\ 1\leq j\leq p}$. Hence, $\left(\left(S_p\right)^k\right)_{u,v} = \left(\left([j \equiv i+k \bmod p]\right)_{1\leq i\leq p,\ 1\leq j\leq p}\right)_{u,v} = [v \equiv u+k \bmod p]$. This proves Corollary 2.7. □

Corollary 2.8. Let p be a positive integer. Then, $\left(S_p\right)^p = I_p$.

Proof of Corollary 2.8. For every $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,p\}$, we have

$$\left[\underbrace{j \equiv i+p \bmod p}_{\substack{\text{this is equivalent to} \\ j\equiv i+0 \bmod p \\ \text{(since } i+p\equiv i=i+0 \bmod p\text{)}}} \right] = [j \equiv i+0 \bmod p]. \tag{6}$$

Proposition 2.6 (applied to $k = 0$) yields

$$\left(S_p\right)^0 = \left([j \equiv i+0 \bmod p]\right)_{1\leq i\leq p,\ 1\leq j\leq p}. \tag{7}$$

Proposition 2.6 (applied to $k = p$) yields

$$\begin{aligned}
\left(S_p\right)^p &= \left(\underbrace{[j \equiv i + p \bmod p]}_{\substack{=[j \equiv i+0 \bmod p] \\ \text{(by (6))}}} \right)_{1 \leq i \leq p,\ 1 \leq j \leq p} \qquad = \left([j \equiv i + 0 \bmod p]\right)_{1 \leq i \leq p,\ 1 \leq j \leq p} \\
&= \left(S_p\right)^0 \qquad \text{(by (7))} \\
&= I_p.
\end{aligned}$$

This proves Corollary 2.8. □

Corollary 2.9. Let p be a positive integer. Let $j \in \{0, 1, \ldots, p-1\}$ and $n \in \mathbb{N}$. Then,

$$\sum_{\substack{m \in \mathbb{N}; \\ m \equiv j \bmod p}} (-1)^m \binom{n}{m} = \left(\left(I_p - S_p\right)^n\right)_{1, j+1}.$$

To prove Corollary 2.9, we shall need the binomial formula, in the following form:

Proposition 2.10. Let $x \in \mathbb{N}$. Then,

$$(1 + X)^x = \sum_{k \in \mathbb{N}} \binom{x}{k} X^k$$

(an equality between polynomials in $\mathbb{Z}[X]$). (The sum $\sum_{k \in \mathbb{N}} \binom{x}{k} X^k$ is an infinite sum, but only finitely many of its addends are nonzero, so it is well-defined.)

Proof of Corollary 2.9. We have $1 \in \{1, 2, \ldots, p\}$ (since p is positive) and $j + 1 \in \{1, 2, \ldots, p\}$ (since $j \in \{0, 1, \ldots, p-1\}$). Hence, every $k \in \mathbb{N}$ satisfies

$$\begin{aligned}
\left(\left(S_p\right)^k\right)_{1, j+1} &= \left[j + 1 \equiv \underbrace{1 + k}_{=k+1} \bmod p \right] \\
&\qquad \text{(by Corollary 2.7 (applied to } u = 1 \text{ and } v = j + 1)) \\
&= \left[\underbrace{j + 1 \equiv k + 1 \bmod p}_{\substack{\text{this is equivalent to} \\ j \equiv k \bmod p}} \right] = \left[\underbrace{j \equiv k \bmod p}_{\substack{\text{this is equivalent to} \\ k \equiv j \bmod p}} \right] \\
&= [k \equiv j \bmod p]. \qquad (8)
\end{aligned}$$

Proposition 2.10 (applied to $x = n$) yields $(1+X)^n = \sum_{k\in\mathbb{N}} \binom{n}{k} X^k$ (an equality between polynomials in $\mathbb{Z}[X]$). If we substitute $-S_p$ for X in this equality, then we obtain $\left(I_p + \left(-S_p\right)\right)^n = \sum_{k\in\mathbb{N}} \binom{n}{k} \left(-S_p\right)^k$ (since the unity of the ring of $p \times p$-matrices is I_p). Thus,

$$\begin{aligned}\left(\underbrace{I_p - S_p}_{=I_p+\left(-S_p\right)}\right)^n &= \left(I_p + \left(-S_p\right)\right)^n = \sum_{k\in\mathbb{N}} \binom{n}{k} \underbrace{\left(-S_p\right)^k}_{=(-1)^k \left(S_p\right)^k} \\ &= \sum_{k\in\mathbb{N}} \binom{n}{k} (-1)^k \left(S_p\right)^k = \sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} \left(S_p\right)^k.\end{aligned}$$

