Coefficients of Gaussian Polynomials modulo N

Dylan Pentland*

Department of Mathematics
Massachusetts Institute of Technology
Massachusetts, U.S.A.

dylanp@mit.edu

Submitted: Apr 24, 2018; Accepted: May 29, 2020; Published: Jun 26, 2020

Abstract

Let $\begin{bmatrix} n \\ k \end{bmatrix}_q$ be a q-binomial coefficient. Stanley conjectured that the function $f_k(n) = \#\left\{\alpha : [q^\alpha] \begin{bmatrix} n \\ k \end{bmatrix}_q \equiv R \pmod N\right\}$ is quasipolynomial for N prime. We prove this for any integer N and obtain an expression for the generating function $F_k(x)$ for $f_k(n)$.

Mathematics Subject Classifications: 05A10, 05A15

1 Introduction

The q-analogue of the binomial coefficient is typically denoted $\begin{bmatrix} n \\ k \end{bmatrix}_q$ and is defined by the rational expression

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]!}{[n-k]![k]!},$$

where $[n]! = \prod_{i=1}^{n} (1-q^i)/(1-q)$. These are polynomials with degree $k(n-k)$.

These polynomials appear in combinatorics and have connections to the theory of symmetric polynomials as well as representation theory. In particular, an important characterization is that they enumerate the Grassmannian $\mathbf{Gr}(k, \mathbb{F}_q^n)$:

Theorem 1.1. *The number of k-dimensional subspaces of $\mathbb{F}_q^n$ is $\begin{bmatrix} n \\ k \end{bmatrix}_q$.*

For a proof see, for example, [6]. While q-binomial coefficients are common objects in combinatorics, recent works such as [3] or [8] have sparked additional interest in these objects and their coefficients.

In this paper, we investigate the behavior of these coefficients modulo some positive integer $N \in \mathbb{N}$. One motivation for this is the classical Lucas' theorem:

*Supported by NSF grant no. DMS-1519580.

Theorem 1.2 (Lucas' Theorem)**.** *For p prime, let $n, k \in \mathbb{N}$ have base p expansions $n = \sum_{i \geqslant 0} n_i p^i, k = \sum_{i \geqslant 0} k_i p^i$. Then*

$$\binom{n}{k} \equiv \prod_{i \geqslant 0} \binom{n_i}{k_i} \pmod{p}.$$

By fixing k, the values of $\binom{n}{k} \pmod{p}$ can be shown to form a repeating sequence related to the base p expansion of k. This extends to modulo N, as seen by the following corollary from [1]:

Theorem 1.3 (Kwong [1])**.** *Let the prime factorization of N be given by $\prod p_i^{e_i}$ for primes p_i. Then $\binom{n}{k}$ is purely periodic modulo N for fixed k, with period*

$$P = \prod p_i^{e_i + b_i - 1},$$

where $b_i \in \mathbb{N}$, $p_i^{b_i - 1} < k < p_i^{b_i}$.

Here, the term purely periodic means that a sequence $(x_n)_{n \in \mathbb{N}}$ has $x_n = x_{n+Q}$ for some Q and all $n \in \mathbb{N}$. The q-binomial coefficients are an example of a "q-analogue", in the sense that $\lim_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}$. As a result, it is reasonable to expect similar structured behavior modulo p or even with general composites in the coefficients of $\begin{bmatrix} n \\ k \end{bmatrix}_q$, since this shows $\binom{n}{k} = \lim_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{i \geqslant 0} [q^i] \begin{bmatrix} n \\ k \end{bmatrix}_q$. Here, $[q^i]f(q)$ denotes the coefficient of q^i in f.

We prove and generalize Conjecture 1.8, that the "residue counting" function for these coefficients is a *quasipolynomial*. From [6], we have the following definition of a quasipolynomial function:

Definition 1.4. A function $f : \mathbb{N} \to \mathbb{C}$ is *quasipolynomial* with degree d if

$$f(n) = c_d(n)n^d + c_{d-1}(n)n^{d-1} + \ldots + c_0(n)$$

where each $c_i(n)$ is a periodic function with integer period and $c_d(n)$ is not identically 0. We call Q a *quasiperiod* of f if it is a common period of all $c_i(n)$. Note that Q is not unique, since kQ is a quasiperiod for $k \in \mathbb{N}$.

Equivalently, we can say $f(n) = P_i(n)$ for $n \equiv i \pmod{Q}$ where $P_i \in \mathbb{Z}[x]$. In order to state the main result (Theorem 1.9), we make the following definitions.

Definition 1.5. For a natural number N that we call the *modulus*, $R \in \mathbb{Z}/N\mathbb{Z}$, and $k \in \mathbb{N}$, we define

$$f_k(n) = \#\left\{\alpha : [q^\alpha] \begin{bmatrix} n \\ k \end{bmatrix}_q \equiv R \pmod{N}\right\}.$$

This function counts the number of coefficients congruent to R modulo N.

Remark 1. From [5], we see that $p_{\leqslant k}(n)$, the number of partitions of n with at most k parts, is also an example of a quasipolynomial function.

Definition 1.6. Define $\pi_N(k)$ as the minimal period of $p_{\leqslant k}(n)$ modulo N.

Definition 1.7. Define $\pi'_N(k)$ as follows:

$$\pi'_N(k) = \pi'_N(k-1)\mathrm{lcm}\left(N, \frac{\pi_N(k)}{\pi_N(k-1)}\right).$$

We set $\pi'_N(1) = 1$.

This definition makes it so that $N \mid \frac{\pi'_N(k)}{\pi'_N(k-1)}$ for $k > 1$. Stanley originally conjectured the following in [7]:

Conjecture 1.8 (Stanley [7])**.** *The function f_k is quasipolynomial for N prime.*

The following theorem, which generalizes Conjecture 1.8, is the main result of this paper. This is shown in Sections 3 and 4.

Theorem 1.9. *For a modulus N, the function $f_k(n)$ is quasipolynomial, with a quasiperiod $\pi'_N(k)$ and degree one.*

The idea will be to formulate an equivalent restatement in Theorem 4.2, which makes a more direct statement about the structure of the coefficients modulo N. In Section 5, we investigate the structure of the generating function

$$F_k(x) = \sum_{n \geqslant k} f_k(n) x^n.$$

In section 6, we investigate some asymptotics of the proven quasiperiod and conjectured minimal quasiperiod.

2 Coefficients of low degree terms in $\begin{bmatrix} n \\ k \end{bmatrix}_q$

We first try to understand the behavior of the coefficient of q^i in $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for small i. The following result is well-known and follows from the identity $\sum_{i \geqslant 0} p(n,k,i) q^i = \begin{bmatrix} n+k \\ k \end{bmatrix}_q$, where $p(n,k,i)$ denotes the number of partitions $\lambda \vdash i$ with at most k parts and maximal part $\leqslant n$.

Lemma 1. *Let $n_0, k \in \mathbb{N}$ be arbitrary, and $n \geqslant n_0 + k$. Then for $0 \leqslant i < n_0$, we have $[q^i] \begin{bmatrix} n \\ k \end{bmatrix}_q = p_{\leqslant k}(i)$.*

Remark 2. A similar result is true for the last n_0 coefficients by the symmetry of the q-binomial coefficients.

This warrants an investigation of the function $p_{\leqslant k}(i)$ modulo N. The following theorem from [4] shows that it is purely periodic, and determines the minimal period for primes. Then in [2], this is extended to prime powers. By the Chinese Remainder Theorem, understanding the behavior of $p_{\leqslant k}(i)$ modulo prime powers is sufficient to understand its behavior modulo N.

Theorem 2.1 (Kwong)**.** *For a prime power p^e, fix a set $S = \{s_0, s_1, \dots s_l\}$ with entries in $\mathbb{N}$. Let $p(n;S)$ be given by the generating function*

$$P(x;S) := \prod_{s\in S} \frac{1}{1-x^s} = \sum_{n\geqslant 0} p(n;S)x^n,$$

hence $p(n;S)$ is the number of partitions λ with parts in S and $|\lambda| = n$. Then $p(*;S)$ is purely periodic modulo p^e, with minimal period

$$\pi_{p^e}(S) = p^{b_p(S)+e-1}L_p(S)$$

where $b_p(S)$ is the smallest integer such that

$$p^{b_p(S)} \geqslant \sum_{s\in S} p^{\nu_p(s)}$$

where $\nu_p(s)$ is the p-adic valuation of s and $L_p(S) := \mathrm{lcm}(S)/p^{\nu_p(\mathrm{lcm}(S))}$ is the p-free part of $\mathrm{lcm}(S)$.

For a more detailed discussion, see [2]. Lemma 1 then shows that for n_0 sufficiently large, the first n_0 coefficients of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for $n-k \geqslant n_0$ will follow a repeating pattern of period $\pi_{p^e}(k) = p^{b_p([k])+e-1}L_p([k])$ modulo p^e. Here, $[k] := \{1, 2, \dots k\}$.

