

# $q$ -congruences, with applications to supercongruences and the cyclic sieving phenomenon

Ofir Gorodetsky

## Abstract

We establish a supercongruence conjectured by Almkvist and Zudilin, by proving a corresponding  $q$ -supercongruence. Similar  $q$ -supercongruences are established for binomial coefficients and the Apéry numbers, by means of a general criterion involving higher derivatives at roots of unity. Our methods lead us to discover new examples of the cyclic sieving phenomenon, involving the  $q$ -Lucas numbers.

## 1 Introduction

A sequence of integers  $\{a_n\}_{n \geq 1}$  is said to satisfy the Gauss congruences if, for all positive integers  $n$ ,

$$\sum_{d|n} \mu(d) a_{\frac{n}{d}} \equiv 0 \pmod{n}, \quad (1.1)$$

where  $\mu$  is the usual Möbius function, defined as

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = \prod_{i=1}^k p_i, p_i \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

Gauss proved that  $a_n = a^n$  satisfies the Gauss congruences for any prime number  $a$ . Gauss's result was later extended (independently by various authors) to the following family of examples:  $a_n = \text{Tr}(A^n)$  where  $A$  can be any square matrix over the integers. See the paper of Zarelua [Zar08] for a detailed survey and proofs (cf. Steinlein [Ste17] and Corollary 3.1 below). Other terms for a sequence satisfying the Gauss congruences include ‘Gauss sequence’ [Gil89, Min14], ‘generalized Fermat sequence’ [DHL03], and ‘Dold sequence’ [JM06, Ch. 3.1]. It is known that condition (1.1) holds if and only if the following holds for all primes  $p$  and positive integers  $n, k$ :

$$a_{p^k n} \equiv a_{p^{k-1} n} \pmod{p^k}, \quad (1.2)$$

see Proposition 3.1. For instance, if  $a \geq b$  are positive integers, it is known that  $a_n = \binom{an}{bn}$  satisfies (1.2) for all primes  $p$  [Rob00, Ch. 7.1.6], and so it satisfies the Gauss congruences.

In this paper we introduce the following  $q$ -analogue of (1.1), which seems to be new. First, for any positive integer  $n$ , define the following polynomial in variable  $q$ , which attains the value  $n$  at  $q = 1$ :

$$[n]_q = \frac{q^n - 1}{q - 1} \in \mathbb{Z}[q].$$

**Definition 1.1.** A sequence of polynomials  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  is said to satisfy the ‘ $q$ -Gauss congruences’ if, for all positive integers  $n$ ,

$$\sum_{d|n} \mu(d) a_{n/d}(q^d) \equiv 0 \pmod{[n]_q}. \quad (1.3)$$

In (1.3), the condition  $f(q) \equiv 0 \pmod{g(q)}$  for polynomials  $f, g \in \mathbb{Z}[q]$  means  $f(q)/g(q) \in \mathbb{Z}[q]$ . Since in (1.3) the modulus  $g$  is a monic polynomial, Gauss's lemma tells us that the weaker condition  $f(q)/g(q) \in \mathbb{Q}[q]$  is equivalent to  $f(q)/g(q) \in \mathbb{Z}[q]$ . Some simple examples of sequences that satisfy the  $q$ -Gauss congruences are  $a_n(q) = 1$  and  $a_n(q) = q^n$ .

An important consequence of the definition, which is the main motivation behind this paper, is that if  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences, then  $\{a_n(1)\}_{n \geq 1}$  satisfies the Gauss congruences – this follows by substituting  $q = 1$  in (1.3). So one possible way to prove that a sequence satisfies the Gauss congruences is to find a  $q$ -analogue of it that satisfies the  $q$ -Gauss congruences. As demonstrated in recent works of Guo and Zudilin [GZ18] and Straub [Str19], the approach of establishing congruences via  $q$ -congruences is fruitful because of additional techniques available in the  $q$ -setting. In this work we make heavy use of the derivative and its properties.

**Remark 1.2.** In Lemma 2.2 we show that if  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences, then for all primes  $p$  and all  $n, k \geq 1$

$$a_{p^k n}(q) \equiv a_{p^{k-1}n}(q^p) \pmod{[p^k]_q}. \quad (1.4)$$

There is no implication in the reverse direction.

**Remark 1.3.** The special case  $k = 1$  of (1.2) is a special case of the Lucas congruences, while the special case  $k = 1$  of (1.4) is a special case of the  $q$ -Lucas congruences.

## 1.1 Notation

We use the following notation throughout. For any positive integer  $n$ , let  $\omega_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$  be a primitive root of unity of order  $n$ , let  $\Phi_n(q) \in \mathbb{Z}[q]$  be the  $n$ -th cyclotomic polynomial, and set  $\mu_n = \{\omega_n^i : i \in \mathbb{Z}\}$ . Given  $\omega \in \mu_n$ , we write  $\text{ord}(\omega)$  for its order. The notation  $[u^n]f(u)$ , where  $f$  is a power series in  $u$ , means the coefficient of  $u^n$  in  $f$ . We will often write  $(a, b)$  instead of  $\gcd(a, b)$ . For any  $n \geq 1$ , we set

$$[n]_q! = \prod_{i=1}^n [i]_q,$$

and also  $[0]_q! = 1$ . We define, for all  $n \geq k \geq 0$ ,

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

The rational functions  $\begin{bmatrix} n \\ k \end{bmatrix}_q$  are in fact polynomials in  $\mathbb{Z}[q]$ , known as Gaussian binomial coefficients or  $q$ -binomial coefficients [Coh04]. Their value at  $q = 1$  is  $\binom{n}{k}$ . The  $q$ -binomial coefficients satisfy the  $q$ -binomial theorem [Cha11, Ch. 3.2]:

$$\prod_{i=0}^{n-1} (1 + tq^i) = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q t^k q^{\binom{k}{2}}. \quad (1.5)$$

We may also take (1.5) to be the definition of  $\begin{bmatrix} n \\ k \end{bmatrix}_q$ .

## 1.2 First examples

A main theme in this work is roots of unity. As we shall show in Corollary 2.3, a sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences if and only if

$$a_n(\omega) = a_{\frac{n}{\text{ord}(\omega)}}(1) \quad (1.6)$$

for all  $n \geq 1$  and  $\omega \in \mu_n$ . This criterion provides almost immediately the examples below, verified in §5.1. Let  $a \geq b \geq 1$  be integers.

**Example 1.4.** The sequence  $a_n(q) = \begin{bmatrix} an \\ bn \end{bmatrix}_q$  satisfies the  $q$ -Gauss congruences. It is a  $q$ -analogue of  $a_n(1) = \binom{an}{bn}$ . Up to a power of  $q$ ,  $\begin{bmatrix} an \\ bn \end{bmatrix}_q$  is the coefficient of  $t^{bn}$  in  $\prod_{i=0}^{an-1} (1 + tq^i)$ , as follows from (1.5).

**Example 1.5.** The sequence  $b_n(q) = \begin{bmatrix} an-1 \\ bn \end{bmatrix}_q$  satisfies the  $q$ -Gauss congruences. It is a  $q$ -analogue of  $b_n(1) = \binom{an-1}{bn}$ . It is equal to the coefficient of  $t^{bn}$  in  $\prod_{i=0}^{an-bn-1} (1 - tq^i)^{-1}$ , as follows from the  $q$ -binomial series [Cha11, Ch. 3.2]:

$$\prod_{i=0}^{n-1} (1 - tq^i)^{-1} = \sum_{k \geq 0} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q t^k.$$

**Example 1.6.** The sequence  $c_n(q) = [t^{bn}] \prod_{i=0}^{n-1} (1 - tq^i)^a$  satisfies the  $q$ -Gauss congruences. It is a  $q$ -analogue of  $c_n(1) = (-1)^{bn} \binom{an}{bn}$ . Choosing  $a = b = 1$ ,  $c_n(q)$  equals  $(-1)^n q^{\binom{n}{2}}$ , which is a  $q$ -analogue of  $(-1)^n$  that satisfies the  $q$ -Gauss congruences.

### 1.3 Main results

The following theorem, proved in §5.1, provides interesting examples of sequences satisfying the  $q$ -Gauss congruences. The theorem is established using criterion (1.6).