Thus,

$$\begin{aligned}&\left(\underbrace{\left(I_p - S_p\right)^n}_{=\sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} \left(S_p\right)^k}\right)_{1,j+1} \\ &= \left(\sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} \left(S_p\right)^k\right)_{1,j+1} = \sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} \underbrace{\left(\left(S_p\right)^k\right)_{1,j+1}}_{\substack{=[k\equiv j \bmod p] \\ \text{(by (8))}}} \\ &= \sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} [k \equiv j \bmod p] \\ &= \sum_{\substack{k\in\mathbb{N}; \\ k\equiv j \bmod p}} (-1)^k \binom{n}{k} \underbrace{[k \equiv j \bmod p]}_{\substack{=1 \\ \text{(since } k\equiv j \bmod p\text{)}}} + \sum_{\substack{k\in\mathbb{N}; \\ k\not\equiv j \bmod p}} (-1)^k \binom{n}{k} \underbrace{[k \equiv j \bmod p]}_{\substack{=0 \\ \text{(since } k\not\equiv j \bmod p\text{)}}} \\ &= \sum_{\substack{k\in\mathbb{N}; \\ k\equiv j \bmod p}} (-1)^k \binom{n}{k} = \sum_{\substack{m\in\mathbb{N}; \\ m\equiv j \bmod p}} (-1)^m \binom{n}{m}\end{aligned}$$

(here, we have renamed the summation index k as m). This proves Corollary 2.9. □

3. The polynomial U

On the other hand, let us recall a standard property of primes:

Proposition 3.1. Let p be a prime. Let $k \in \{0, 1, \ldots, p-1\}$. Then,

$$\binom{p-1}{k} \equiv (-1)^k \bmod p.$$

Proposition 3.1 is well-known; we give its proof in the appendix (Section 5) for the sake of completeness.

Corollary 3.2. Let p be a prime. For every $k \in \{0, 1, \ldots, p-1\}$, we have $\dfrac{(-1)^k \dbinom{p-1}{k} - 1}{p} \in \mathbb{Z}$.

Proof of Corollary 3.2. Let $k \in \{0, 1, \ldots, p-1\}$. Then, Proposition 3.1 shows that $\dbinom{p-1}{k} \equiv (-1)^k \bmod p$. Hence,

$$(-1)^k \underbrace{\binom{p-1}{k}}_{\equiv (-1)^k \bmod p} \equiv (-1)^k (-1)^k = \left((-1)^k\right)^2 = 1 \bmod p$$

(since $(-1)^k \in \{1, -1\}$). In other words, $p \mid (-1)^k \dbinom{p-1}{k} - 1$. In other words, $\dfrac{(-1)^k \dbinom{p-1}{k} - 1}{p} \in \mathbb{Z}$. This proves Corollary 3.2. □

We recall that $\mathbb{Z}[X]$ denotes the ring of all polynomials in one indeterminate X with integer coefficients.

Corollary 3.3. Let p be a prime. Then, there exists a polynomial $U \in \mathbb{Z}[X]$ such that $(1-X)^p = (1-X^p) + p(1-X)U$.

Proof of Corollary 3.3. For every $k \in \{0, 1, \ldots, p-1\}$, we have $\dfrac{(-1)^k \dbinom{p-1}{k} - 1}{p} \in \mathbb{Z}$ (by Corollary 3.2). Thus, for every $k \in \{0, 1, \ldots, p-1\}$, we can define an element $a_k \in \mathbb{Z}$ by $a_k = \dfrac{(-1)^k \dbinom{p-1}{k} - 1}{p}$. Consider these elements a_k. Every $k \in \{0, 1, \ldots, p-1\}$ satisfies

$$pa_k = (-1)^k \binom{p-1}{k} - 1 \tag{9}$$

(since $a_k = \dfrac{(-1)^k \binom{p-1}{k} - 1}{p}$).

Define a polynomial $A \in \mathbb{Z}[X]$ by $A = \sum_{k=0}^{p-1} a_k X^k$.

The binomial formula says the following: If a and b are any two elements of a commutative ring $\mathfrak{A}$, and if $g \in \mathbb{N}$, then

$$(a+b)^g = \sum_{k=0}^{g} \binom{g}{k} a^k b^{g-k}.$$

This formula (applied to $\mathfrak{A} = \mathbb{Z}[X]$, $a = -X$, $b = 1$ and $g = p-1$) yields

$$\begin{aligned}((-X)+1)^{p-1} &= \sum_{k=0}^{p-1} \binom{p-1}{k} \underbrace{(-X)^k}_{=(-1)^k X^k} \underbrace{1^{p-1-k}}_{=1} \\ &= \sum_{k=0}^{p-1} \underbrace{\binom{p-1}{k} (-1)^k}_{=(-1)^k \binom{p-1}{k}} X^k = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} X^k.\end{aligned}$$

Since $(-X)+1 = 1-X$, this rewrites as follows:

$$(1-X)^{p-1} = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} X^k. \tag{10}$$

On the other hand, a well-known identity states the following: If a and b are any two elements of a commutative ring $\mathfrak{A}$, and if $g \in \mathbb{N}$, then

$$a^g - b^g = (a-b) \sum_{k=0}^{g-1} a^k b^{g-1-k}.$$

This formula (applied to $\mathfrak{A} = \mathbb{Z}[X]$, $a = 1$, $b = X$ and $g = p$) yields

$$\begin{aligned}1^p - X^p &= (1-X) \sum_{k=0}^{p-1} \underbrace{1^k}_{=1} X^{p-1-k} = (1-X) \sum_{k=0}^{p-1} X^{p-1-k} \\ &= (1-X) \sum_{k=0}^{p-1} X^k \end{aligned} \tag{11}$$

(here, we have substituted k for $p-1-k$ in the sum).