It is worth noting that the statement is slightly incorrect: the theorem does not hold in the trivial case $k = 1$ where $\pi_N(k) = 1$. However, there seem to be no other errors otherwise with the proof. Fortunately, this case is simple and can be ignored. From now on, we have $k \geqslant 2$.

Definition 2.2. Fix k, a modulus $N \in \mathbb{N}$, and $n > \pi_N(k)$. Let $\mathcal{S}$ be the sequence of the first $\pi_N(k)$ coefficients of $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ reduced mod N. It is given by $\mathcal{S} = (s_0, s_1, \dots s_{\pi_N - 1})$, where $s_\alpha \equiv [q^\alpha] \begin{bmatrix} n+k \\ k \end{bmatrix}_q \pmod N$.

Theorem 2.1 and Lemma 1 show that $\mathcal{S}$ determines the periodic sequence $p_{\leqslant k}(i)$ modulo N.

Example 1. One example of this sequence for $N = 2$ and $k = 3$ is shown in Figure 1.

s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}
1	1	0	1	0	1	1	0	0	0	0	0

Figure 1: Values of $\mathcal{S}$ modulo 2.

Next, we study $\mathcal{S}$ for prime powers p^e as the modulus. The generating function of $p_{\leqslant k}(n)$ is given by

$$P_{\leqslant k}(q) := \sum_{n\geqslant 0} p_{\leqslant k}(n)q^n = \frac{1}{\prod_{i\in[k]} 1-q^i}.$$

Lemma 2. $\operatorname{lcm}([k]) \mid \pi_{p^e}(k)$.

Proof. By Theorem 2.2, it suffices to show that $b_p([k]) \geqslant \nu_p(\operatorname{lcm}([k]))$. We can then see

$$p^{b_p([k])} \geqslant \sum_{i\in[k]} p^{\nu_p(i)} \geqslant p^{\max_{i\in[k]}\nu_p(i)} = p^{\nu_p(\operatorname{lcm}([k]))}.$$

Taking logs, the result follows. □

Definition 2.3. Define the operator $\Delta_Q : \mathbb{Z}[[q]] \to \mathbb{Z}[[q]]$ for $Q \in \mathbb{N}$ via the formula

$$\begin{aligned}(\Delta_Q F)(q) &= F(q) - q^Q F(q)\\ &= \sum_{n\geqslant 0} f(n)q^n - \sum_{n\geqslant Q} f(n-Q)q^n,\end{aligned}$$

This can be viewed as an analogue of the finite difference operator (Δ, as in [6] §1.9) acting on formal power series.

Example 2. Consider the generating function $F(q) = \frac{q}{(1-q)^2} = \sum_{i\geqslant 0} iq^i$. Suppose we want to calculate $\Delta_5 F(q)$: then we have

$$\begin{aligned}\Delta_5 F(q) &= \frac{q}{(1-q)^2} - \frac{q^6}{(1-q)^2}\\ &= \frac{5q^5}{1-q} + (4q^4 + 3q^3 + 2q^2 + 1q).\end{aligned}$$

This demonstrates a key aspect of the Δ_Q operator: the lowest Q monomials remain unchanged, while the rest of the sequence can be viewed as a union of Q subsequences with the traditional finite difference operator applied.

Theorem 2.4. *Fix n, k. Consider the sequence $\mathcal{S}$ where we take coefficients modulo $N = p^e$. Then $s_{|\mathcal{S}|-1}, \ldots s_{|\mathcal{S}|-\binom{k+1}{2}+1}$ are all 0 modulo N, and $s_i = (-1)^{k+1} s_{\pi_N(k)-\binom{k+1}{2}-i}$ for $\pi_N(k) - \binom{k+1}{2} - i \geqslant 0$ and $i \geqslant 0$.*

Proof. The main idea behind this result is to exploit the simple form of the generating function $P_{\leqslant k}(q)$. We can re-write it as follows, letting $Q := \pi_{p^e}(k)$:

$$P_{\leqslant k}(q) = \frac{1}{\prod_{i\in[k]} 1-q^i} = \frac{\gamma(q)}{(1-q^Q)^k}, \tag{1}$$

where we can obtain

$$\gamma(q) = \frac{(1-q^Q)^k}{\prod_{i\in[k]} 1-q^i} = \prod_{d\mid Q} \Phi_d(q)^{f(d)} \tag{2}$$

where $f(d) = k - \#\{i \in [k] : d \mid i\} \geqslant 0$ and Φ_d denotes the dth cyclotomic polynomial. To show (2), note that $f(d)$ accounts for every factor in the denominator, and is bounded below by 0. This follows from Lemma 2 and the fact that each cyclotomic factor of the denominator can appear at most k times (at most once for each factor $(1-q^i)$). Thus we conclude that $\gamma(q) \in \mathbb{Z}[q]$ and that $\deg \gamma(q) = kQ - \binom{k+1}{2}$. Using Δ_Q as in Definition 2.3, we obtain

$$\Delta_Q^k P_{\leqslant k}(q) = \gamma(q).$$

Using the fact that $P_{\leqslant k}(q)$ can be written as $P_{\leqslant k}(q) \equiv \frac{\gamma_0(q)}{1-q^Q} \pmod{p^e}$ for some unique $\gamma_0(q)$ with $\deg \gamma_0 < Q$ by Theorem 2.1, we can see that $\Delta_Q P_{\leqslant k}(q) \equiv \gamma_0(q) \pmod{p^e}$. It follows from this that

$$\Delta_Q^k P_{\leqslant k}(q) \equiv \sum_{i \geqslant 0} (-1)^i \binom{k-1}{i} \gamma_0(q) q^{Qi} \pmod{p^e},$$

using the formula for $\Delta^k f(n)$ from [6] in §1.9. This is straightforward to verify using induction. Thus, for $r \in \mathbb{Z}/Q\mathbb{Z}$ we have

$$[q^{r+Q(k-1)}]\gamma(q) \equiv (-1)^{k-1}[q^r]\gamma(q) \pmod{p^e}.$$

Knowing that $\deg \gamma = kQ - \binom{k+1}{2}$, there must be $\binom{k+1}{2} - 1$ zeroes at the end of $\mathcal{S}$. Furthermore, the polynomial $\gamma(q)$ can be shown to be symmetric using (2) and the symmetry of the cyclotomic polynomials (this is only true for Φ_d when $d > 1$, but $d = 1$ is not an issue as $f(1) = 0$). Referring to Figure 2, this shows the symmetry of $\mathcal{S}$ when the trailing zeroes are ignored: by the symmetry of $\gamma(q)$, the elements with label i in Figure 2 are equal. These are also identical instances of $\mathcal{S}$ without the trailing zeroes up to sign, so $\left\{s_0, \dots s_{|\mathcal{S}|-\binom{k+1}{2}}\right\}$ is symmetric or "anti-symmetric" about its center. Precisely, this says that $s_i = (-1)^{k+1} s_{\pi_N(k)-\binom{k+1}{2}-i}$. □

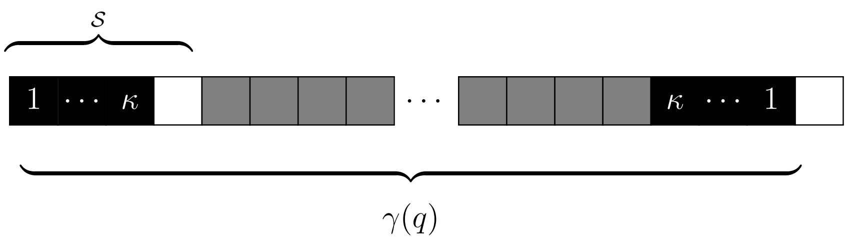

Figure 2: Symmetry in $\mathcal{S}$. White boxes represent sections of zeroes modulo p^e, gray sections represent the other values of coefficients of $\gamma(q)$ modulo p^e. The coefficients are ordered from left to right by increasing associated powers of q. We define $\kappa = Q - \binom{k+1}{2}$, so that the white numbers $1, 2, \dots, \kappa$ enumerate coefficients in the black sections.

These ideas can be generalized using the Chinese Remainder Theorem.

Lemma 3. *Partitions with at most k parts are purely periodic modulo N for all $N \in \mathbb{N}$, with period*

$$\pi_N(k) = \operatorname*{lcm}_{p|N}\big(\pi_{p^{\nu_p(N)}}(k)\big).$$

Corollary 2.5. *Theorem 2.4 also holds for $\mathcal{S}$ for arbitrary moduli N.*

Theorem 2.6. *Let $k \geqslant 0$ and N be odd. If k is odd and $\gcd\left(\frac{\pi_N(k+1)}{\pi_N(k)}, N\right) > 1$, then we have*

$$\frac{\pi_N(k+1)}{\pi_N(k)} \sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}.$$

Otherwise we have the stronger result $\sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}$.