**Theorem 1.1.** The following sequences satisfy the  $q$ -Gauss congruences.

1.  $d_n(q) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} q^{i(i+b)} \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{bmatrix} n-i \\ i \end{bmatrix}_q$ , for any integer  $b \geq -1$ .
2.  $e_n(q) = \text{Tr}(A(q^{n-1})A(q^{n-2}) \cdots A(1))$ , where

$$A(x) = \begin{bmatrix} 1 & x \\ 1 & 0 \end{bmatrix} \in \text{Mat}_2(\mathbb{Z})[x].$$

The sequence  $d_n(q)$  is a  $q$ -analogue of  $d_n(1) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i} \binom{n-i}{i}$ , the central trinomial coefficient, that is, the  $n$ -th coefficient of  $(1 + x + x^2)^n$ . This  $q$ -analogue was first introduced by Andrews and Baxter [AB87, Eq. (2.7);  $A = 0$ ] in the context of statistical mechanics. More generally, the trinomial coefficient  $\binom{n}{a}_2$  is the coefficient of  $x^a$  in  $(1 + x + x^{-1})^n$ , and it has the  $q$ -analogue [AB87, Eq. (2.7)]

$$\begin{bmatrix} n; b; q \\ a \end{bmatrix}_2 = \sum_{i=0}^{\lfloor \frac{n-a}{2} \rfloor} q^{i(i+b)} \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{bmatrix} n-i \\ i+a \end{bmatrix}_q, \quad (1.7)$$

where  $b$  is an integer parameter. This  $q$ -analogue was studied extensively by Andrews [And90a, And90b, And94] and Warnaar [War01, War03] and we shall return to it in the next theorem. In §3 we show that  $d_n(1)$  satisfies the Gauss congruences, independently of Theorem 1.1. A congruence for  $d_n(1)$  of different flavor (namely, of Lucas type) was proved by Deutsch and Sagan [DS06, Thm. 4.7].

The sequence  $e_n(q)$  is a  $q$ -analogue of  $e_n(1) = \text{Tr}(A(1)^n) = L_n$ , the Lucas numbers, defined usually as  $L_n = F_{n-1} + F_{n+1}$ , where  $F_n$  are the Fibonacci numbers. Schur [Sch17] considered the following  $q$ -analogues of the Fibonacci numbers, in his study of the Rogers-Ramanujan identities:

$$\begin{aligned} F_n(q) &= F_{n-1}(q) + q^{n-2} F_{n-2}(q), & F_0(q) &= 0, F_1(q) = 1, \\ G_n(q) &= G_{n-1}(q) + q^{n-1} G_{n-2}(q), & G_0(q) &= 0, G_1(q) = 1. \end{aligned}$$

These  $q$ -analogues were studied by Andrews [And04], Carlitz [Car74, Car75], Cigler [Cig03, Cig04, Cig16], Pan [Pan06, Pan13] and others. As can be shown inductively, we have [Cig16, Eq. (1.8)]

$$A(q^{n-1})A(q^{n-2}) \cdots A(1) = \begin{bmatrix} F_{n+1}(q) & G_n(q) \\ F_n(q) & G_{n-1}(q) \end{bmatrix},$$

and so

$$e_n(q) = F_{n+1}(q) + G_{n-1}(q) \quad (1.8)$$

for all  $n \geq 1$ . The  $q$ -analogue  $e_n(q)$  of the Lucas numbers, as defined in (1.8), was introduced by Pan, who proved that [Pan13, Thm. 1.1;  $(\alpha, \beta, \gamma, \delta) = (0, 0, 1, 1)$ ]

$$e_n(q) \equiv 1 \pmod{\Phi_n(q)} \quad (1.9)$$

for all  $n \geq 1$  (Pan stated his result for  $n \geq 3$ , but a short calculation shows that it holds for  $n = 1, 2$  as well). We use (1.9) in the proof of Theorem 1.1, which can be considered as a generalization of it. Indeed, using criterion (1.6) with  $a_n(q) = e_n(q)$  and with primitive roots of unity of order  $n$ , one recovers (1.9).

Theorem 1.1 suggests new examples of the Cyclic Sieving Phenomenon (CSP). We recall the definition of the CSP, which was first defined by Reiner, Stanton and White [RSW04]. Let  $X$  be a finite set,  $C$  be a

finite cyclic group acting on  $X$ , and  $f(q)$  be a polynomial in  $q$  with non-negative integer coefficients. Then the triple  $(X, C, f(q))$  exhibits the CSP if, for all  $g \in C$ , we have

$$|X^g| = f(\omega),$$

where  $X^g$  is the fixed point set of  $g$ , and  $\omega$  is a root of unity whose order is the same as  $g$ 's. The simplest interesting example is probably the following. Let  $A_{n,k}$  be the set of words (that is, finite sequences)  $w$  of length  $n$  with  $k$  0-s and  $n - k$  1-s. Let  $\mathbb{Z}/n\mathbb{Z}$  act on  $A_{n,k}$  by rotation. Then  $(A_{n,k}, \mathbb{Z}/n\mathbb{Z}, \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_q)$  exhibits the CSP. We suggest Sagan's survey [Sag11] on the topic.

The behavior of sequences satisfying the  $q$ -Gauss congruences on roots of unity, described by criterion (1.6), makes them plausible candidates for the CSP. Indeed, suppose that  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences and that  $a_n(q)$  has non-negative coefficients for all  $n \geq 1$ . Suppose further that there are sets  $\{X_n\}_{n \geq 1}$  such that  $|X_n| = a_n(1)$ , and  $\mathbb{Z}/n\mathbb{Z}$  acts on  $X_n$  in such a way that  $|X_n^i| = |X_{\gcd(n,i)}|$  for all  $n \geq 1$ ,  $i \in \mathbb{Z}/n\mathbb{Z}$ . Then, by definition,  $(X_n, \mathbb{Z}/n\mathbb{Z}, a_n(q))$  exhibits the CSP for all  $n \geq 1$ .

In particular, Theorem 1.1 gives rise to two families exhibiting the CSP. Let  $B_{n,0}$  be the set of words of length  $n$  on letters 0, 1 and 2, such that the number of 0-s is equal to the number of 2-s. Let  $C_n$  be the set of words  $w$  of length  $n$  on letters 0 and 1, such that there are no consecutive 1-s in  $w$ , not even cyclically ( $w_1 = w_n = 1$  is not allowed). Let  $\mathbb{Z}/n\mathbb{Z}$  act by rotation on both  $B_{n,0}$  and  $C_n$ . A short calculation using Theorem 1.1 shows that  $(B_{n,0}, \mathbb{Z}/n\mathbb{Z}, d_n(q))$  and  $(C_n, \mathbb{Z}/n\mathbb{Z}, e_n(q))$  exhibit the CSP for all  $n \geq 1$ . The following result, proved in §6, shows that much more is true.

**Theorem 1.2.**

1. Fix integers  $n \geq 1$ ,  $|k| \leq n$  and  $b \geq -1$ . Let  $B_{n,k}$  be the set of words  $w$  of length  $n$  on letters 0, 1 and 2, such that the number of 0-s minus the number of 2-s is equal to  $k$ . Let  $\mathbb{Z}/n\mathbb{Z}$  act on  $B_{n,k}$  by rotation. Then  $(B_{n,k}, \mathbb{Z}/n\mathbb{Z}, \left[ \begin{smallmatrix} n; b; q \\ k \end{smallmatrix} \right]_2)$  exhibits the CSP, where  $\left[ \begin{smallmatrix} n; b; q \\ k \end{smallmatrix} \right]_2$  is defined in (1.7).
2. Fix integers  $n \geq 1$ ,  $0 \leq k \leq \frac{n+1}{2}$ . Let  $C_{n,k}$  be the set of words  $w$  of length  $n$  with  $k$  1-s and  $n - k$  0-s, such that there are no consecutive 1-s in  $w$ , not even cyclically ( $w_1 = w_n = 1$  is not allowed). Let  $\mathbb{Z}/n\mathbb{Z}$  act on  $C_{n,k}$  by rotation. Set  $e_{n,k}(q) = [t^k] \text{Tr}(A(q^{n-1}, t)A(q^{n-2}, t) \cdots A(1, t))$  where

$$A(x, t) = \begin{bmatrix} 1 & x \\ t & 0 \end{bmatrix} \in \text{Mat}_2(\mathbb{Z})[x, t].$$

Then  $(C_{n,k}, \mathbb{Z}/n\mathbb{Z}, e_{n,k}(q))$  exhibits the CSP.