Now,

$$\begin{aligned}
&\underbrace{(1-X)^p}_{=(1-X)(1-X)^{p-1}} - \left(\underbrace{1}_{=1^p} - X^p\right) \\
&= (1-X)(1-X)^{p-1} - \underbrace{\left(1^p - X^p\right)}_{\substack{=(1-X)\sum_{k=0}^{p-1} X^k \\ \text{(by (11))}}} \\
&= (1-X)(1-X)^{p-1} - (1-X)\sum_{k=0}^{p-1} X^k = (1-X)\left((1-X)^{p-1} - \sum_{k=0}^{p-1} X^k\right).
\end{aligned}$$

Since

$$\begin{aligned}
&\underbrace{(1-X)^{p-1}}_{\substack{=\sum_{k=0}^{p-1}(-1)^k\binom{p-1}{k}X^k \\ \text{(by (10))}}} - \sum_{k=0}^{p-1} X^k \\
&= \sum_{k=0}^{p-1}(-1)^k\binom{p-1}{k}X^k - \sum_{k=0}^{p-1} X^k = \sum_{k=0}^{p-1}\underbrace{\left((-1)^k\binom{p-1}{k} - 1\right)}_{\substack{=pa_k \\ \text{(by (9))}}}X^k \\
&= \sum_{k=0}^{p-1} pa_k X^k = p\underbrace{\sum_{k=0}^{p-1} a_k X^k}_{\substack{=A \\ \text{(since } A=\sum_{k=0}^{p-1} a_k X^k\text{)}}} = pA,
\end{aligned}$$

this becomes

$$\begin{aligned}
(1-X)^p - (1-X)^p &= (1-X)\underbrace{\left((1-X)^{p-1} - \sum_{k=0}^{p-1} X^k\right)}_{=pA} \\
&= (1-X)\,pA = p\,(1-X)\,A.
\end{aligned}$$

In other words, $(1-X)^p = (1-X^p) + p\,(1-X)\,A$. Hence, there exists a polynomial $U \in \mathbb{Z}[X]$ such that $(1-X)^p = (1-X^p) + p\,(1-X)\,U$ (namely, $U = A$). This proves Corollary 3.3. □

4. Back to the matrix

We now shall use the polynomial U from Corollary 3.3 to factor out powers of p from powers of $I_p - S_p$ when p is a prime.

Proposition 4.1. Let p be a prime. Corollary 3.3 shows that there exists a polynomial $U \in \mathbb{Z}[X]$ such that $(1-X)^p = (1-X^p) + p(1-X)U$. Consider this U.

Let $U_p = U(S_p)$. (This is the $p \times p$-matrix obtained by substituting the matrix S_p for X in the polynomial U.)

(a) We have $(I_p - S_p) U_p = U_p (I_p - S_p)$.

(b) We have $(I_p - S_p)^p = p (I_p - S_p) U_p$.

(c) For every $q \in \mathbb{N}$, we have

$$(I_p - S_p)^{q(p-1)+1} = p^q (I_p - S_p) (U_p)^q.$$

We shall now prove this proposition. Our proof will use some very basic abstract algebra (namely, the notion of a $\mathbb{Z}$-subalgebra generated by some elements, and the fact that any $\mathbb{Z}$-algebra generated by a single element is commutative). We shall show a way to avoid this proposition in the appendix (Section 6).

Proof of Proposition 4.1. Corollary 2.8 yields $(S_p)^p = I_p$. Hence, $I_p - (S_p)^p = 0$.

Let $\mathbb{Z}^{p \times p}$ denote the $\mathbb{Z}$-algebra of all $p \times p$-matrices. Let $\mathfrak{A}$ denote the $\mathbb{Z}$-subalgebra of $\mathbb{Z}^{p \times p}$ generated by S_p. Hence, $\mathfrak{A}$ is a $\mathbb{Z}$-algebra generated by a single element (namely, by S_p). Recall that every $\mathbb{Z}$-algebra generated by a single element is commutative. Thus, the $\mathbb{Z}$-algebra $\mathfrak{A}$ is commutative (since $\mathfrak{A}$ is a $\mathbb{Z}$-algebra generated by a single element). The matrix S_p belongs to this commutative $\mathbb{Z}$-algebra $\mathfrak{A}$ (since $\mathfrak{A}$ is generated by S_p). Hence, we can substitute S_p for X on both sides of the equality

$$(1-X)^p = (1-X^p) + p(1-X)U.$$

We thus obtain

$$(I_p - S_p)^p = \underbrace{\left(I_p - (S_p)^p\right)}_{=0} + p (I_p - S_p) \underbrace{U(S_p)}_{=U_p} = p (I_p - S_p) U_p.$$

This proves Proposition 4.1 **(b)**.

[Notice that the elements of $\mathfrak{A}$ are known as the *circulant matrices* of size p.]

(a) Proposition 4.1 **(a)** follows easily from the commutativity of $\mathfrak{A}$. We leave the details to the reader, since we will not actually use Proposition 4.1 **(a)**.