Proof. First, we prove this for when k is even. We have two cases. First, suppose $\frac{\pi_N(k)-\binom{k+1}{2}+1}{2} \notin \mathbb{Z}$. This means there exists a "central" element that is self-inverse ($x = -x$ mod N) in $\mathcal{S}$ by Corollary 2.5. Since N is odd it is 0 mod N. Using Corollary 2.5 we pair all other terms in $\sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i)$ in zero-sum pairs.

Otherwise, $\frac{\pi_N(k)-\binom{k+1}{2}+1}{2} \in \mathbb{Z}$. There is no central entry, and pairing via Corollary 2.5 suffices to show $\sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}$.

For k odd, we use a different method since $(-1)^{k+1} = 1$. We have

$$\begin{aligned}
\sum_{i \in \mathbb{Z}/\pi_N(k+1)\mathbb{Z}} p_{\leqslant k+1}(i) - p_{\leqslant k}(i) &\equiv \sum_{i \in \mathbb{Z}/\pi_N(k+1)\mathbb{Z}} p_{=(k+1)}(i) \pmod{N} \\
&\equiv \sum_{i \in \mathbb{Z}/\pi_N(k+1)\mathbb{Z}} p_{\leqslant k+1}(i-(k+1)) \pmod{N} \\
&\equiv 0 \pmod{N}. \quad \text{(by even case, shift invariance)}
\end{aligned}$$

Thus, we obtain

$$\frac{\pi_N(k+1)}{\pi_N(k)} \sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}$$

Unless $\gcd\left(\frac{\pi_N(k+1)}{\pi_N(k)}, N\right) > 1$, the stronger statement $\sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}$ holds since $\frac{\pi_N(k+1)}{\pi_N(k)}$ would be invertible modulo N. ☐

Corollary 2.7. *Suppose $\sum_{i \in \mathbb{Z}/\pi_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}$ for odd N. Then the same holds for modulo $2N$ and π_{2N} given $\frac{\pi_2(k)-\binom{k+1}{2}+1}{2} \in \mathbb{Z}$.*

Proof. Because $\pi_N(k) \mid \pi_{2N}(k)$, we get that $\sum_{i \in \mathbb{Z}/\pi_{2N}(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{N}$. Next, consider the sum modulo 2. We have $\sum_{i \in \mathbb{Z}/\pi_2(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{2}$, since modulo 2 the symmetry relation in Theorem 2.4 becomes $s_i \equiv -s_{\pi_2(k)-\binom{k+1}{2}-i}$ because $1 \equiv -1$ modulo 2 - hence, the reasoning in Theorem 2.6 even k applies to all k. Since $\pi_2(k) \mid \pi_{2N}(k)$, we see that

$$\sum_{i \in \mathbb{Z}/\pi_{2N}(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod{2}.$$

Using the Chinese Remainder Theorem, this is 0 modulo $2N$. ☐

3 Decomposition of $\begin{bmatrix} n \\ k \end{bmatrix}_q$

In this section and the next, we exploit the results from Section 2 regarding the periodicity of $\mathcal{S}$ and the structure of $\mathcal{S}$ (as described by Theorem 2.4) in order to prove Theorem 1.7.

Definition 3.1. For a modulus N, we define the function $\mathcal{L}_k^{(i)}$ by

$$f_k(n) = \mathcal{L}_k^{(i)}\left(\frac{n-i}{\pi'_N(k)}\right),$$

if $n \equiv i \pmod{\pi'_N(k)}$.

Remark 3. The change of variables $n \mapsto \frac{n-i}{\pi'_N(k)}$ is used to simplify proofs.

The aim is now to show that the functions $\mathcal{L}_k^{(i)}$ are linear, from which it follows by definition that f_k is quasipolynomial. To do this, we will use the following general strategy:

- Partition the coefficients of $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ into different classes with periodic behavior.
- Using the periodicity of the first $\pi_N(k)$ coefficients (by Lemma 3), inductively show that these sections are also periodic using a partition decomposition (Lemma 4).
- Use this last fact to show that $n \mapsto n + \pi'_N(k)$ changes $f_k(n+r)$ a constant amount depending only on r.
- Conclude f_k is quasipolynomial, since the previous point shows $\mathcal{L}_k^{(i)}$ are linear.

We begin with the division of coefficients in $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ into different sections.

Definition 3.2. The ith *section* of the q-binomial coefficient $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ is the sequence of coefficients denoted by S_i with jth term given by

$$p_{\leqslant k}^{(i)}(j) = [q^{in+j}]\begin{bmatrix} n+k \\ k \end{bmatrix}_q,$$

where $j \in \mathbb{Z}/n\mathbb{Z}$. As a special case, S_0 is just a concatenation of copies of $\mathcal{S}$.

Recall the identity

$$\sum_{i \geqslant 0} p(n,k,i)q^i = \begin{bmatrix} n+k \\ k \end{bmatrix}_q,$$

where $p(n,k,i)$ denotes the number of partitions $\lambda \vdash i$, with at most k parts and maximal part $\leqslant n$.

This definition allows us to loosely determine a section by saying terms in the sequence contain the number of partitions which fit in a $n \times k$ box of size $|\lambda| = l$ for l such that there exists a partition $\lambda \vdash l$ covering i complete rows but no partition covering $i+1$ rows.

Definition 3.3. Let $X = (x_0, \ldots, x_{|X|-1})$ and $Y = (y_0, \ldots, y_{|Y|-1})$ be finite sequences. The concatenation operator $\oplus$ is defined as $X \oplus Y = (x_0, x_1, \ldots x_{|X|-1}, y_0, y_1, \ldots y_{|Y|-1})$.

We then make the following decomposition of S_i that proves useful:

$$\mathsf{S}_i = \mathsf{B}_i^1 \oplus \mathsf{B}_i^2 \oplus \ldots \oplus \mathsf{B}_i^l \oplus \mathsf{R}_i,$$

where the B_i^j are $\pi'_N(k)$-length subsequences and R_i is the remainder after these $l = \lfloor \frac{n}{\pi'_N(k)} \rfloor$ consecutive subsequences are removed from S_i. Informally, if we regard $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ as a sequence ordered by the associated exponents of q, we can relate $X = \bigoplus_{i \in [k]} \mathsf{S}_{i-1} \oplus (1)$ to its corresponding q-binomial coefficient. Here, (1) is just a sequence only containing 1. We can index X starting at 0, obtaining

$$\begin{bmatrix} n+k \\ k \end{bmatrix}_q = \sum_{x_i \in X} x_i q^i.$$

The net result of this decomposition is illustrated in Figure 3.

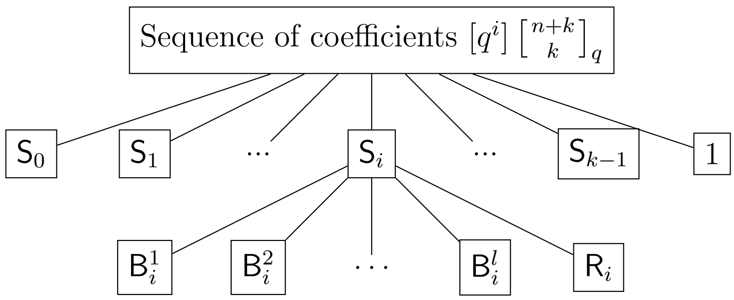

Figure 3: Decomposition of a q-binomial coefficient into sections modulo N. Here, edge connections denote concatenation (as per Definition 3.3) from left to right and $l := \lfloor \frac{n}{\pi'_N(k)} \rfloor$.

4 Proving f_k is quasipolynomial

Using the definitions from Section 3, we investigate the structure of each individual section.

Definition 4.1. Fix a q-binomial coefficient $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$. Let $\mathcal{P}_{i,m}^{\text{bad}}(j)$ be the set containing all pairs of partitions (λ, μ) such that

- $|\lambda| + |\mu| = mn + j$.
- λ has at most k parts each at most n, of which i are equal to n.
- μ has exactly i parts.

Lemma 4. *Fix n, m, k. For $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ we have the following identity for the associated functions $p^{(m)}_{\leqslant k}$:*

$$p^{(m)}_{\leqslant k}(j) = p_{\leqslant k}(mn + j) - \sum_{i \in [m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j).$$

Proof. Let S be the set of partitions counted by $p^{(m)}_{\leqslant k}(j)$ and S' be defined similarly for $p_{\leqslant k}(mn+j)$. It is clear that $S \subseteq S'$, so we wish to show that $\sum_{i\in[m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j)$ enumerates all of the additional partitions that "leave the $n \times k$ box" or have some part greater than n. Consider Figure 4 below.