Note that  $e_n(q) = \sum_k e_{n,k}(q)$ . The polynomial  $e_{n,k}(q)$  has a closed form. For a word  $w$  of length  $n$  on letters 0 and 1, let

$$W_1(w) = \sum_{1 \leq i \leq n: w_i=1} (n-i), \quad W_2(w) = \sum_{1 \leq i \leq n: w_i=1} i.$$

In (6.7) we prove that  $e_{n,k}(q)$  is equal to  $\sum_{w \in C_{n,k}} q^{W_1(w)}$ . Since  $w \in C_{n,k}$  if and only if the mirror image of  $w$  (namely the word  $w_n, w_{n-1}, \dots, w_1$ ) is in  $C_{n,k}$ , this shows that  $e_{n,k}(q) = g(n, k)/q^k$ , where  $g(n, k)$  is a polynomial in  $q$  given by

$$g(n, k)(q) = \sum_{w \in C_{n,k}} q^{W_2(w)}.$$

The polynomial  $g(n, k)$  was studied by Carlitz [Car74], who proved that

$$g(n, k) = q^{k^2} \begin{bmatrix} n-k+1 \\ k \end{bmatrix}_q - q^{n+(k-1)^2} \begin{bmatrix} n-k-1 \\ k-2 \end{bmatrix}_q.$$

The following theorem concerns supercongruences, an informal notion referring to congruences where the modulus is a surprisingly high power. Before we state our theorem, we need the following definition.

**Definition 1.7.** Let  $r$  be a positive integer. A sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  is said to satisfy the ' $q$ -Gauss congruences of order  $r$ ' if it satisfies the  $q$ -Gauss congruences, and in addition, for all  $n \geq 1$  and  $1 \leq j \leq r-1$ , the function

$$f_{n,j}: \mu_n \rightarrow \mathbb{C}, \quad \omega \mapsto \omega^j a_n^{(j)}(\omega),$$

depends only on  $\text{ord}(\omega)$ . Here  $a_n^{(j)}(q)$  is the  $j$ -th derivative of  $a_n(q)$ .

As we shall show in Theorem 2.4, we have the following implication. If  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences of order  $r$  then for all  $n, k \geq 1$  and primes  $p \geq r + 1$ , we have

$$a_{np^k}(1) \equiv a_{np^{k-1}}(1) \pmod{p^{rk}}. \quad (1.10)$$

The following theorem concerns three different sequences. For each sequence, a more detailed theorem is given later in Theorems 2.6, 2.7, 2.8.

**Theorem 1.3.** *The following sequences satisfy the  $q$ -Gauss congruences of order 3.*

1.  $f_n(q) = \left[ \frac{an}{bn} \right]_q$  for  $a \geq b \geq 1$ .
2.  $g_n(q) = \sum_{k=0}^n \left[ \frac{n}{k} \right]_q^2 \left[ \frac{n+k}{k} \right]_q^2 q^{f(n,k)}$ , where  $f(x, y) = y^2 + Axy + Bx^2 \in \mathbb{Z}[x, y]$  is a polynomial satisfying  $f(n, k) \geq 0$  for all  $n, k \geq 0$ .
3.  $h_n(q) = \sum_{\substack{0 \leq \ell \leq k \leq n \\ n \leq k+\ell}} \left[ \frac{n}{k} \right]_q^2 \left[ \frac{n}{\ell} \right]_q \left[ \frac{k}{\ell} \right]_q \left[ \frac{k+\ell}{n} \right]_q q^{f(n,k,\ell)}$ , where  $f(x, y, z) = y^2 + z^2 + Ax^2 + Bxy + Cxz + Dyz \in \mathbb{Z}[x, y, z]$  is a polynomial satisfying  $f(n, k, \ell) \geq 0$  for all  $n, k, \ell \geq 0$ .

From Theorem 1.3 and (1.10) we have the following corollary.

**Corollary 1.4.** *Let  $p \geq 5$  be a prime. Then, in the notation of Theorem 1.3, for all  $n, k \geq 1$  we have*

$$\left( \frac{ap^k}{bp^k} \right) \equiv \left( \frac{ap^{k-1}}{bp^{k-1}} \right) \pmod{p^{3k}}, \quad (1.11)$$

$$g_{np^k}(1) \equiv g_{np^{k-1}}(1) \pmod{p^{3k}}, \quad (1.12)$$

$$h_{np^k}(1) \equiv h_{np^{k-1}}(1) \pmod{p^{3k}}. \quad (1.13)$$

The supercongruence (1.11) is attributed to Ljunggren and Jacobsthal [BSF<sup>+</sup>52]. The sequence  $g_n(q)$  is a  $q$ -analogue of

$$g_n(1) = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2,$$

a sequence of integers named ‘‘Apéry numbers’’ after Roger Apéry, who introduced them in his proof of the irrationality of  $\zeta(3)$  [Apé79], where  $\zeta$  is the Riemann zeta function. The supercongruence (1.12) was proved by Beukers [Beu85] and Coster [Cos88]. Before (1.12) was proved, the special case  $k = 1$  was conjectured by Chowla, Cowles and Cowles [CCC80] and proved by Gessel [Ges82] and Mimura [Mim83]. Apéry has shown that the sequence  $\{g_n(1)\}_{n \geq 1}$  satisfies the recurrence relation

$$(n+1)^3 u_{n+1} - (2n+1)(17n^2 + 17n + 5)u_n + n^3 u_{n-1} = 0, \quad (u_0 = 0, u_1 = 5),$$

which implies that the generating function  $F(x) = \sum_{n \geq 1} g_n(1)x^n$  satisfies a third-order differential equation. The function  $F(x)$  also enjoys a ‘modular parameterization’, see [Beu87]. The supercongruence (1.13) is new. The sequence  $h_n(q)$  is a  $q$ -analogue of

$$h_n(1) = \sum_{k, \ell} \binom{n}{k}^2 \binom{n}{\ell} \binom{k}{\ell} \binom{k+\ell}{n},$$

a sequence of integers introduced originally by Almkvist and Zudilin in their study of Calabi-Yau differential equations [AZ06]. The sequence is denoted there by the letter  $\zeta$ , and this is the way it is referred to in the literature [AvSZ11, OSS16, MS16]. Almkvist and Zudilin found the sequence by searching, empirically, for *integer* sequences satisfying the recurrence

$$(n+1)^3 u_{n+1} - (2n+1)(an^2 + an + b)u_n + cn^3 u_{n-1} = 0$$

for some  $a, b, c \in \mathbb{Z}$  (see Zagier [Zag09] and Cooper [Coo12] for related searches). They found 5 solutions apart from the Apéry numbers (cf. [AvSZ11, Eq. (4.12)], [OSS16, Table 2], [MS16, Table 2]), which are often

referred to as Apéry-like sequences. One of them is  $h_n(1)$ , corresponding to  $(a, b, c) = (9, 3, -27)$ . These 5 sequences are conjectured to satisfy the supercongruences

$$u_{np^k} \equiv u_{np^{k-1}} \pmod{p^{3k}}. \quad (1.14)$$

for all  $n, k \geq 1$  and primes  $p \geq 5$ . For three out of these 5 sequences, (1.14) was proved by Osburn and Sahu [OS13] and Osburn, Sahu and Straub [OSS16]. For another one of these sequences, (1.14) was proved in the case  $k = 1$  by Amdeberhan and Tauraso [AT16]. Malik and Straub [MS16, Thm. 3.1] have proved that all 5 Apéry-like sequences satisfy Lucas-type congruences.

Theorem 2.4 below gives us much more than integer congruences. It uses the fact that  $a_n(q)$  satisfies the  $q$ -Gauss congruences of order  $r$  to construct an explicit formula for the remainder of  $a_{np^k}(q)$  upon division by  $[p^k]_q^r$  ( $p \geq r + 1$ ), let us denote it by  $r(q)$ . The supercongruence (1.10) is deduced by substituting  $q = 1$  in the  $q$ -supercongruence  $a_{np^k}(q) \equiv r(q) \pmod{[p^k]_q^r}$ . The details are provided in the next section.

**Remark 1.8.** *Theorem 2.4 determines not only the remainder of  $a_{np^k}(q)$  modulo  $[p^k]_q^r$  for primes  $p \geq r + 1$ , but actually the remainder of  $a_{nm}(q)$  modulo  $[m]_q^r$  for any  $m \geq 1$  which is not divisible by primes less than  $r + 1$ .*

## 2 Methods

Most of the proofs of the results in §1.2–1.3 follow from Corollaries 2.3 and 2.5, which themselves follow from more general results that we discuss here. To state these results, we introduce some new notions.