(c) We shall prove Proposition 4.1 **(c)** by induction over q:

Induction base: We have $(I_p - S_p)^{0(p-1)+1} = p^0 (I_p - S_p) (U_p)^0$ (in fact, both sides of this equality equal $I_p - S_p$). In other words, Proposition 4.1 **(c)** holds for $q = 0$. This completes the induction base.

Induction step: Let $Q \in \mathbb{N}$. Assume that Proposition 4.1 **(c)** holds for $q = Q$. We must now prove that Proposition 4.1 **(c)** holds for $q = Q+1$.

We have assumed that Proposition 4.1 **(c)** holds for $q = Q$. In other words, we have

$$\left(I_p - S_p\right)^{Q(p-1)+1} = p^Q \left(I_p - S_p\right) \left(U_p\right)^Q. \tag{12}$$

Now,

$$\underbrace{(Q+1)(p-1)}_{=Q(p-1)+(p-1)} + 1 = Q(p-1) + \underbrace{(p-1)+1}_{=p} = Q(p-1) + p,$$

so that

$$\begin{aligned}
&\left(I_p - S_p\right)^{(Q+1)(p-1)+1} \\
&= \left(I_p - S_p\right)^{Q(p-1)+p} = \left(I_p - S_p\right)^{Q(p-1)} \underbrace{\left(I_p - S_p\right)^p}_{\substack{=p\left(I_p-S_p\right)U_p \\ \text{(by Proposition 4.1 \textbf{(b)})}}} \\
&= \left(I_p - S_p\right)^{Q(p-1)} p \left(I_p - S_p\right) U_p = p \underbrace{\left(I_p - S_p\right)^{Q(p-1)} \left(I_p - S_p\right)}_{\substack{=\left(I_p-S_p\right)^{Q(p-1)+1} \\ =p^Q\left(I_p-S_p\right)\left(U_p\right)^Q \\ \text{(by (12))}}} U_p \\
&= \underbrace{pp^Q}_{=p^{Q+1}} \left(I_p - S_p\right) \underbrace{\left(U_p\right)^Q U_p}_{=\left(U_p\right)^{Q+1}} = p^{Q+1} \left(I_p - S_p\right) \left(U_p\right)^{Q+1}.
\end{aligned}$$

In other words, Proposition 4.1 **(c)** holds for $q = Q+1$. This completes the induction step. Thus, Proposition 4.1 **(c)** is proven by induction. □

Corollary 4.2. Let p be a prime. Let $u \in \{1, 2, \ldots, n\}$ and $v \in \{1, 2, \ldots, n\}$. Let j, n and q be elements of $\mathbb{N}$ such that $q \leq \dfrac{n-1}{p-1}$. Then, $p^q \mid \left(\left(I_p - S_p\right)^n\right)_{u,v}$.

Proof of Corollary 4.2. Define U and U_p as in Proposition 4.1.

Since p is prime, we have $p > 1$, so that $p - 1 > 0$. Hence, we can multiply the inequality $q \leq \dfrac{n-1}{p-1}$ by $p-1$. We thus obtain $q(p-1) \leq n-1$, so that $n - 1 \geq q(p-1)$.

Let $h = n - 1 - q(p-1)$. Thus, $h \in \mathbb{N}$ (since $n - 1 \geq q(p-1)$).

Now,

$$n = \underbrace{(n - 1 - q(p-1))}_{=h} + (q(p-1) + 1) = h + (q(p-1) + 1).$$

Hence,

$$\begin{aligned}
\left(I_p - S_p\right)^n &= \left(I_p - S_p\right)^{h+(q(p-1)+1)} = \left(I_p - S_p\right)^h \underbrace{\left(I_p - S_p\right)^{q(p-1)+1}}_{\substack{=p^q\left(I_p-S_p\right)\left(U_p\right)^q \\ \text{(by Proposition 4.1 \textbf{(c)})}}} \\
&\qquad \left(\text{since } h \in \mathbb{N} \text{ and } q\left(p-1\right)+1 \in \mathbb{N}\right) \\
&= \left(I_p - S_p\right)^h p^q \left(I_p - S_p\right) \left(U_p\right)^q = p^q \underbrace{\left(I_p - S_p\right)^h \left(I_p - S_p\right)}_{=\left(I_p-S_p\right)^{h+1}} \left(U_p\right)^q \\
&= p^q \left(I_p - S_p\right)^{h+1} \left(U_p\right)^q .
\end{aligned}$$

Therefore,

$$\left(\underbrace{\left(I_p - S_p\right)^n}_{=p^q\left(I_p-S_p\right)^{h+1}\left(U_p\right)^q} \right)_{u,v} = \left(p^q \left(I_p - S_p\right)^{h+1} \left(U_p\right)^q\right)_{u,v} = p^q \left(\left(I_p - S_p\right)^{h+1} \left(U_p\right)^q\right)_{u,v}.$$

This is clearly divisible by p^q (since $\left(\left(I_p - S_p\right)^{h+1} \left(U_p\right)^q\right)_{u,v} \in \mathbb{Z}$). In other words, $\left(\left(I_p - S_p\right)^n\right)_{u,v}$ is divisible by p^q. In other words, $p^q \mid \left(\left(I_p - S_p\right)^n\right)_{u,v}$. This proves Corollary 4.2. □