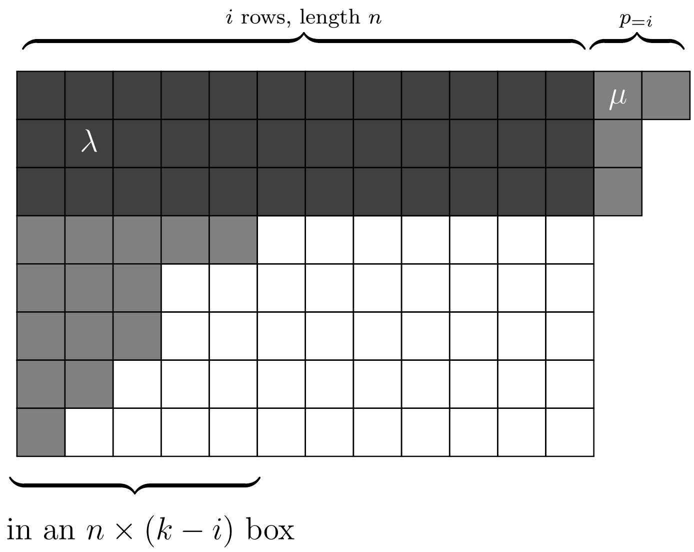

Figure 4: Classification of partitions in $\mathcal{P}^{\text{bad}}_{i,m}(j)$

Figure 4 depicts a pair $(\lambda, \mu) \in \mathcal{P}^{\text{bad}}_{i,m}(j)$. Here, λ is represented by the shaded boxes inside the $n \times k$ box. The darker boxes depict the i parts of λ that are exactly n, while the lighter gray boxes below depict the part of λ that can vary. Outside of the $n \times k$ boxes is μ, with precisely i parts. As labelled in the diagram, it is easy to see that λ are enumerated by $p^{(m-i)}_{\leqslant k-i}$ and μ are enumerated by $p_{=i}$. Construct a partition $\Pi = \lambda + \mu$ via part-wise addition. This is counted in S' by $p_{\leqslant k}$ but not in S since it *must* leave the $n \times k$ box. Thus, sending $(\lambda, \mu) \in \bigcup_{i\in[m]} \mathcal{P}^{\text{bad}}_{i,m}(j)$ to $\Pi = \lambda + \mu$ is a map ϕ from $\bigcup_{i\in[m]} \mathcal{P}^{\text{bad}}_{i,m}(j)$ to $S' \setminus S$. We claim ϕ is a bijection. It is not too difficult to see that ϕ is an injection: if $\lambda + \mu = \lambda' + \mu'$ then μ and μ' have the same number of parts and from this it is evident $\mu = \mu', \lambda = \lambda'$.

Now we show ϕ is a surjection. Take a "bad" partition $\Pi = \{\pi_1, \ldots, \pi_k\}$ with $|\Pi| = mn + j$ leaving the box. Such a partition must leave the box for the first i rows for some $i \in [m]$ (we cannot have $i > m$, since $|\Pi| = mn + j \leqslant (m + 1)n$). Setting $\mu = \{\pi_\alpha - n : \pi_\alpha > n\}$ and $\lambda = \{\pi_\alpha : \pi_\alpha \leqslant n\} \cup \{n : \pi_\alpha > n\}$, we construct a pair (λ, μ). Both λ, μ satisfy the last two conditions of Definition 4.1 due to the construction. The first condition $|\lambda| + |\mu| = mn + j$ is also satisfied, as

$$|\lambda| + |\mu| = \sum_{\pi_\alpha > n} (\pi_\alpha - n) + n + \sum_{\pi_\alpha \leqslant n} \pi_\alpha = |\Pi| = mn + j.$$

Thus $(\lambda, \mu) \in \mathcal{P}^{\text{bad}}_{i,m}(j)$, and $\lambda + \mu = \Pi$.

Thus, we have a bijection ϕ from $\bigcup_{i \in [m]} \mathcal{P}^{\text{bad}}_{i,m}(j)$ to $S' \setminus S$, and it follows that

$$\sum_{i \in [m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j) = |S' \setminus S|. \qquad \square$$

The following is a restatement of Theorem 1.9 and is the main result.

Theorem 4.2. *Let $N \in \mathbb{N}$ be the modulus of f_k. Then f_k is quasipolynomial, with quasiperiod $\pi'_N(k)$. Additionally, all $\mathcal{L}^{(i)}_k$ are linear functions.*

Proof. Let $Q := \pi'_N(k)$. To prove the claim, the central idea of the argument is to show that in the section S_i of $\begin{bmatrix} Ql+r+k \\ k \end{bmatrix}_q$ we have $\mathsf{B}^1_i \equiv \mathsf{B}^2_i \equiv \ldots \equiv \mathsf{B}^l_i \pmod N$. From this fact, we make a simple argument that shows the claim. We use the q-binomial coefficient $\begin{bmatrix} n+k \\ k \end{bmatrix}_q = \begin{bmatrix} Ql+k+r \\ k \end{bmatrix}_q$ so that we can read off that B_i have length Q, R_i has length r, and that l is the number of B_i in the decomposition of S_i.

To prove that $\mathsf{B}^1_i \equiv \mathsf{B}^2_i \equiv \ldots \equiv \mathsf{B}^l_i \pmod N$, we induct on the indices $m = 1, 2, \ldots, k-1$ of the sections, holding k fixed, and then induct on k.

In §2, we already showed that S_0 has the aforementioned property for all k by considering partitions with at most k parts. One can also show that $\mathsf{B}^1_i = \mathsf{B}^2_i = \ldots = \mathsf{B}^l_i$ holds when $k = 2$ by explicit computation of $p_{\leqslant 2}(j) = \lfloor \frac{j}{2} \rfloor + 1$. This establishes the base cases $m = *, k = 2$ and $m = 0, k = *$.

We show the claim holds for S_m assuming it holds for S_i $(i < m)$ and all smaller k. Using Lemma 4, we have for $j \in \mathbb{Z}/(Ql + r)\mathbb{Z}$,

$$\begin{aligned} p^{(m)}_{\leqslant k}(j) &\equiv p_{\leqslant k}(j + mr) - \sum_{i \in [m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j) \\ &\equiv p_{\leqslant k}(j + mr) - \sum_{i \in [m]} \sum_{\ell + \ell' = C_{i,m}(j)} [q^\ell] \begin{bmatrix} n + (k-i) \\ k - i \end{bmatrix}_q p_{=i}(\ell') \pmod N \qquad (3) \end{aligned}$$

where $C_{i,m}(j) = |\lambda| + |\mu| - ni$ for $(\lambda, \mu) \in \mathcal{P}^{\text{bad}}_{i,m}(j)$ (or more explicitly $C_{i,m}(j) = (m - i)(Ql + r) + j$) and $\ell, \ell' \geqslant 0$. The functions $p_{=i}$ and $[q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q$ count μ and λ in $\mathcal{P}^{\text{bad}}_{i,m}$ respectively in (3). Note that

$$p_{=i}(\ell) = p_{\leqslant i}(\ell - i),$$

an explicit bijection being given by taking $\tau \vdash n$ counted by $p_{=i}$ and decreasing each part by one. Thus, we see $p_{=i}$ has period Q as $\pi_N(i) | \pi_N(k) | Q$. We claim that the map $j \mapsto j + Q$ leaves $p^{(m)}_{\leqslant k}(j)$ unchanged modulo N, or that $p^{(m)}_{\leqslant k}(j + Q) - p^{(m)}_{\leqslant k}(j) \equiv 0 \pmod N$. Note here that $j + Q < n$, otherwise this statement does not make sense (so for example, $l \geqslant 1$

so we have a complete block B_i). Since $p_{\leqslant k}$ has period $\pi_N(k) \mid \pi'_N(k)$, the function $p_{\leqslant k}$ will vanish in the difference. So it suffices to show that $\Delta := \#\mathcal{P}^{\text{bad}}_{i,m}(j+Q) - \#\mathcal{P}^{\text{bad}}_{i,m}(j) \equiv 0 \pmod N$.

$$\begin{aligned}\Delta &\equiv \sum_{\ell+\ell'=C_{i,m}(j+Q)} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') - \sum_{\ell+\ell'=C_{i,m}(j)} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \\ &\equiv \sum_{\substack{\ell+\ell'\equiv j \\ (\operatorname{mod} Q)}} p^{(m-i)}_{\leqslant k-i}(\ell) p_{=i}(\ell'). \pmod N \end{aligned} \tag{4}$$

The final congruence requires some elaboration. Here, we observe that ℓ determines ℓ' entirely, and that $C_{i,m}(j+Q) - C_{i,m}(j) = Q$. Since $p_{=i}(\ell')$ has period Q modulo N, we can add Q to ℓ' to eliminate all terms except for $C_{i,m}(j) < \ell \leqslant C_{i,m}(j+Q)$. The exact bounds for ℓ are unimportant, since $p_{=i}(0) = 0$ and hence we can ignore terms where $\ell' \equiv 0 \pmod Q$ in the sum - thus, equivalently we have $C_{i,m}(j) \leqslant \ell \leqslant C_{i,m}(j+Q)$ or $C_{i,m}(j) \leqslant \ell < C_{i,m}(j+Q)$. Hence, this corresponds to $p^{(m-i)}_{\leqslant k-i}(\overline{\ell}) := [q^{(m-i)n+\overline{\ell}}] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q$ for $\overline{\ell} \in \mathbb{Z}/Q\mathbb{Z}$. Note that since $l \geqslant 1$, this stays within bounds for ℓ for $p^{(m-i)}_{\leqslant k-i}(\ell)$.