### 2.1 Gauss congruences with respect to a set of primes

Let  $\mathbb{P}$  denote the set of primes. Given  $S \subseteq \mathbb{P}$ , we denote by  $\mathbb{N}_S$  the set of positive integers divisible only by primes from  $S$ .

**Definition 2.1.** Let  $S \subseteq \mathbb{P}$ . A sequence of integers  $\{a_n\}_{n \geq 1}$  is said to satisfy the ‘Gauss congruences with respect to  $S$ ’ if, for all  $n \in \mathbb{N}_S$  and  $m \geq 1$ ,

$$\sum_{d|n} \mu(d) a_{\frac{n}{d}} \equiv 0 \pmod{n}. \quad (2.1)$$

A sequence of polynomials  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  is said to satisfy the ‘ $q$ -Gauss congruences with respect to  $S$ ’ if, for all  $n \in \mathbb{N}_S$  and  $m \geq 1$ ,

$$\sum_{d|n} \mu(d) a_{\frac{n}{d}}(q^d) \equiv 0 \pmod{[n]_q}. \quad (2.2)$$

We see that if  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences with respect to  $S$ , then  $\{a_n(1)\}_{n \geq 1}$  satisfies the Gauss congruences with respect to  $S$ . In the special case  $S = \{p\}$ , (2.1) becomes (1.2) with the prime  $p$  fixed, and (2.2) becomes (1.4) with the prime  $p$  fixed. In §3, we prove the following.

**Lemma 2.1.**

1. A sequence  $\{a_n\}_{n \geq 1} \subseteq \mathbb{Z}$  satisfies the Gauss congruences with respect to  $S \subseteq \mathbb{P}$  if and only if (1.2) holds for all  $p \in S$ .
2. A sequence  $\{a_n\}_{n \geq 1} \subseteq \mathbb{Z}$  satisfies the Gauss congruences with respect to  $\mathbb{P}$  if and only if it satisfies the Gauss congruences.

We have a partial  $q$ -analogue of Lemma 2.1, proved in §4.

**Lemma 2.2.**

1. If a sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences with respect to  $S \subseteq \mathbb{P}$  then (1.4) holds for all  $p \in S$  and all  $n, k \geq 1$ .

2. A sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences with respect to  $\mathbb{P}$  if and only if it satisfies the  $q$ -Gauss congruences.

In view of the second part of Lemma 2.2, whenever we prove a theorem on sequences satisfying the  $q$ -Gauss congruences with respect to an arbitrary  $S \subseteq \mathbb{P}$ , we also obtain, in the special case  $S = \mathbb{P}$ , a result on sequences satisfying the  $q$ -Gauss congruences.

## 2.2 General results

In §4 we prove the following characterization.

**Proposition 2.2.** *Let  $S \subseteq \mathbb{P}$  and  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$ . The following are equivalent.*

1.  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences with respect to  $S$ .
2. For all  $m \geq 1$  and  $n \in \mathbb{N}_S$ , and every  $\omega \in \mu_n$ , we have

$$a_{nm}(\omega) = a_{\frac{nm}{\text{ord}(\omega)}}(1). \quad (2.3)$$

3. For all  $m \geq 1$  and  $n \in \mathbb{N}_S$ , and every  $d \mid n$ , we have

$$a_{nm}(q) \equiv a_{\frac{nm}{d}}(1) \pmod{\Phi_d(q)}.$$

In particular, we have the following immediate corollary of Lemma 2.2 and Proposition 2.2, obtained by taking  $S = \mathbb{P}$  in Proposition 2.2.

**Corollary 2.3.** *The sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences if and only if, for all  $n, i \geq 1$ , we have*

$$a_n(\omega_n^i) = a_{(n,i)}(1),$$

which holds if and only if, for all  $n \geq 1$  and every  $d \mid n$ , we have

$$a_n(q) \equiv a_{n/d}(1) \pmod{\Phi_d(q)}.$$

**Example 2.3.** *Let  $a$  be a positive integer. Pan [Pan08] studied  $a_n(q) = \prod_{i=1}^n [a]_{q^i}$ , a  $q$ -analogue of  $a_n(1) = a^n$ . He proved that*

$$\sum_{d \mid n} \mu(d) a_{n/d}(q^d) \equiv 0 \pmod{[n]_{q^{\gcd(n,a)}}}$$

for all  $n \geq 1$ . Using Proposition 2.2, it can be shown quickly that  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences with respect to  $S = \mathbb{P} \setminus \{p \in \mathbb{P} : p \mid a\}$ . Indeed, for all  $m \geq 1$ ,  $n \in \mathbb{N}_S$  and  $\omega \in \mu_n$ , we have

$$\begin{aligned} a_{nm}(\omega) &= \prod_{i=1}^{nm} [a]_{\omega^i} = \left( \prod_{i=1}^{\text{ord}(\omega)} [a]_{\omega^i} \right)^{nm/\text{ord}(\omega)} \\ &= \left( a \prod_{i=1}^{\text{ord}(\omega)-1} \frac{\omega^{ia} - 1}{\omega^i - 1} \right)^{nm/\text{ord}(\omega)} = a^{nm/\text{ord}(\omega)} = a_{nm/\text{ord}(\omega)}(1). \end{aligned}$$

Our next proposition shows that if  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences with respect to  $S$ , then we can determine the remainder of  $a_{nm}(q)$  upon division by  $[n]_q$  as long as  $n \in \mathbb{N}_S$ . It will be convenient to introduce the following polynomials.

**Definition 2.4.** For any  $n \geq 1$ , let  $D_n = \{d : d \text{ a divisor of } n, d \neq n\}$  be the set of proper divisors of  $n$ . For a function  $g : D_n \rightarrow \mathbb{C}$ , let

$$G_{g,n}(q) = \sum_{d \in D_n} \frac{[n]_q}{[n/d]_q} \frac{\sum_{e \mid d} \mu\left(\frac{d}{e}\right) g(e)}{d} \in \mathbb{C}[q].$$

The main property of  $G_{g,n}$  is that the value of  $G_{g,n}(\omega)$  for  $\omega \in \mu_n$  depends only on the order of  $\omega$ . In §4 we establish the following formula.

**Proposition 2.5.** *Assume that the sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences with respect to  $S \subseteq \mathbb{P}$ . Let  $n, m$  be positive integers with  $n \in \mathbb{N}_S$ . Then the remainder of  $a_{nm}(q)$  upon division by  $[n]_q$  is*

$$a_{nm}(q) \equiv G_{g,n}(q) \pmod{[n]_q},$$

where

$$g: D_n \rightarrow \mathbb{C}, \quad g(d) = a_{dm}(1).$$

Our next theorem concerns sequences satisfying the  $q$ -Gauss congruences of order  $r$  with respect to  $S \subseteq \mathbb{P}$ . This notion generalizes Definition 1.7, which corresponds to the special case  $S = \mathbb{P}$ .

**Definition 2.6.** Let  $S \subseteq \mathbb{P}$  and  $r$  a positive integer. A sequence  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  is said to satisfy the ‘ $q$ -Gauss congruences of order  $r$  with respect to  $S$ ’ if it satisfies the  $q$ -Gauss congruences with respect to  $S$ , and in addition, for all  $m \geq 1$ ,  $n \in \mathbb{N}_S$  and  $1 \leq j \leq r-1$ , the function

$$f_{n,m,j}: \mu_n \rightarrow \mathbb{C}, \quad \omega \mapsto \omega^j a_{nm}^{(j)}(\omega)$$

depends only on  $\text{ord}(\omega)$ .

The next theorem shows that if  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences of order  $r$  with respect to  $S$ , then we can determine the remainder of  $a_{nm}(q)$  upon division by  $[n]_q^r$  as long as  $n \in \mathbb{N}_S$  and  $n$  is not divisible by primes less than  $r+1$ . Our theorem is most easily stated using the notion of  $[n]_q$ -digits of a polynomial.

**Definition 2.7.** For any polynomial  $F(q) \in \mathbb{C}[q]$  and any integer  $n > 1$ , we may expand  $F$  in base  $[n]_q$ , that is, we may write

$$F(q) = \sum_{i=0}^{\lfloor \deg F / (n-1) \rfloor} f_i(q) [n]_q^i,$$

with  $\deg f_i(q) < n-1$ . For every  $i$ ,  $f_i(q)$  is unique and we refer to it as the  $i$ -th  $[n]_q$ -digit of  $F$ . We define  $f_i = 0$  for  $i > \lfloor \deg F / (n-1) \rfloor$ .