We can now finally prove Theorem 1.2:

Proof of Theorem 1.2. Let s and k be the quotient and the remainder when j is divided by p. Thus, $k \in \{0,1,\ldots,p-1\}$ and $j = ps+k$. Now, $j = \underbrace{p}_{\equiv 0 \bmod p} s + k \equiv k \bmod p$. Hence, for every $m \in \mathbb{N}$, the condition $\left(m \equiv j \bmod p\right)$ is equivalent to the condition $\left(m \equiv k \bmod p\right)$. Hence, we can replace the summation sign $\sum\limits_{\substack{m\in\mathbb{N}; \\ m\equiv j \bmod p}}$ in the sum $\sum\limits_{\substack{m\in\mathbb{N}; \\ m\equiv j \bmod p}} (-1)^m \dbinom{n}{m}$ by $\sum\limits_{\substack{m\in\mathbb{N}; \\ m\equiv k \bmod p}}$. Thus,

$$\underbrace{\sum_{\substack{m\in\mathbb{N}; \\ m\equiv j \bmod p}}}_{=\sum\limits_{\substack{m\in\mathbb{N}; \\ m\equiv k \bmod p}}} (-1)^m \binom{n}{m} = \sum_{\substack{m\in\mathbb{N}; \\ m\equiv k \bmod p}} (-1)^m \binom{n}{m} = \left(\left(I_p - S_p\right)^n\right)_{1,k+1} \tag{13}$$

(by Corollary 2.9).

Notice that $k \in \{0,1,\ldots,p-1\}$, so that $k+1 \in \{1,2,\ldots,p\}$. Also, $1 \in \{1,2,\ldots,p\}$ (since $p \geq 1$).

But Corollary 4.2 (applied to $u = 1$ and $v = k+1$) yields $p^q \mid \left(\left(I_p - S_p\right)^n\right)_{1,k+1}$. In light of (13), this rewrites as $p^q \mid \sum\limits_{\substack{m \in \mathbb{N}; \\ m \equiv j \bmod p}} (-1)^m \binom{n}{m}$. In other words, $\sum\limits_{\substack{m \in \mathbb{N}; \\ m \equiv j \bmod p}} (-1)^m \binom{n}{m} \equiv 0 \bmod p^q$. This proves Theorem 1.2. □

5. Appendix 1: Proof of Proposition 3.1

We are going to prove Proposition 3.1. Let us first recall a really basic fact from number theory:

Proposition 5.1. Let a, b and c be three integers such that b is coprime to c. Assume that $c \mid ab$. Then, $c \mid a$.

Proposition 5.1 appears (for example) in [NiZuMo91, Theorem 1.10].

Next, we observe the following:

Lemma 5.2. Let p be a prime. Let $k \in \{0, 1, \ldots, p-1\}$. Then, $k!$ is coprime to p.

Proof of Lemma 5.2. We shall prove Lemma 5.2 by induction over k:

Induction base: Clearly, $0!$ is coprime to any integer (since $0! = 1$), thus in particular to p. In other words, Lemma 5.2 holds for $k = 0$. This completes the induction base.

Induction step: Let $K \in \{0, 1, \ldots, p-1\}$ be positive. Assume that Lemma 5.2 holds for $k = K-1$. We must prove that Lemma 5.2 holds for $k = K$.

We have assumed that Lemma 5.2 holds for $k = K-1$. In other words, $(K-1)!$ is coprime to p.

Set $q = \gcd(K!, p)$. Then, $q = \gcd(K!, p)$ is a positive integer (since $K!$ and p are positive integers). Also, $q = \gcd(K!, p) \mid K!$ and $q = \gcd(K!, p) \mid p$.

Assume (for the sake of contradiction) that $q \neq 1$. Then, $q > 1$ (since q is a positive integer).

The number q is a positive divisor of p (since q is positive and $q \mid p$). Therefore, q is either 1 or p (since the only positive divisors of p are 1 and p (since p is prime)). Since $q \neq 1$, we thus conclude that $q = p$. Hence, $p = q \mid K! = K \cdot (K-1)!$. Recall also that $(K-1)!$ is coprime to p. Thus, Proposition 5.1 (applied to $a = K$, $b = (K-1)!$ and $c = p$) shows that $p \mid K$. Since K and p are positive, this entails that $K \geq p$.

But $K \in \{0, 1, \ldots, p-1\}$, so that $K \leq p-1 < p$. This contradicts $K \geq p$. This contradiction proves that our assumption (that $q \neq 1$) was wrong. Hence, we cannot have $q \neq 1$. Thus, we must have $q = 1$. In view of $q = \gcd(K!, p)$, this rewrites as $\gcd(K!, p) = 1$. In other words, $K!$ is coprime to p. In other words,

Lemma 5.2 holds for $k = K$. This completes the induction step. Lemma 5.2 is thus proven by induction. □

Here is another lemma, which shows how we can (sometimes) cancel factors from congruences:

Lemma 5.3. Let b and c be integers such that c is nonzero and such that b is coprime to c. Let a and a' be integers such that $ba \equiv ba' \bmod c$. Then, $a \equiv a' \bmod c$.