In the final sum in (4), $\ell, \ell' \in \mathbb{Z}/Q\mathbb{Z}$. It follows immediately from the definition of $\pi'_N(k)$ that $\pi'_N(k)/\pi'_N(k-1) \in N\mathbb{Z}$. But note that $p^{(m-i)}_{\leqslant k-i}$ and $p_{=i}$ have periods dividing $\pi'_N(k-1)$ as it is always true that $1 \leqslant i \leqslant k-1$ for each sum, and hence residues modulo N are repeated some multiple of N times in the sum. Thus $p^{(m)}_{\leqslant k}(j)$ is Q-periodic since the sum is 0 modulo N, and by strong induction the same is true for each S_m. This completes the induction.

Then $l \mapsto l+1$ simply adds on another identical period in each S_m. Hence, we may write

$$\mathsf{S}_i = \mathsf{B}_i \oplus \mathsf{B}_i \oplus \ldots \oplus \mathsf{B}_i \oplus \mathsf{R}_i,$$

where the B_i are identical modulo N. For short, denote this $\mathsf{S}_i = \mathsf{B}_i^{\oplus l} \oplus \mathsf{R}_i$. More importantly, this indicates that $f_k(Q(l+1)+r) - f_k(Ql+r)$ is a constant depending on r. Thus, we can write

$$f_k(n) = \mathcal{L}^{(i)}_k \left(\frac{n-i}{Q} \right),$$

which is precisely what we wanted. □

The decomposition used in the Theorem 4.2 also allows us to prove the following observation about a special case of $p^{(m)}_{\leqslant k}$:

Corollary 4.3. *The last* $\binom{k+1-m}{2} - 1$ *entries of each component* B^i_m *of* S_m *are* 0 *modulo* N *for* $\begin{bmatrix} \pi'_N(k)l+k \\ k \end{bmatrix}_q$.

Proof. This is given for $m = 0$ by Corollary 2.5, so let $m > 0$. Similarly, $k = 2$ is trivial. We proceed by strong induction on k, m. By Lemma 4, for $j \in \mathbb{Z}/\pi'_N(k)l\mathbb{Z}$ we have

$$p^{(m)}_{\leqslant k}(j) \equiv p_{\leqslant k}(j) - \sum_{i\in[m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j) \pmod N.$$

Noting that $\binom{a}{2} < \binom{b}{2}$ when $a < b$ we see for $j \in [\pi'_N(k) - \binom{k+1-m}{2}, \pi'_N(k) - 1]$ that $p_{\leqslant k}(j) \equiv 0 \pmod N$ by Corollary 2.5. Therefore, for such j we have the simplified form $p^{(m)}_{\leqslant k}(j) \equiv -\sum_{i\in[m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j) \pmod N$. We wish to show $\sum_{i\in[m]} \#\mathcal{P}^{\text{bad}}_{i,m}(j) \equiv 0 \pmod N$ for such j. To do this, we use the expansion of $\#\mathcal{P}^{\text{bad}}_{i,m}(j)$ from the main theorem and exploit that $\#\mathcal{P}^{\text{bad}}_{i,m}(j + \pi'_N(k)) \equiv \#\mathcal{P}^{\text{bad}}_{i,m}(j) \pmod N$ to obtain

$$\begin{aligned}\#\mathcal{P}^{\text{bad}}_{i,m}(j) &\equiv \sum_{\ell+\ell'=j} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \pmod N \\ &\equiv \sum_{\substack{\ell+\ell'\equiv j \\ (\text{mod } \pi'_N(k))}} p^{(0)}_{\leqslant k-i}(\ell) p_{=i}(\ell') \pmod N\end{aligned}$$

The final congruence is because the last $\binom{(k-i)+1}{2} - 1 \geqslant \binom{k+1-m}{2} - 1$ entries of $[q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q$ are 0 by Corollary 2.5 and Lemma 1 as $\ell < \pi'_N(k)$. All added terms in the summation will have ℓ, ℓ' lie in the interval $[j, \pi'_N(k) - 1]$ and our specifically chosen j makes it so that each new term added must then be 0 mod N. The final sum is 0 modulo N for the same reasons as in the main theorem, since $k - 1 \geqslant i \geqslant 1$ and hence as a function of ℓ the function $p^{(0)}_{\leqslant k-i}(\ell) p_{=i}(\ell')$ has a period P so $\pi'_N(k)/P \in N\mathbb{Z}$ by definition of $\pi'_N(k)$. □

Remark 4. Using the symmetry of the q-binomial coefficients, we can show that a similar claim holds for the first entries of B^i_m. Explicitly, the first $\binom{k+1-((k-1)-m)}{2} - 1 = \binom{m+2}{2} - 1$ entries are 0 modulo N.

5 The generating function of f_k

The result from the previous section allows for the generating function for f_k to be explicitly calculated.

Theorem 5.1. *For a modulus $N \in \mathbb{N}$, we have*

$$F_k(x) := \sum_{n\geqslant 0} f_k(n)x^n = \frac{1}{(1-x^Q)^2} \sum_{i\in\mathbb{Z}/Q\mathbb{Z}} (1-x^Q)b_i x^i + m_i x^{Q+i},$$

where $\mathcal{L}^{(i)}_k$ has constant term b_i and slope m_i and $Q = \pi'_N(k)$.

Proof. For simplicity, let $\mathcal{L}_i = \mathcal{L}^{(i)}_k$, and $Q = \pi'_N(k)$ as above. Then we let $F_{\mathcal{L}_i}(x) = \sum_{j\geqslant 0} \mathcal{L}_i(j)x^{jQ+i}$, so that

$$F_k(x) = \sum_{i\in\mathbb{Z}/Q\mathbb{Z}} F_{\mathcal{L}_i}(x).$$

Fortunately, each term is simple to find. We have

$$\begin{aligned}\sum_{i\in\mathbb{Z}/Q\mathbb{Z}} F_{\mathcal{L}_i}(x) &= \sum_{i\in\mathbb{Z}/Q\mathbb{Z}} x^i \left(\sum_{j\geqslant 0} b_i x^{jQ} + \sum_{j\geqslant 0} m_i j x^{jQ}\right) \\ &= \sum_{i\in\mathbb{Z}/Q\mathbb{Z}} x^i \left(\frac{b_i}{1-x^Q} + \frac{m_i x^Q}{(1-x^Q)^2}\right) \\ &= \frac{1}{(1-x^Q)^2} \sum_{i\in\mathbb{Z}/Q\mathbb{Z}} (1-x^Q) b_i x^i + m_i x^{Q+i}\end{aligned}$$

which proves the theorem. □

Letting $Q' = \pi'_N(k-1)$, it turns out that one can often rewrite this as

$$F_k(x) = \frac{1}{(1-x^Q)^2}\left(\sum_{i\in\mathbb{Z}/Q\mathbb{Z}} (1-x^Q) b_i x^i + \sum_{i\in\mathbb{Z}/Q'\mathbb{Z}} m_i x^{Q+i} \frac{x^Q-1}{x^{Q'}-1}\right).$$

This stems from the fact that the slopes of the functions $\mathcal{L}_k^{(i)}$ often have a smaller period (in i, where k, R are fixed) than the actual quasiperiod itself, namely Q'. This is formalized by Theorem 5.3, and an example is given in Figure 5.