If  $F(q) \in \mathbb{Z}[q]$ , then since  $[n]_q$  is monic, the polynomials  $\{f_i(q)\}_{i=0}^{\lfloor \deg F / (n-1) \rfloor}$  must have integer coefficients. In particular, for all  $k \geq 0$ ,

$$F(1) \equiv \sum_{i=0}^{k-1} f_i(1) n^i \pmod{n^k}.$$

We see that determining  $[n]_q$ -digits of  $F$  gives us information on  $F(1)$  modulo higher powers of  $n$ . We may now state the theorem, which is an extension of Proposition 2.5.

**Theorem 2.4.** *Assume that  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences of order  $r$  with respect to  $S \subseteq \mathbb{P}$ , for some  $r \geq 0$ . Let  $n \geq 2$ ,  $m \geq 1$  be integers with  $n \in \mathbb{N}_S$ . Let  $p$  be the smallest prime divisor of  $n$ . For any  $0 \leq i \leq r-1$ , define the function*

$$g_i: D_n \rightarrow \mathbb{C}, \quad g_i(d) = (\omega_n^d)^i a_{mn}^{(i)}(\omega_n^d).$$

Then the first  $1 + \min\{p-2, r-1\}$   $[n]_q$ -digits of  $a_{mn}(q)$  are given recursively by

$$f_i(q) = \frac{1}{i! n^i} \left( (q-1)^i G_{g_i,n}(q) - \sum_{m_1=0}^{i-1} \sum_{m_2=m_1}^i \binom{i}{m_2} f_{m_1}^{(i-m_2)}(q) R_{n,m_1,m_2}(q) (q-1)^{i-m_2} q^{i-m_2} \right), \quad (2.4)$$

for  $0 \leq i \leq \min\{p-2, r-1\}$ , where  $R_{n,m_1,m_2}(t) \in \mathbb{Z}[t]$  are defined in Lemma 7.1. The digit  $f_i(q)$  is divisible by  $q-1$  for  $1 \leq i \leq \min\{p-2, r-1\}$ . Additionally, we have

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) a_{md}(1) \equiv 0 \pmod{n^{1+\min\{p-2, r-1\}}}. \quad (2.5)$$



**Remark 2.8.** When  $p < r + 1$ , Theorem 2.4 does not give us  $r$   $[n]_q$ -digits of  $a_{nm}(q)$ , but the proof shows that in any case the polynomial

$$r(q) = \sum_{i=0}^{r-1} f_i(q)[n]_q^i \in \mathbb{Q}[q]$$

satisfies  $r^{(j)}(\omega) = a_{nm}^{(j)}(\omega)$  for all  $\omega \in \mu_n \setminus \{1\}$  and  $0 \leq j \leq r - 1$ .

Assume that the conditions of Theorem 2.4 hold and consider the base- $[n]_q$  expansion

$$a_{nm}(q) \equiv \sum_{i=0}^{\min\{p-2, r-1\}} f_i(q)[n]_q^i \bmod [n]_q^{1+\min\{p-2, r-1\}}. \quad (2.6)$$

We regard (2.6) as a  $q$ -analogue of (2.5). Indeed, (2.5) follows quickly by plugging  $q = 1$  in (2.6), see the proof of Theorem 2.4 in §7.2.

To deduce Corollary 1.4 from Theorem 1.3, we only need the case  $S = \mathbb{P}$ ,  $r = 3$  of Theorem 2.4, which is given by the following corollary. In order to compute  $f_0$ ,  $f_1$  and  $f_2$  using the recursion (2.4), we need the following values of  $R_{n, m_1, m_2}$ :  $R_{n, 0, m_2} = \delta_{m_2, 0}$  (Kronecker delta),  $R_{n, 1, 1} = n$ ,  $R_{n, 1, 2}(t) = n(n-1)(t-1) - 2nt$ .

**Corollary 2.5.** Assume that  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences of order 3. Then for all  $m \geq 1$ ,  $n \geq 2$  with  $(n, 6) = 1$  we have

$$a_{nm}(q) \equiv f_0(q) + f_1(q)[n]_q + f_2(q)[n]_q^2 \bmod [n]_q^3,$$

where  $f_0, f_1, f_2 \in \mathbb{Z}[q]$  are the first three  $[n]_q$ -digits of  $a_{nm}(q)$ , given by

$$\begin{aligned} f_0(q) &= G_{g_0, n}(q), & f_1(q) &= \frac{q-1}{n} (G_{g_1, n}(q) - qG'_{g_0, n}(q)), \\ f_2(q) &= \frac{(q-1)^2}{2n^2} (G_{g_2, n}(q) + G''_{g_0, n}(q)q^2 + (qG'_{g_0, n}(q) - G_{g_1, n}(q))(n-1) + 2q(G'_{g_0, n}(q) - G'_{g_1, n}(q))), \end{aligned}$$

and  $g_0, g_1, g_2: D_n \rightarrow \mathbb{C}$  are given by

$$g_0(d) = a_{md}(1), \quad g_1(d) = a'_{mn}(\omega_n^d)\omega_n^d, \quad g_2(d) = a''_{mn}(\omega_n^d)\omega_n^{2d}.$$

## 2.3 $q$ -supercongruences

Below we use that  $G_{g, p^k}(1) = g(p^{k-1})$  when  $p$  is a prime and  $k \geq 1$ , and in particular  $G_{g, p}(q) = g(1)$ .

**Theorem 2.6.** Let  $a_n(q) = \left[ \frac{an}{bn} \right]_q$ . For all  $n \geq 1$  and  $\omega \in \mu_n$ , we have

$$a_n(\omega) = a_{\frac{n}{\text{ord}(\omega)}}(1), \quad (2.7)$$

$$\omega a'_n(\omega) = \text{ord}(\omega)^2 \left( \frac{\frac{an}{\text{ord}(\omega)}}{\frac{bn}{\text{ord}(\omega)}} \right) \frac{b(a-b)n^2}{2}, \quad (2.8)$$

$$\omega^2 a''_n(\omega) = \left( \frac{\frac{an}{\text{ord}(\omega)}}{\frac{bn}{\text{ord}(\omega)}} \right) b(a-b)n^2 \left( \frac{b(a-b)n^2}{4} + \frac{an \cdot \text{ord}(\omega) - 5}{12} \right), \quad (2.9)$$

In particular,  $a_n(q)$  satisfies the  $q$ -Gauss congruences of order 3. Thus, in the notation of Corollary 2.5, for all  $m \geq 1$ ,  $n \geq 2$  with  $(n, 6) = 1$  we have

$$a_{nm}(q) \equiv f_0(q) + f_1(q)[n]_q + f_2(q)[n]_q^2 \bmod [n]_q^3. \quad (2.10)$$

Specializing (2.10) to  $n = p^k$  ( $p \geq 5$  a prime,  $k \geq 1$ ),  $m = 1$  and  $q = 1$ , we obtain (1.11) (since  $f_0(1) = a_{p^{k-1}}(1)$ ,  $f_1(1) = f_2(1) = 0$ ). Theorem 2.6 is the first result providing a  $q$ -analogue of (1.11) for  $k > 1$ . Previously, various  $q$ -analogues were found only for the case  $k = 1$ . Clark [Cla95] has shown that

$$\left[ \frac{an}{bn} \right]_q \equiv \left[ \frac{a}{b} \right]_{q^{n^2}} \bmod \Phi_n^2(q),$$

where  $\Phi_n(q)$  is the  $n$ -th cyclotomic polynomial, which coincides with  $[n]_q$  for  $n$  a prime. Andrews [And99, Thm. 3] has shown that if  $p$  is an odd prime, then

$$\begin{bmatrix} ap \\ bp \end{bmatrix}_q \equiv q^{(a-b)b\binom{p}{2}} \begin{bmatrix} a \\ b \end{bmatrix}_{q^p} \pmod{[p]_q^2}.$$