Proof of Lemma 5.3. We have $ba \equiv ba' \bmod c$. In other words, $c \mid ba - ba'$. In other words, $c \mid (a - a')\, b$ (since $ba - ba' = b\,(a - a') = (a - a')\, b$). Thus, Proposition 5.1 (applied to $a - a'$ instead of a) yields $c \mid a - a'$. In other words, $a \equiv a' \bmod c$. This proves Lemma 5.3. □

First proof of Proposition 3.1. The definition of $\binom{p-1}{k}$ yields

$$\binom{p-1}{k} = \frac{(p-1)\,(p-2)\cdots(p-k)}{k!}.$$

Hence, $k!\binom{p-1}{k} = (p-1)\,(p-2)\cdots(p-k)$.

But $p - i \equiv -i \bmod p$ for every $i \in \mathbb{Z}$. Multiplying these congruences for all $i \in \{1, 2, \ldots, k\}$, we obtain

$$\begin{aligned}(p-1)\,(p-2)\cdots(p-k) &\equiv (-1)\,(-2)\cdots(-k) \\ &= (-1)^k \underbrace{(1 \cdot 2 \cdot \cdots \cdot k)}_{=k!} = (-1)^k\, k! \bmod p.\end{aligned}$$

Hence,

$$k!\binom{p-1}{k} = (p-1)\,(p-2)\cdots(p-k) \equiv (-1)^k\, k! = k!\,(-1)^k \bmod p. \tag{14}$$

But Lemma 5.2 shows that $k!$ is coprime to p. Hence, from (14), we obtain $\binom{p-1}{k} \equiv (-1)^k \bmod p$ (by Lemma 5.3, applied to $c = p$, $a = \binom{p-1}{k}$, $a' = (-1)^k$ and $b = k!$). This proves Proposition 3.1. □

We are now done proving Proposition 3.1; but let us explore the surroundings a bit more and give a (slightly) different proof of Proposition 3.1, which shows a generalization. But first, here is a simple fact about binomial coefficients:

Proposition 5.4. Let $k \in \mathbb{N}$. Then, $\binom{-1}{k} = (-1)^k$.

In this proposition, we are using the fact that binomial coefficients $\binom{n}{k}$ are defined for negative n just as well as for $n \in \mathbb{N}$. These binomial coefficients no longer count subsets (after all, they can be negative), but nevertheless are integers[3].

Proof of Proposition 5.4. The definition of $\binom{-1}{k}$ yields

$$\begin{aligned}\binom{-1}{k} &= \frac{(-1)(-2)\cdots(-k)}{k!} = \frac{1}{k!}\underbrace{(-1)(-2)\cdots(-k)}_{=(-1)^k(1\cdot 2\cdot\cdots\cdot k)} \\ &= \frac{1}{k!}(-1)^k\underbrace{(1\cdot 2\cdot\cdots\cdot k)}_{=k!} = \frac{1}{k!}(-1)^k k! = (-1)^k.\end{aligned}$$

Proposition 5.4 is proven. □

We can now generalize Proposition 3.1:

Proposition 5.5. Let p be a prime. Let u and v be two integers such that $u \equiv v \bmod p$. Let $k \in \{0,1,\ldots,p-1\}$. Then, $\binom{u}{k} \equiv \binom{v}{k} \bmod p$.

Notice the condition $k \in \{0,1,\ldots,p-1\}$. Proposition 5.5 no longer holds when $k = p$ (indeed, $p \equiv 0 \bmod p$ but $\binom{p}{p} \not\equiv \binom{0}{p} \bmod p$). When you work modulo p, you cannot blindly replace an integer by a different integer congruent to it modulo p when said integer appears inside a binomial coefficient.

Proof of Proposition 5.5. The definition of $\binom{u}{k}$ yields $\binom{u}{k} = \dfrac{u(u-1)\cdots(u-k+1)}{k!}$. Hence, $k!\binom{u}{k} = u(u-1)\cdots(u-k+1)$. The same argument (applied to v instead of u) shows that $k!\binom{v}{k} = v(v-1)\cdots(v-k+1)$.

But every $i \in \mathbb{Z}$ satisfies $u - i \equiv v - i \bmod p$ (since $u \equiv v \bmod p$). Multiplying these congruences for all $i \in \{0,1,\ldots,k-1\}$, we obtain

$$u(u-1)\cdots(u-k+1) \equiv v(v-1)\cdots(v-k+1) \bmod p.$$

Hence,

$$\begin{aligned}k!\binom{u}{k} &= u(u-1)\cdots(u-k+1) \\ &\equiv v(v-1)\cdots(v-k+1) = k!\binom{v}{k} \bmod p. \qquad (15)\end{aligned}$$

[3]See [Grinbe17, Proposition 3.20] for the proof of this fact.