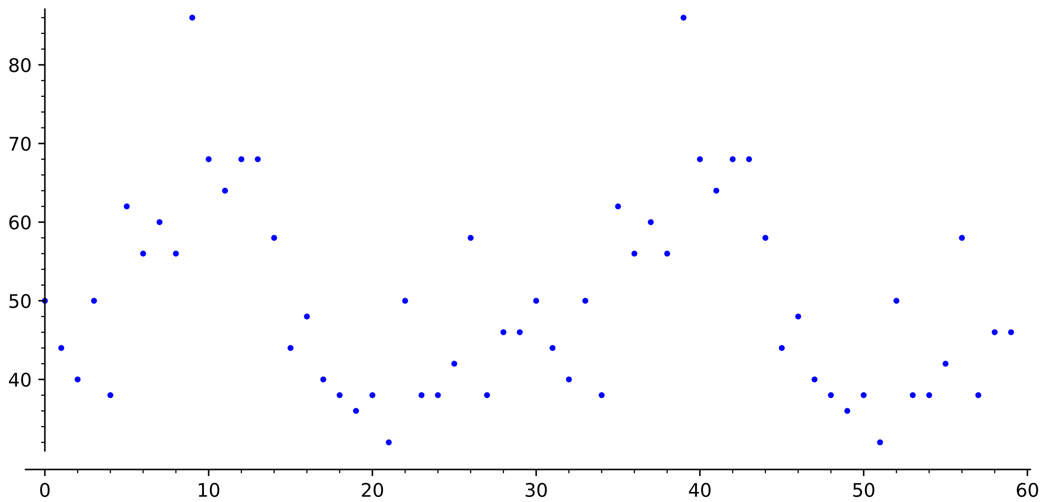

Figure 5: **An illustration of Theorem 5.3.** This figure shows the slopes of the functions $\mathcal{L}_4^{(i)}$ when $N = 5, R = 1$. The horizontal axis is i, while the vertical axis is the slope. Notice that the slopes have a period that is half of the actual minimal quasiperiod (in this case, given by the function π_5) and $\pi_5(4)/\pi_5(3) = 60/30 = 2$, as claimed.

Theorem 5.2. *Let $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ be a q-binomial coefficient where $n > \pi'_N(k)$ so that we have an entire block B_i in each section. Fix a pair (k, N) such that $\sum_{i\in\mathbb{Z}/\pi'_N(k)\mathbb{Z}} p_{\leqslant k}(i) \equiv 0 \pmod N$ by Theorem 2.6. Then $\sum_{i\in\mathbb{Z}/\pi'_N(k)\mathbb{Z}} p^{(m)}_{\leqslant k}(i) \equiv 0 \pmod N$.*

Proof. We use Lemma 4. This yields, following the same expansion as in Theorem 4.2,

$$p^{(m)}_{\leqslant k}(j) \equiv p_{\leqslant k}(j+mn) - \sum_{i\in[m]} \left(\sum_{\ell+\ell'=C_{i,m}(j)} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \right) \pmod N.$$

Summing over $j \in \mathbb{Z}/\pi'_N(k)\mathbb{Z}$, by assumption the $p_{\leqslant k}$ term disappears since $p_{\leqslant k}$ has period $\pi_N(k)$. It suffices to show that

$$\sum_{j\in\mathbb{Z}/\pi'_N(k)\mathbb{Z}} \sum_{\ell+\ell'=C_{i,m}(j)} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \equiv 0 \pmod N.$$

We can equivalently sum over ℓ and then ℓ' so that $\ell + \ell' \in [C_{i,m}(0), C_{i,m}(\pi'_N(k) - 1)]$. Suppose that $\ell \leqslant C_{i,m}(0)$. Observe that

$$\sum_{j\in\mathbb{Z}/\pi'_N(k)\mathbb{Z}} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell'+j) \equiv 0 \pmod N,$$

since $[q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q$ is fixed and $p_{=i}(\ell)$ is $p_{\leqslant i}(\ell - i)$ and so this sum becomes 0 by our assumption.

We need to show that the sum of all terms $\ell > C_{i,m}(0)$ is zero. Our reformulation gives us a sum over ℓ and ℓ' so $\ell + \ell' \leqslant C_{i,m}(\pi'_N(k) - 1)$ and $\ell > C_{i,m}(0)$. Although we can ignore $\ell = C_{i,m}(0)$ because it have no contribution, we include it in the following calculation to make it simpler. We can observe that by the restrictions on n that $[q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q$ stays in the same section. Let $Q = \max(\pi'_N(k-i), \pi'_N(i))$. Each possible pairing $([q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q, p_{=i}(\ell'))$ modulo N is repeated a multiple of $\sum_{x\in[\pi'_N(k)/Q]} x = \frac{1}{2}(\pi'_N(k)/Q)(\pi'_N(k)/Q + 1)$ times due to their respective periods. But since N divides $\pi'_N(k)/Q$ ($i \leqslant m \leqslant k-1$) and N is odd (the pairs in Theorem 2.6 have odd N), this is a multiple of N and hence the entire sum becomes 0 modulo N. □

Theorem 5.3. *Fix a pair (k, N) such that*

$$\sum_{i\in\mathbb{Z}/\pi'_N(k-1)\mathbb{Z}} p_{\leqslant k-1}(i) \equiv 0. \pmod N$$

by Theorem 2.6. Then the slope of $\mathcal{L}^{(i)}_k$ is equal to that of $\mathcal{L}^{(i')}_k$ where $i' \equiv i + \pi'_N(k-1) \pmod{\pi'_N(k)}$.

Proof. In order to prove the theorem, we actually make a deeper claim. Consider the q-binomial coefficients $\begin{bmatrix} n+k \\ k \end{bmatrix}_q, \begin{bmatrix} \widetilde{n}+k \\ k \end{bmatrix}_q$ where $\widetilde{n} = n + \pi'_N(k-1)$ and decompose the coefficients into S_i and $\widetilde{\mathsf{S}}_i$ respectively. Then when we make the decompositions $\mathsf{S}_i = \mathsf{B}_i^{\oplus l} \oplus \mathsf{R}_i$ and $\widetilde{\mathsf{S}}_i = \widetilde{\mathsf{B}}_i^{\oplus l} \oplus \widetilde{\mathsf{R}}_i$, we want to show that B_i is a cyclic shift of $\widetilde{\mathsf{B}}_i$. Since the main theorem implies that B_i is determined by the residue class of $n \pmod{\pi'_N(k)}$, it suffices to show this for n sufficiently large.

Using Lemma 4, we have

$$p_{\leqslant k}^{(m)}(j) \equiv p_{\leqslant k}(j+mn) - \sum_{i \in [m]} \left(\sum_{\ell + \ell' = C_{i,m}(j)} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \right) \pmod{N}$$

where $C_{i,m}(j) = (m-i)n + j$. Now we take $n \mapsto \widetilde{n} = n + \pi'_N(k-1)$ and obtain a function $\widetilde{p}_{\leqslant k}^{(m)}(j)$ for $\widetilde{\mathsf{S}}_m$. If we take $j \mapsto \widetilde{j} = j + m\pi'_N(k-1)$, we claim that

$$p_{\leqslant k}^{(m)}(\widetilde{j}) \equiv \widetilde{p}_{\leqslant k}^{(m)}(j) \pmod{N}.$$

This is equivalent to B_i being a cyclic shift of $\widetilde{\mathsf{B}}_i$. Here, we are implicitly taking $\widetilde{j} \pmod{\pi'_N(k)}$ and treating $p_{\leqslant k}^{(m)}$ as a periodic sequence - this avoids confusion with $\widetilde{\mathsf{R}}_i$, as the shift is within each block $\mathsf{B}_i \mapsto \widetilde{\mathsf{B}}_i$. Using Lemma 4 again, we see this is equivalent to

$$p_{\leqslant k}(\widetilde{j}+mn) - \sum_{i \in [m]} \#\mathcal{P}_{i,m}^{\text{bad}}(\widetilde{j}) \equiv p_{\leqslant k}(j + m\widetilde{n}) - \sum_{i \in [m]} \#\mathcal{P}_{i,m}^{\text{bad}}(j) \pmod{N}.$$

As $\widetilde{j} + mn = j + m\widetilde{n}$, we need only consider the sums $\sum_{i \in [m]} \#\mathcal{P}_{i,m}^{\text{bad}}(\cdot)$. We want to show that this is invariant modulo N under $j \mapsto \widetilde{j}$ and $n \mapsto \widetilde{n}$. We get for individual terms (indexed by i) the difference

$$\sum_{\ell+\ell' = C_{i,m}(\widetilde{j})} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') - \sum_{\ell+\ell' = \widetilde{C}_{i,m}(j)} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \pmod{N}$$

where $\widetilde{C}_{i,m}(j) = (m-i)\widetilde{n} + j$, differing from $C_{i,m}(j)$ by a multiple of $\pi'_N(k-1)$. We claim that this is 0 for $i > 1$. Because $p_{=i}$ has period $\pi_N(i) \mid \pi'_N(k-1)$ and $\pi'_N(k-1) \mid C_{i,m}(\widetilde{j}) - \widetilde{C}_{i,m}(j)$, we can add this quantity to ℓ' in the second sum (leaving it unchanged) to cancel terms. After this, we are left with

$$\sum_{\substack{\ell+\ell' = C_{i,m}(\widetilde{j}) \\ \ell > \widetilde{C}_{i,m}(j)}} [q^\ell] \begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q p_{=i}(\ell') \pmod{N}.$$

The difference is $C_{i,m}(\widetilde{j}) - \widetilde{C}_{i,m}(j) = i\pi'_N(k-1)$. For $k-1 > i > 1$, recall the division of residues in $\begin{bmatrix} n+(k-i) \\ k-i \end{bmatrix}_q \pmod{N}$ - the blocks have size $\pi'_N(k-i) = \text{len}(\mathsf{B}_\bullet)$ in each section. For n sufficiently large, we can keep all ℓ in the same section as $n = \text{len}(\mathsf{S}_\bullet)$ and $i\pi'_N(k-1)$ is independent of n. Note also that $\pi'_N(i)$ is a period of $p_{=i}$. As $\pi'_N(k-1)/\pi'_N(k-i), \pi'_N(k-1)/\pi'_N(i) \in N\mathbb{Z}$ for $1 < i < k-1$, this implies the entire sum is 0 because we repeat each period a multiple of N times and either $\pi'_N(i) \mid \pi'_N(k-i)$ or the other way around. At $i = k-1$, the q-binomial coefficient has all coefficients 1 so this becomes 0 by the restrictions on (k, N). For $i = 1$, $p_{=1}(\ell') = 1$ and the sum is 0 again by the restrictions on (k, N) and Theorem 5.2, since n is large enough that the ℓ values stay in the same section and we just sum over a period i times.