Straub [Str11, Thm. 1], building on a work of Shi and Pan [SP07], proved that for any prime  $p \geq 5$ ,

$$\begin{bmatrix} ap \\ bp \end{bmatrix}_q \equiv \begin{bmatrix} a \\ b \end{bmatrix}_{q^{p^2}} - \binom{a}{b} b(a-b) \frac{p^2-1}{24} (q^p-1)^2 \pmod{[p]_q^3}, \quad (2.11)$$

which refines Clark's result for  $n = p$ . Cai and García-Pulgarín [CGP01] obtained some variants of (2.11) when  $a = 2$ ,  $b = 1$ . When  $m = 1$  and  $n = p \geq 5$  is a prime, (2.10) simplifies to

$$\begin{bmatrix} ap \\ bp \end{bmatrix}_q \equiv \binom{a}{b} + \frac{\binom{a}{b} b(a-b)p}{2} (q^p-1) + \frac{\binom{a}{b} b(a-b)}{2} \left( \frac{b(a-b)}{4} p^2 + \frac{ap^2-5}{12} - \frac{p-1}{2} \right) (q^p-1)^2 \pmod{[p]_q^3}. \quad (2.12)$$

Recently, Straub [Str19, Thm. 2.2] extended (2.11) as follows:

$$\begin{bmatrix} am \\ bm \end{bmatrix}_q \equiv \begin{bmatrix} a \\ b \end{bmatrix}_{q^{m^2}} - \binom{a}{b} b(a-b) \frac{m^2-1}{24} (q^m-1)^2 \pmod{\Phi_m(q)^3} \quad (2.13)$$

for all  $m \geq 1$  with  $(m, 6) = 1$ . As  $\Phi_{p^k}(q) = p$  when  $p$  is a prime and  $k \geq 1$ , substituting  $m = p^k$  in (2.13) gives the congruence  $\begin{bmatrix} ap^k \\ bp^k \end{bmatrix} \equiv \binom{a}{b} \pmod{p^3}$ . Although (2.12) does not imply Straub's results, in §8.6 we explain how to derive (2.13) quickly using our methods. Recently Zudilin computed  $\begin{bmatrix} am \\ bm \end{bmatrix}_q$  modulo a fourth power of  $\Phi_m$  [Zud19, Thms. 1,2], but we shall not pursue such higher congruences here.

The following theorem is proved in §8.4.

**Theorem 2.7.** *Let  $a_n(q)$  be the sequence  $g_n(q)$  defined in Theorem 1.3. For any  $P \in \mathbb{C}[x, y]$ , let*

$$a_{n,P} = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{n}^2 P(n, k).$$

*For all  $n \geq 1$  and  $\omega \in \mu_n$ , we have*

$$a_n(\omega) = a_{\frac{n}{\text{ord}(\omega)}}(1), \quad (2.14)$$

$$\omega a'_n(\omega) = \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, 2xy-y^2+f(x,y)}, \quad (2.15)$$

$$\omega^2 a''_n(\omega) = \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, (2xy-y^2+f(x,y))^2 + \frac{x^2y}{3} - \frac{(x-y)^2}{6}} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, \frac{x^2}{6} - 2xy + y^2 - f(x,y)}. \quad (2.16)$$

*In particular,  $a_n(q)$  satisfies the  $q$ -Gauss congruences of order 3. Thus, in the notation of Corollary 2.5, for all  $m \geq 1$ ,  $n \geq 2$  with  $(n, 6) = 1$  we have*

$$a_{nm}(q) \equiv f_0(q) + f_1(q)[n]_q + f_2(q)[n]_q^2 \pmod{[n]_q^3}. \quad (2.17)$$

Specializing (2.17) to  $n = p^k$  ( $p \geq 5$  a prime,  $k \geq 1$ ) and  $q = 1$ , we obtain (1.12) (since  $f_0(1) = a_{p^k-1,m}(1)$ ,  $f_1(1) = f_2(1) = 0$ ). The sequence  $a_n(q)$  was studied by Krattenthaler, Rivoal and Zudilin [KRZ06] and Zheng [Zhe11] in the case  $f(x, y) = (x - y)^2$  and recently by Straub [Str19] for general  $f$ . A different  $q$ -analogue of the Apéry numbers was considered by Adamczewski, Bell, Delaygue and Jouhet [ABDJ17, Prop. 1.5].

Theorem 2.7 is the first result providing a  $q$ -analogue of (1.12) for  $k > 1$ . Straub [Str19, Cor. 1.1] proved that for any  $m \geq 1$  with  $(m, 6) = 1$ , we have

$$a_{nm}(q) \equiv a_n(q^{m^2}) - (q^m - 1)^2 \frac{m^2 - 1}{12} n^2 a_n(1) \pmod{\Phi_m(q)^3}. \quad (2.18)$$

As  $\Phi_{p^k}(q) = p$  when  $p$  is a prime and  $k \geq 1$ , substituting  $m = p^k$  in (2.18) gives the congruence  $a_{np^k}(1) \equiv a_n(1) \pmod{p^3}$ . When  $n = p \geq 5$  is a prime, (2.17) simplifies to

$$a_{mp}(q) \equiv a_m(1) + b_m(q^p - 1) + c_m(q^p - 1)^2 \pmod{[p]_q^3} \quad (2.19)$$

for

$$\begin{aligned} b_m &= pa_{m, 2xy - y^2 + f(x, y)}, \\ c_m &= \frac{1}{2}(p^2 a_{m, (2xy - y^2 + f(x, y))^2 + \frac{x^2 y}{3} - \frac{(x-y)^2}{6}} + a_{m, \frac{x^2}{6} - 2xy + y^2 - f(x, y)} - (p-1)a_{m, 2xy - y^2 + f(x, y)}). \end{aligned}$$

Although (2.19) does not imply (2.18), in §8.6 we explain how to derive (2.18) using our methods.

**Remark 2.9.** *Straub also allowed  $f(x, y)$ , in the definition of  $a_n(q)$ , to assume negative values, by working in the ring  $\mathbb{Z}[q, q^{-1}]$  of Laurent polynomials.*

The following theorem is proved in §8.5.

**Theorem 2.8.** *Let  $a_n(q)$  be the sequence  $h_n(q)$  defined in Theorem 1.3. For any  $P \in \mathbb{C}[x, y, z]$ , let*

$$a_{n,P} = \sum_{k,\ell} \binom{n}{k}^2 \binom{n}{\ell} \binom{k}{\ell} \binom{k+\ell}{n} P(n, k, \ell).$$

For all  $n \geq 1$  and  $\omega \in \mu_n$ , we have

$$a_n(\omega) = a_{\frac{n}{\text{ord}(\omega)}}(1), \quad (2.20)$$

$$\omega a'_n(\omega) = \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, xz - y^2 - z^2 + \frac{3xy + yz - x^2}{2} + f(x, y, z)}, \quad (2.21)$$

$$\omega^2 a''_n(\omega) = \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, Q_1} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, Q_2}, \quad (2.22)$$

where

$$\begin{aligned} Q_1 &= \left( xz - y^2 - z^2 + \frac{3xy + yz - x^2}{2} + f(x, y, z) \right)^2 + \frac{x^2 y - xy^2 + 2xyz + y^2 z - yz^2}{12} \\ &\quad + \frac{-x^2 + xy - y^2 - z^2 + zy + zx}{6}, \\ Q_2 &= \frac{1}{12}(7x^2 - 17xy + 12y^2 - 12xz - 7zy + 12z^2) - f(x, y, z). \end{aligned}$$

In particular,  $a_n(q)$  satisfies the  $q$ -Gauss congruences of order 3. Thus, in the notation of Corollary 2.5, for all  $m \geq 1$ ,  $n \geq 2$  with  $(n, 6) = 1$  we have

$$a_{nm}(q) \equiv f_0(q) + f_1(q)[n]_q + f_2(q)[n]_q^2 \pmod{[n]_q^3}. \quad (2.23)$$

Specializing (2.23) to  $n = p^k$  ( $p \geq 5$  a prime,  $k \geq 1$ ), we obtain the supercongruence (1.13) (since  $f_0(1) = a_{p^{k-1}m}(1)$ ,  $f_1(1) = f_2(1) = 0$ ). When  $n = p \geq 5$  a prime, (2.23) simplifies to

$$a_{mp}(q) \equiv a_m(1) + b_m(q^p - 1) + c_m(q^p - 1)^2 \pmod{[p]_q^3}$$

for

$$\begin{aligned} b_m &= pa_{m, xz - y^2 - z^2 + \frac{3xy + yz - x^2}{2} + f(x, y, z)}, \\ c_m &= \frac{1}{2} \left( p^2 a_{m, Q_1} + a_{m, Q_2} - (p-1)a_{m, xz - y^2 - z^2 + \frac{3xy + yz - x^2}{2} + f(x, y, z)} \right). \end{aligned}$$

In §8.6 we show that for  $m \geq 1$  with  $(m, 6) = 1$ , we also have the more elegant  $q$ -supercongruence

$$a_{nm}(q) \equiv a_n(q^{m^2}) - (q^m - 1)^2 \frac{m^2 - 1}{24} a_{n, x^2 + xy - yz} \pmod{\Phi_m(q)^3}. \quad (2.24)$$

The proofs of Theorems 2.6, 2.7, 2.8 involve differentiating the relevant sequences and evaluating them at roots of unity, by using the values of the derivatives of the  $q$ -binomial coefficients at roots of unity. These values are given in §8.1, and especially in Corollary 8.2, which might be of independent interest.