But Lemma 5.2 shows that $k!$ is coprime to p. Hence, from (15), we obtain $\binom{u}{k} \equiv \binom{v}{k} \bmod p$ (by Lemma 5.3, applied to $c = p$, $a = \binom{u}{k}$, $a' = \binom{v}{k}$ and $b = k!$). Proposition 5.5 is proven. □

Second proof of Proposition 3.1. We have $p - 1 \equiv -1 \bmod p$. Hence, Proposition 5.5 (applied to $u = p - 1$ and $v = -1$) shows that

$$\binom{p-1}{k} \equiv \binom{-1}{k} = (-1)^k \bmod p \qquad \text{(by Proposition 5.4)}.$$

This proves Proposition 3.1 again. □

Let us record a simple (and really classical) fact that follows from Proposition 3.1:

Corollary 5.6. Let p be a prime. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$.

Proof of Corollary 5.6. We have $k \in \{1, 2, \ldots, p-1\} \subseteq \{0, 1, \ldots, p-1\}$. Thus, Proposition 3.1 yields $\binom{p-1}{k} \equiv (-1)^k \bmod p$.

But $k \in \{1, 2, \ldots, p-1\}$, and thus $k - 1 \in \{0, 1, \ldots, (p-1)-1\} \subseteq \{0, 1, \ldots, p-1\}$. Thus, Proposition 3.1 (applied to $k-1$ instead of k) yields $\binom{p-1}{k-1} \equiv (-1)^{k-1} \bmod p$.

But the recurrence relation of the binomial coefficients (see, e.g., [Grinbe17, Proposition 3.11]) shows that $\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}$ for every $m \in \mathbb{Q}$ and every positive integer n. Applying this to $m = p$ and $n = k$, we obtain

$$\begin{aligned}\binom{p}{k} &= \underbrace{\binom{p-1}{k-1}}_{\equiv (-1)^{k-1} \bmod p} + \underbrace{\binom{p-1}{k}}_{\equiv (-1)^k = -(-1)^{k-1} \bmod p} \\ &\equiv (-1)^{k-1} + \left(-(-1)^{k-1}\right) = 0 \bmod p.\end{aligned}$$

In other words, $p \mid \binom{p}{k}$. This proves Corollary 5.6. □

6. Appendix 2: avoiding subalgebras

Above, we have derived Corollary 4.2 from Proposition 4.1, which was proven using a little bit of abstract algebra. Let us now show how essentially the same argument could have been rewritten in fully elementary terms. We shall derive Corollary 4.2 from the following fact:

Proposition 6.1. Let p be a prime.

For every $k \in \{0, 1, \ldots, p-1\}$, we have $\dfrac{(-1)^k \binom{p-1}{k} - 1}{p} \in \mathbb{Z}$ (by Corollary 3.2).

Thus, for every $k \in \{0, 1, \ldots, p-1\}$, we can define an element $a_k \in \mathbb{Z}$ by $a_k = \dfrac{(-1)^k \binom{p-1}{k} - 1}{p}$. Consider these elements a_k.

Define a $p \times p$-matrix U_p by $U_p = \sum_{k=0}^{p-1} a_k \left(S_p\right)^k$.

(a) We have $\left(I_p - S_p\right)^p = p\left(I_p - S_p\right) U_p$.

(b) For every $q \in \mathbb{N}$, we have

$$\left(I_p - S_p\right)^{q(p-1)+1} = p^q \left(I_p - S_p\right) \left(U_p\right)^q.$$

The proof of this proposition will mostly be a mix of our above proof of Proposition 4.1 and our proof of Corollary 3.3.

Proof of Proposition 6.1. **(a)** Every $k \in \{0, 1, \ldots, p-1\}$ satisfies

$$pa_k = (-1)^k \binom{p-1}{k} - 1 \tag{16}$$

(since $a_k = \dfrac{(-1)^k \binom{p-1}{k} - 1}{p}$).

Let $\mathbb{Z}^{p \times p}$ denote the ring of all $p \times p$-matrices. The two matrices $-S_p$ and I_p in $\mathbb{Z}^{p \times p}$ commute (since $\left(-S_p\right) I_p = -S_p = I_p \left(-S_p\right)$). Thus, $-S_p$ and I_p are two commuting elements of the ring $\mathbb{Z}^{p \times p}$.

The binomial formula says the following: If a and b are any two commuting elements of a ring $\mathfrak{A}$ (that is, any two elements of a ring $\mathfrak{A}$ satisfying $ab = ba$), and if $g \in \mathbb{N}$, then

$$(a+b)^g = \sum_{k=0}^{g} \binom{g}{k} a^k b^{g-k}.$$

This formula (applied to $\mathfrak{A} = \mathbb{Z}^{p\times p}$, $a = -S_p$, $b = I_p$ and $g = p-1$) yields

$$\left(\left(-S_p\right) + I_p\right)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} \underbrace{\left(-S_p\right)^k}_{=(-1)^k \left(S_p\right)^k} \underbrace{\left(I_p\right)^{p-1-k}}_{=I_p}$$
$$= \sum_{k=0}^{p-1} \underbrace{\binom{p-1}{k} (-1)^k}_{=(-1)^k \binom{p-1}{k}} \left(S_p\right)^k = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} \left(S_p\right)^k.$$

Since $\left(-S_p\right) + I_p = I_p - S_p$, this rewrites as follows:

$$\left(I_p - S_p\right)^{p-1} = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} \left(S_p\right)^k. \tag{17}$$