Thus, for sufficiently large n we have $p^{(m)}_{\leqslant k}(\widetilde{j}) = \widetilde{p}^{(m)}_{\leqslant k}(j)$. We conclude that $\widetilde{\mathsf{B}}_i$ is a cyclic shift of B_i and the result follows since the slopes of $\mathcal{L}^{(i)}_k$ depend only on the number of occurrences of the residue R in each B_i (which clearly is the same under a cyclic shift). □

6 Asymptotics for the quasiperiod

Given the complex nature of the definition for $\pi'_N(k)$ it is worth investigating asymptotics to understand how quickly $f_k(n)$ and its generating function grow in complexity. First we investigate asymptotics for $\pi_p(k)$ for each prime p. We have the expansion

$$\pi_p(k) = p^{b_p([k])} L_p([k]),$$

where $b_p([k])$ and $L_p([k])$ are as previously defined in Theorem 2.1. Note that $\text{lcm}([k]) = e^{\psi(k)}$ where $\psi(k)$ is the Chebyshev function. Let

$$\Pi(k) := \sum_{i \in [k]} p^{\nu_p(i)}.$$

We first consider the asymptotics of this function in Lemma 5.

Lemma 5.

$$\Pi(k) = \sum_{i \in [k]} p^{\nu_p(i)} \sim \frac{p-1}{p} k \log_p(k).$$

Proof. This can be done by observing that $\sum_{i \in [k]} p^{\nu_p(i)} = \sum_{i=0}^{\lfloor \log_p(k) \rfloor} \#V_{i,p} p^i$, where $V_{i,p} = \{j | j \in [k], \nu_p(j) = i\}$. Now we can take $\#V_{i,p} = \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^{i+1}} \right\rfloor$, yielding

$$\sum_{i=0}^{\lfloor \log_p(k) \rfloor} \#V_{i,p} p^i = \sum_{i \geqslant 0} \left(\left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^{i+1}} \right\rfloor \right) p^i \sim (p-1) \left(\sum_{i \geqslant 1} \left\lfloor \frac{k}{p^i} \right\rfloor p^{i-1} \right).$$

We now want to show $\sum_{i \geqslant 1} \left\lfloor \frac{k}{p^i} \right\rfloor p^{i-1} \sim \frac{k \log_p(k)}{p}$ for large k. That is, we want to show that $\lim_{k \to \infty} \frac{k \log_p(k)}{\sum_{i \geqslant 1} \left\lfloor \frac{k}{p^i} \right\rfloor p^i} = 1$. We obtain upper and lower bounds for the limit via $\frac{k}{p^i} \geqslant \lfloor \frac{k}{p^i} \rfloor \geqslant \frac{k}{p^i} - 1$, yielding the bounds

$$k \log_p(k) \geqslant \sum_{i \geqslant 1} \left\lfloor \frac{k}{p^i} \right\rfloor p^i \geqslant k \left(\log_p(k) - 1 - \frac{p}{p-1} \right).$$

Upon dividing we see

$$\frac{k\log_p(k)}{\sum_{i\geqslant 1}\left\lfloor \frac{k}{p^i}\right\rfloor p^i} \leqslant \frac{k\log_p(k)}{k(\log_p(k)-1-\frac{p}{p-1})} = 1 + \frac{(1+\frac{p}{p-1})k}{k\log_p(k)-(1+\frac{p}{p-1})k}.$$

Thus, the limit is bounded above by 1. The lower bound clearly goes to 1, and we conclude that

$$\sum_{i\in[k]} p^{\nu_p(i)} \sim \frac{p-1}{p} k\log_p(k).$$ □

The following lemma will be useful in understanding $L_p([k])$.

Lemma 6. $\nu_p(\mathrm{lcm}([k])) = \lfloor \log_p(k)\rfloor$.

Now we can make an asymptotic analysis for the log of $\pi_p(k)$, since we have asymptotics relating to both components of $\pi_p(k)$.

Theorem 6.1. *We have*

$$\log_p(\pi_p(k)) \sim \log_p\log_p(k) + \frac{\psi(k)}{\ln p}.$$

Proof. Using Lemma 6, we see

$$\pi_p(k) = p^{b_p([k])}L_p([k]) = \mathrm{lcm}([k])p^{b_p([k])-\lfloor\log_p(k)\rfloor}.$$

This can be simplified to

$$\begin{aligned}\log_p \pi_p(k) &= \frac{\psi(k)}{\ln p} + \big(b_p([k]) - \lfloor\log_p(k)\rfloor\big)\\ &= \frac{\psi(k)}{\ln p} + \big(\lceil\log_p \Pi(k)\rceil - \lfloor\log_p(k)\rfloor\big).\end{aligned} \tag{5}$$

We use Lemma 5 to show $\log_p \Pi(k) \sim \log_p\left(\frac{p-1}{p}k\log_p(k)\right)$. Ignoring constant terms, we simplify this asymptotic to

$$\log_p \Pi(k) \sim \log_p\log_p(k) + \log_p(k),$$

and in the limit floors become irrelevant so the $\log_p(k)$ term is cancelled in (5), yielding the desired asymptotic. □

Lemma 7. $\log_p\left(\frac{\pi_p'(k)}{\pi_p(k)}\right) \sim k - \log_p(k) - \log_p\log_p(k)$

Proof. Note that

$$\frac{\pi'_p(k)}{\pi_p(k)} = p^{\#S_k},$$

where

$$S_k = \left\{ i : i \leqslant k, \frac{\pi_p(i)}{\pi_p(i-1)} \notin p\mathbb{Z} \right\}.$$

The condition in S_k can be re-written in terms of the p-adic valuation as $\nu_p(\pi_p(i)) = \nu_p(\pi_p(i-1))$. But this valuation is just $b_p([i])$, so we really have $\#S_k = k - b_p([k])$. Now we can write

$$\#S_k = k - \lceil \log_p (\Pi(k)) \rceil$$

where we already have an asymptotic formula for $\Pi(k)$. We can obtain

$$\#S_k \sim k - \log_p \left(\frac{p-1}{p} k \log_p(k) \right).$$

This implies that

$$\begin{aligned} \log_p \left(\frac{\pi'_p(k)}{\pi_p(k)} \right) &= \#S_k \\ &\sim k - \log_p \left(\frac{p-1}{p} k \log_p(k) \right). \end{aligned}$$

Ignoring constants in the above asymptotic, we obtain the desired asymptotic. □

By understanding π_p, we can easily derive formulas for π'_p by simply accounting for a power of p as above. That is,

$$\begin{aligned} \log_p \pi'_p(k) &\sim \log_p \pi_p(k) + k - \log_p(k) - \log_p \log_p(k) \\ &\sim \frac{\psi(k)}{\ln p} + k - \log_p(k), \end{aligned}$$

where we have already bounded π_p via Theorem 6.1. The next task is to understand $\pi'_{p^e}(k)$. The lemma below yields an asymptotic estimate for $\log_p \pi'_{p^e}(k)$ through Theorem 6.1 and Lemma 7.

Lemma 8. *For prime powers of an odd prime, we have the formula*

$$\pi'_{p^e}(k) = p^{(k-1)(e-1)} \pi'_p(k). \tag{6}$$

For $p = 2$, this is off by a constant factor of $\frac{1}{2}$ if $e > 1$.

Proof. The idea behind this is to show $\nu_p(\pi_p(j+1)/\pi_p(j)) \leqslant 1$ for $j \geqslant 2$. This follows from $b_p([j+1]) - b_p([j]) \leqslant 1$, so we prove this claim instead. Observe that $\Pi(j+1) - \Pi(j) \leqslant j+1$. Let $p^i \leqslant j$ be the largest prime power of p less than or equal to j. But then

$$\Pi(j+1) \leqslant p^{b_p([j])} + j + 1 \leqslant p^{b_p([j])} + p^{i+1} \leqslant p^{b_p([j])+1}.$$

Note that $b_p([j]) \geqslant i+1$, since $j \geqslant 2$ implies $\Pi(j) > p^i$. Then we conclude the final inequality from $p^{b_p([j])} + p^{i+1} = (1+p^{-\ell})p^{b_p([j])}$ for some $\ell \geqslant 0$, and $p \geqslant 1+p^{-\ell}$ as $p \geqslant 2$. It follows that $b_p([j+1]) - b_p([j]) \leqslant 1$ and $\nu_p(\pi_p(j+1)/\pi_p(j)) \leqslant 1$ for $j \geqslant 2$.