### 3 Criteria for Gauss congruences

Here we review some classical results on Gauss congruences, mostly for comparison with results we obtain on  $q$ -Gauss congruences.

**Proposition 3.1.** *[Sta99, Ch. 5, Ex. 5.2(a) and its solution] Let  $\{a_n\}_{n \geq 1}$  be a sequence of integers. The following conditions are equivalent.*

1.  $\{a_n\}_{n \geq 1}$  satisfies the Gauss congruences
2. For all  $n, k \geq 1$  and all primes  $p$ :  $a_{p^k n} \equiv a_{p^{k-1}n} \pmod{p^k}$
3.  $\exp(\sum_{n \geq 1} a_n x^n / n) \in \mathbb{Z}[[x]]$

The next proposition generalizes the equivalence between the first two conditions in Proposition 3.1.

**Proposition 3.2.** *[AZ06, Prop. 11] Let  $\{a_n\}_{n \geq 1}$  be a sequence of integers and let  $m$  be a positive integer. The following conditions are equivalent.*

1. For all  $n \geq 1$ :  $\sum_{d|n} \mu(n/d) a_d \equiv 0 \pmod{n^m}$
2. For all  $n, k \geq 1$  and primes  $p$ :  $a_{p^k n} \equiv a_{p^{k-1}n} \pmod{p^{km}}$

The following result is a corollary of the Lagrange inversion theorem.

**Proposition 3.3.** *Let  $f \in \mathbb{Z}[[u]]$  with  $f(0) = 1$ . The sequence  $\{[u^n]f^n(u)\}_{n \geq 1}$  satisfies the Gauss congruences.*

*Proof.* Let  $a_n = [u^n]f^n(u)$ . From [Ges80, Eq. (3.8)], we have

$$\exp\left(\sum_{n \geq 1} a_n x^n / n\right) = \sum_{n \geq 1} ([u^{n-1}]f^n(u)/n) x^{n-1}. \quad (3.1)$$

Since  $(f^n)' = n \cdot f' \cdot f^{n-1}$ , we have

$$[u^{n-1}]f^n(u) = \frac{1}{n-1} [u^{n-2}](f^n)'(u) = \frac{n}{n-1} [u^{n-2}]f'(u)f^{n-1}(u). \quad (3.2)$$

for all  $n \geq 2$ . From (3.2), it follows that  $[u^{n-1}] \frac{f^n(u)}{n} \in \frac{1}{n}\mathbb{Z} \cap \frac{1}{n-1}\mathbb{Z} = \mathbb{Z}$ , and so from (3.1) it follows that  $\exp(\sum_{n \geq 1} a_n x^n / n) \in \mathbb{Z}[[x]]$ . Proposition 3.1 applied to  $\{a_n\}_{n \geq 1}$  concludes the proof of the proposition.  $\square$

**Corollary 3.1.** *The following sequences satisfy the Gauss congruences.*

1. [Zar08]  $a_n = \text{Tr}(A^n)$ , where  $A \in \text{Mat}_m(\mathbb{Z})$ .
2.  $a_n = \binom{an}{n}$  and  $a_n = \binom{an-1}{n}$ , where  $a \geq 2$  is an integer.
3.  $a_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{k} \binom{n-k}{k}$ .

*Proof.* For the first part, note that

$$\exp\left(\sum_{n \geq 1} \frac{\text{Tr}(A^n)x^n}{n}\right) = \exp(\text{Tr}(-\ln(I - Ax))) = \frac{1}{\det(I - Ax)} = \sum_{i \geq 0} \text{TrSym}^i(A)x^i,$$

where  $\text{Sym}^i(A)$  is the  $i$ -th symmetric power of  $A$ . Thus, Proposition 3.1 implies that  $\{\text{Tr}(A^n)\}_{n \geq 1}$  satisfies the Gauss congruences.

For the second part, apply Proposition 3.3 with  $f(x) = (1+x)^a$  and  $f(x) = (1-x)^{-(a-1)}$ . For the third part, apply Proposition 3.3 with  $f(x) = 1+x+x^2$ .  $\square$

We also have a  $p$ -adic version of Proposition 3.1.

**Proposition 3.4.** *Let  $\{a_n\}_{n \geq 1}$  be a sequence of integers. Fix a prime  $p$ , let  $\mathbb{Z}_p$  be the ring of  $p$ -adic integers and  $\mathbb{Q}_p$  be its fraction field. Set  $F(x) = \exp(\sum_{n \geq 1} a_n x^n / n) \in \mathbb{Q}[[x]] \subseteq \mathbb{Q}_p[[x]]$ . The following conditions are equivalent.*

1.  $\{a_n\}_{n \geq 1}$  satisfies the Gauss congruences with respect to  $\{p\}$
2.  $F(x) \in \mathbb{Z}_p[[x]]$
3.  $F(x^p)/F(x)^p \in 1 + px\mathbb{Z}_p[[x]]$

*Proof.* The equivalence of the second and the third conditions is known as the Dieudonné-Dwork criterion, see [Rob00, § VII.2.3]. The equivalence of the first and the second conditions follows from the proof of the equivalence of the second and third conditions in Proposition 3.1. Indeed, following the proof of Proposition 3.1 but working in the ring  $\mathbb{Z}_p$  instead of  $\mathbb{Z}$ , we see that  $F(x) \in \mathbb{Z}_p[[x]]$  holds if and only if

$$a_{r^k n} \equiv a_{r^{k-1} n} \pmod{r^k \mathbb{Z}_p}. \quad (3.3)$$

for all  $n, k \geq 1$  and all primes  $r$ . Since a prime  $r$  is invertible in  $\mathbb{Z}_p$  whenever  $r \neq p$ , condition (3.3) is non-trivial only for  $r = p$ , in which case it becomes

$$a_{p^k n} \equiv a_{p^{k-1} n} \pmod{p^k}$$

for all  $n, k \geq 1$ , as needed.  $\square$

### 3.1 Proof of Lemma 2.1

The first part of the lemma is proved as follows.

$\Rightarrow$ : Assume that  $\{a_n\}_{n \geq 1}$  satisfies the Gauss congruences with respect to  $S$ . Then for any  $p \in S$ , we may choose  $n = p^k$  in (2.1) and obtain (1.2), as needed.

$\Leftarrow$ : Assume that (1.2) holds for all  $p \in S$ . Let  $n \in \mathbb{N}_S$ , and suppose that  $n$  factors as  $n = \prod_{i=1}^r p_i^{e_i}$ . Let  $m \geq 1$ . Fix  $i \in \{1, 2, \dots, r\}$ . Set  $S_n = \{d : d \text{ divides } n, \mu(d) \neq 0\}$  and  $T_n = \{d \in S_n : p_i \nmid d\}$ . We partition  $S_n$  into a disjoint union of pairs:  $S_n = \cup_{d \in T_n} \{d, dp_i\}$ . Then

$$\sum_{d|n} \mu(d) a_{nm/d} = \sum_{d \in S_n} \mu(d) a_{nm/d} = \sum_{d \in T_n} \mu(d) (a_{nm/d} - a_{nm/dp_i}). \quad (3.4)$$

Each summand in the right-hand side of (3.4) is divisible by  $p_i^{e_i}$  by (1.2), which shows that  $\sum_{d|n} \mu(d) a_{nm/d}$  is divisible by  $p_i^{e_i}$ . Since  $i$  was arbitrary,  $\sum_{d|n} \mu(d) a_{nm/d}$  is divisible by  $n$ , as needed.

We continue to the second part of the lemma.

$\Rightarrow$ : Assume that  $\{a_n\}_{n \geq 1}$  satisfies the Gauss congruences with respect to  $\mathbb{P}$ . Choosing  $m = 1$  in (2.1), we see that  $\{a_n\}_{n \geq 1}$  satisfies the Gauss congruences.