On the other hand,

$$\left(I_p - S_p\right) \sum_{k=0}^{p-1} \left(S_p\right)^k = \sum_{k=0}^{p-1} \left(S_p\right)^k - \underbrace{S_p \sum_{k=0}^{p-1} \left(S_p\right)^k}_{=\sum_{k=0}^{p-1} S_p \left(S_p\right)^k} = \sum_{k=0}^{p-1} \left(S_p\right)^k - \sum_{k=0}^{p-1} \underbrace{S_p \left(S_p\right)^k}_{=\left(S_p\right)^{k+1}}$$
$$= \sum_{k=0}^{p-1} \left(S_p\right)^k - \sum_{k=0}^{p-1} \left(S_p\right)^{k+1} = \underbrace{\sum_{k=0}^{p-1} \left(S_p\right)^k}_{=\left(S_p\right)^0 + \sum_{k=1}^{p-1} \left(S_p\right)^k} - \underbrace{\sum_{k=1}^{p} \left(S_p\right)^k}_{=\sum_{k=1}^{p-1} \left(S_p\right)^k + \left(S_p\right)^p}$$

(here, we have substituted k for $k+1$ in the second sum)

$$= \left(\left(S_p\right)^0 + \sum_{k=1}^{p-1} \left(S_p\right)^k\right) - \left(\sum_{k=1}^{p-1} \left(S_p\right)^k + \left(S_p\right)^p\right)$$
$$= \underbrace{\left(S_p\right)^0}_{=I_p} - \underbrace{\left(S_p\right)^p}_{=I_p} = I_p - I_p = 0. \tag{18}$$

(by Corollary 2.8)

Now,

$$\begin{aligned}
&\left(I_p - S_p\right)^p \\
&= \underbrace{\left(I_p - S_p\right)^p}_{=\left(I_p - S_p\right)\left(I_p - S_p\right)^{p-1}} - \underbrace{0}_{=\left(I_p - S_p\right)\sum\limits_{k=0}^{p-1}\left(S_p\right)^k \text{ (by (18))}} \\
&= \left(I_p - S_p\right)\left(I_p - S_p\right)^{p-1} - \left(I_p - S_p\right)\sum_{k=0}^{p-1}\left(S_p\right)^k \\
&= \left(I_p - S_p\right)\left(\left(I_p - S_p\right)^{p-1} - \sum_{k=0}^{p-1}\left(S_p\right)^k\right).
\end{aligned}$$

Since

$$\begin{aligned}
&\underbrace{\left(I_p - S_p\right)^{p-1}}_{=\sum\limits_{k=0}^{p-1}(-1)^k\binom{p-1}{k}\left(S_p\right)^k \text{ (by (17))}} - \sum_{k=0}^{p-1}\left(S_p\right)^k \\
&= \sum_{k=0}^{p-1}(-1)^k\binom{p-1}{k}\left(S_p\right)^k - \sum_{k=0}^{p-1}\left(S_p\right)^k = \sum_{k=0}^{p-1}\underbrace{\left((-1)^k\binom{p-1}{k} - 1\right)}_{=pa_k \text{ (by (16))}}\left(S_p\right)^k \\
&= \sum_{k=0}^{p-1} pa_k\left(S_p\right)^k = p\underbrace{\sum_{k=0}^{p-1} a_k\left(S_p\right)^k}_{=U_p \text{ (since } U_p=\sum\limits_{k=0}^{p-1}a_k\left(S_p\right)^k)} = pU_p,
\end{aligned}$$

this becomes

$$\begin{aligned}
\left(I_p - S_p\right)^p &= \left(I_p - S_p\right)\underbrace{\left(\left(I_p - S_p\right)^{p-1} - \sum_{k=0}^{p-1}\left(S_p\right)^k\right)}_{=pU_p} \\
&= \left(I_p - S_p\right)pU_p = p\left(I_p - S_p\right)U_p.
\end{aligned}$$

This proves Proposition 6.1 **(a)**.

(b) Proposition 6.1 **(b)** can be derived from Proposition 6.1 **(a)** in the same way as Proposition 4.1 **(c)** was derived from Proposition 4.1 **(b)**. □

Second proof of Corollary 4.2. We can copy the above proof of Corollary 4.2 verbatim, with the only change that we use Proposition 6.1 **(b)** instead of Proposition 4.1 **(c)**. □

References

[Granvi05] Andrew Granville, *Binomial coefficients modulo prime powers*.
`http://www.dms.umontreal.ca/~andrew/PDF/BinCoeff.pdf`

[Grinbe15] Darij Grinberg, *An analogue of Hensel's lifting for Fibonacci numbers*, math.stackexchange answer #1441518, Mathematics Stack Exchange.
`http://math.stackexchange.com/q/1441518`

[Grinbe17] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`https://github.com/darijgr/detnotes/releases/tag/2019-01-10`
See also `http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf` for a version that is getting updates.

[NiZuMo91] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, Wiley 1991.

[SchWal12] Andrew Schultz, Robert Walker, *A generalization of the Gaussian formula and a q-analog of Fleck's congruence*, arXiv:1202.0199.
`http://arxiv.org/abs/1202.0199`