Suppose we know $\nu_p(\pi_p(j+1)/\pi_p(j)) \leqslant 1$ at j. First consider the case when $\nu_p(\pi_p(j+1)/\pi_p(j)) = 1$. By definition

$$\pi'_{p^e}(j+1) = \pi'_{p^e}(j)\text{lcm}\left(p^e, \frac{\pi_p(j+1)}{\pi_p(j)}\right)$$

since $\pi_p(j+1)/\pi_p(j) = \pi_{p^e}(j+1)/\pi_{p^e}(j)$. In this case, to obtain $\pi'_{p^e}(j+1)$ we scale $\pi'_{p^e}(j)$ by p^{e-1} in addition to scaling by $\frac{\pi_p(j+1)}{\pi_p(j)}$. In the case where $\nu_p(\pi_p(j+1)/\pi_p(j)) = 0$, the very same reasoning shows we scale $\pi'_{p^e}(j)$ by p^e in addition to scaling by $\frac{\pi_p(j+1)}{\pi_p(j)}$.

Using this, we can obtain the exact formula for $\pi'_{p^e}(k)$ recursively if we assume $\nu_p(\pi_p(j+1)/\pi_p(j)) \leqslant 1$ holds for $1 \leqslant j < k$ (we proved it for $j \geqslant 2$). In $k-1$ recursive steps, we arrive at $\pi'_{p^e}(1) := 1$. Using the results above, we obtain

$$\pi'_{p^e}(k) = \prod_{1 \leqslant j < k} p^{e-\nu_p\left(\frac{\pi_p(j+1)}{\pi_p(j)}\right)} \frac{\pi_p(j+1)}{\pi_p(j)}$$

by compactly summarizing the factors across the two cases $\nu_p\left(\frac{\pi_p(j+1)}{\pi_p(j)}\right) = 1$ and 0. Since these are the only possibilities, when we pull out $p^{(e-1)(k-1)}$ we see that the factor which remains is $p^\ell(\prod_{1 \leqslant j<k} \frac{\pi_p(j+1)}{\pi_p(j)})$ where $\ell = \#\{j : 1 \leqslant j < k, \nu_p\left(\frac{\pi_p(j+1)}{\pi_p(j)}\right) = 0\}$ is the number of times we have p^e instead of p^{e-1}. Applying the same recursive computation in the $e=1$ case for $\pi'_p(k)$, this is $\pi'_p(k)$. Hence, assuming $\nu_p(\pi_p(j+1)/\pi_p(j)) \leqslant 1$ for all steps we obtain $\pi'_{p^e}(k) = p^{(k-1)(e-1)}\pi'_p(k)$.

For $p \neq 2$, we encounter no issues because we still have $\nu_p(\pi_p(2)/\pi_p(1)) \leqslant 1$, and so the exact formula holds. This is because $b_p([2]) - b_p([1]) = 1 - 0 = 1$. For $p = 2$ this does not hold, but our description of the recursive steps holds for all but the $j = 1$ step where it is off by a constant factor, and so for $p = 2$ the formula is off by a constant factor which is straighforward to compute. □

A useful consequence of this lemma is that

$$\nu_q(\pi'_{p^e}(k)) \sim \nu_q(p^{(k-1)(e-1)}\pi'_p(k))$$

for any prime q since for odd primes these are equal and for $p = 2$ they differ by a constant. Similarly, replacing ν_q with $\log_q$ or ln we have asymptotics for the logs.

We wish to use this result to understand the growth of $\ln \pi'_N(k)$. We can obtain a loose upper bound on $\ln \pi'_N(k) = \ln \text{lcm}_{p|N}\pi'_{p^{\nu_p(N)}}(k)$ by taking the product of these asymptotics. However, we can do better. As $k \to \infty$, we simply need to identify which term has the largest power of p associated to it for a given p. Set $\nu_q(N) = e_q$. For a prime $q \mid N$ not equal to p, we get

$$\nu_p(\pi'_{q^{e_q}}(k)) \sim \nu_p\left(q^{(k-1)(e_q-1)}\pi'_q(k)\right) = \nu_p(\pi'_q(k)).$$

The last equality is because $\nu_p(q) = 0$. We have $\nu_p(\pi'_q(k)) \sim \log_p(k)$ by Lemma 6. For p, we get

$$\nu_p\left(p^{(k-1)(e_p-1)}\pi'_p(k)\right) = \nu_p(\pi'_p(k)) + (k-1)(e_p-1).$$

Asymptotically, it is clear that this will quickly become dominant. We have

$$\nu_p\big(\pi'_p(k)\big) \sim k - \log_p(k) - \log_p \log_p(k) + \log_p \Pi(k)$$

by Lemma 7, $\nu_p(\pi_p(k)) = b_p([k]) \sim \log_p \Pi_p(k)$, and that $\pi'_p(k)/\pi_p(k)$ is a power of p. Thus, using Lemma 5 we see that only the k is relevant for the asymptotic, so for $p \mid N$ we have $\nu_p(\pi'_N(k)) \sim \nu_p(\pi'_{p^{e_p}}(k)) \sim ke_p$. For primes $p \nmid N$, we get an overall contribution to $\ln \pi'_N(k)$ in the limit of $\ln(\mathrm{lcm}([k])) - \sum_{p|N} \ln k$, where the sum comes from Lemma 6. Putting these together, since the logs in the sum are dominated by other terms we have

$$\begin{aligned}\ln \pi'_N(k) &\sim \sum_{p|N} ke_p \ln p + \psi(k)\\ &= k\ln N + \psi(k).\end{aligned}$$

Thus, we have proven the following theorem:

Theorem 6.2. *We have*

$$\ln \pi'_N(k) \sim k\ln N + \psi(k).$$

7 Conclusion and future directions

We have shown that the function $f_k(n)$ is quasipolynomial modulo any $N \in \mathbb{N}$, from which an explicit formula for the generating function $F_k(x)$ follows. Additionally, the structure of the coefficients of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ has been described in terms of the sections S_i of that q-binomial coefficient, and the repeating period in each section has been shown to retain some of the properties of $\mathcal{S}$.

A good future direction is to determine the minimal quasiperiod of $f_k(n)$. It is expected to lie somewhere between $\pi_N(k)$ and $\pi'_N(k)$ but it is unclear how the function actually behaves.

It is also interesting to investigate symmetry in the minimal period of the slopes of the functions $\mathcal{L}_k^{(i)}$ — if we let this period be P, we mean to determine when the slope of $\mathcal{L}_k^{(i)}$ matches that of $\mathcal{L}_k^{(P-i)}$ for $0 \leqslant i \leqslant P$. Figure 5 gives a counterexample (the slopes for $0 \leqslant i < 30$ are not symmetric in this way), but in many examples the pattern holds true.

Acknowledgements

The author thanks the MIT PRIMES program for making this research possible, as well as Younhun Kim for his guidance and Professor Stanley for suggesting the problem and giving feedback. Additionally, the author would like to thank the anonymous reviewer for several comments that improved the paper.

This material is based upon work supported by the National Science Foundation under grant no. DMS-1519580.

References

[1] Y. H. Kwong, *Minimum periods of binomial coefficients modulo m*, Fibonacci Quarterly, 27 (1989), pp. 348–351.

[2] ——, *Minimum periods of partition functions modulo m*, Utilitas Mathematica, 35 (1989), pp. 3–8.

[3] L. Manivel, *On the asymptotics of Kronecker coefficients*, Journal of Algebraic Combinatorics, 42 (2015), pp. 999–1025.

[4] A. Nijenhuis and H. S. Wilf, *Periodicities of partition functions and Stirling numbers modulo p*, Journal of Number Theory, 25 (1987), pp. 308–312.

[5] A. Sills and D. Zeilberger, *Formulæ for the number of partitions of n into at most m parts (using the quasi-polynomial ansatz)*, Advances in Applied Mathematics, 48 (2012), pp. 640–645.

[6] R. P. Stanley, *Enumerative Combinatorics: Volume 1*, Cambridge University Press, New York, NY, 2nd ed., 2012.

[7] ——, *Additional problems for EC1 and EC2*. http://www-math.mit.edu/~rstan/ec, 2017.

[8] R. P. Stanley and F. Zanello, *Some asymptotic results on q-binomial coefficients*, Annals of Combinatorics, 20 (2016), pp. 623–634.