$\Leftarrow$ : Assume that  $\{a_n\}_{n \geq 1}$  satisfies the Gauss congruences. By Proposition 3.1, we have that  $a_{p^k n} \equiv a_{p^{k-1} n} \pmod{p^k}$  for all  $n, k \geq 1$  and all primes  $p$ . Let  $m \geq 1$ . Replacing  $n$  with  $nm$ , we see that  $a_{p^k nm} \equiv a_{p^{k-1} nm} \pmod{p^k}$  for all  $n, k \geq 1$  and all primes  $p$ . By another application of Proposition 3.1 it follows that the sequence  $b_n := a_{nm}$  satisfies the Gauss congruences, which gives us (2.1) with fixed  $m$  and for all  $n \geq 1$ . Since  $m$  was arbitrary, it follows that (2.1) holds with  $S = \mathbb{P}$ , as needed.  $\square$

## 4 Criteria for $q$ -Gauss congruences

### 4.1 Auxiliary lemmas

**Lemma 4.1.** [IR90, Ch. 2]

1. The divisor sum  $\sum_{d|n} \mu(d)$  equals 1 if  $n = 1$ , and is 0 otherwise.
2. The Möbius function is multiplicative, that is,  $\mu(n_1 n_2) = \mu(n_1) \mu(n_2)$  whenever  $(n_1, n_2) = 1$ .

**Lemma 4.2.** *Let  $f(q) \in \mathbb{C}[q]$  and  $n \geq 1$ . Assume that as a function of  $\omega \in \mu_n$ ,  $f(\omega)$  depends only on the order of  $\omega$ . Then the remainder of  $f(q)$  upon division by  $[n]_q$  is*

$$G_{g,n}(q)$$

for

$$g: D_n \rightarrow \mathbb{C}, \quad g(d) = f(\omega_n^d).$$

*Proof.* The degree of  $G_{g,n}(q)$  is less than  $\deg[n]_q$ , since if  $d \in D_n$  then  $\deg \frac{[n]_q}{[n/d]_q} = n - \frac{n}{d} < n - 1 = \deg[n]_q$ . Let  $\omega \in \mu_n \setminus \{1\}$ . We have, for any  $d$  dividing  $n$ ,

$$\frac{[n]_q}{[n/d]_q} \Big|_{q=\omega} = \begin{cases} d & \text{if } d \mid \frac{n}{\text{ord}(\omega)}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$G_{g,n}(\omega) = \sum_{d \mid \frac{n}{\text{ord}(\omega)}} \sum_{e \mid d} \mu\left(\frac{d}{e}\right) f(\omega_n^e). \quad (4.1)$$

Changing the order of summation in (4.1), we obtain

$$G_{g,n}(\omega) = \sum_{e \mid \frac{n}{\text{ord}(\omega)}} f(\omega_n^e) \sum_{d: e \mid d \mid \frac{n}{\text{ord}(\omega)}} \mu\left(\frac{d}{e}\right) = \sum_{e \mid \frac{n}{\text{ord}(\omega)}} f(\omega_n^e) \sum_{d': d' \mid \frac{n}{\text{ord}(\omega)e}} \mu(d'),$$

which equals  $f(\omega_n^{\frac{n}{\text{ord}(\omega)}}) = f(\omega)$  by the first part of Lemma 4.1. This implies that  $f(q) - G_{g,n}(q)$  is divisible by  $[n]_q$ , as needed.  $\square$

## 4.2 Proof of Proposition 2.2

The equivalence of the second and the third conditions in Proposition 2.2 follows from a general observation: a polynomial  $F(q) \in \mathbb{C}[q]$  is divisible by  $\Phi_k(q)$  if and only if  $F(\omega) = 0$  for any primitive root of unity  $\omega$  of order  $k$ . We turn to prove the equivalence of the first and the second conditions.

$\Leftarrow$ : Assume that  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies (2.3), that is,

$$a_{nm}(\omega_n^i) = a_{m(n,i)}(1). \quad (4.2)$$

for all  $n \in \mathbb{N}_S$  and  $m, i \geq 1$ . We establish (2.2), which may be stated as follows:

$$\sum_{d \mid n} \mu(d) a_{nm/d}(\omega_n^{id}) = 0. \quad (4.3)$$

for all  $n \in \mathbb{N}_S$  and  $m, i \geq 1$  with  $n \nmid i$ . We simplify (4.3) using (4.2) as follows:

$$\sum_{d \mid n} \mu(d) a_{nm/d}(\omega_n^{id}) = \sum_{d \mid n} \mu(d) a_{\frac{n}{d}m}(\omega_{n/d}^i) = \sum_{d \mid n} \mu(d) a_{(\frac{n}{d}, i)m}(1). \quad (4.4)$$

If  $a_f(1)$  appears in the right-hand side of (4.4), then  $f = f'm$  for some  $f' \mid (n, i)$ . For any  $f' \mid (n, i)$ , the term  $a_{f'm}(1)$  appears in the right-hand side of (4.4) with coefficient

$$\sum_{\substack{d \mid n \\ (\frac{n}{d}, i) = f'}} \mu(d) = \sum_{\substack{d \mid \frac{n}{f'} \\ (\frac{n}{df'}, \frac{i}{f'}) = 1}} \mu(d). \quad (4.5)$$

Let  $g$  be the largest divisor of  $\frac{n}{f'}$  which is divisible only by primes dividing  $\frac{i}{f'}$ . The condition  $(\frac{n}{df'}, \frac{i}{f'}) = 1$  is equivalent to  $g \mid d$ . Also let  $(\frac{\tilde{n}}{gf'})$  denote the largest factor of  $\frac{n}{gf'}$  coprime to  $g$ . Using Lemma 4.1, the sum in the right-hand side of (4.5) is

$$\sum_{d' \mid \frac{n}{gf'}} \mu(gd') = \mu(g) \sum_{d' \mid (\frac{\tilde{n}}{gf'})} \mu(d') = \mu(g) 1_{(\frac{\tilde{n}}{gf'})=1}. \quad (4.6)$$

We now explain why the sum in (4.5) is necessarily 0. Otherwise, by (4.6),  $g$  must be squarefree and every prime factor of  $\frac{n}{gf'}$  must be a factor of  $g$ . In particular, every prime factor of  $\frac{n}{f'}$  divides  $g$ . Combined with the fact  $g$  is squarefree and the definition of  $g$ , it follows that  $g = \frac{n}{f'}$ . Again, by the definition of  $g$ , every prime factor of the squarefree number  $g = \frac{n}{f'}$  divides  $\frac{i}{f'}$ , and thus  $n$  divides  $i$ , a contradiction. Thus, the sum in (4.4) is also 0, as needed.

$\Rightarrow$ : Assume that  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  satisfies the  $q$ -Gauss congruences with respect to  $S$ . We show by induction on  $n \in \mathbb{N}_S$  that (4.3) implies (4.2). For  $n = 1$ , (4.2) is a tautology. We assume that (4.2) holds for all  $n \in \mathbb{N}_S$  smaller than  $k \in \mathbb{N}_S$ , and prove it for  $n = k$ . If  $i$  is divisible by  $k$ , there is nothing to prove. Otherwise, if  $k$  does not divide  $i$ , we have from (4.3) that

$$\sum_{d|k} \mu(d) a_{km/d}(\omega_k^{id}) = 0 \quad (4.7)$$

whenever  $k \nmid i$ . The induction hypothesis tells us that for any  $d \neq 1$  dividing  $k$ ,

$$a_{km/d}(\omega_k^{id}) = a_{km/d}(\omega_{k/d}^i) = a_{m(k/d,i)}(1). \quad (4.8)$$

From (4.7) and (4.8) we obtain

$$a_{km}(\omega_k^i) + \sum_{d|k, d \neq 1} \mu(d) a_{m(k/d,i)}(1) = 0. \quad (4.9)$$

We need to prove that  $a_{km}(\omega_k^i) = a_{m(k,i)}(1)$ , which, using (4.9), becomes the following equivalent condition:

$$\sum_{d|k} \mu(d) a_{m(k/d,i)}(1) = 0,$$

which was established in the other direction of the proof by showing that the coefficient of  $a_{f'm}(1)$  (where  $f' \mid (k, i)$ ) is 0, so we are done.  $\square$

### 4.3 Proof of Lemma 2.2

The first part of the lemma follows immediately by choosing  $n = p^k$  for  $p \in S$  in (2.2). We turn to the proof of the second part of the lemma.

$\Rightarrow$ : Suppose that  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences with respect to  $\mathbb{P}$ . Then by choosing  $m = 1$  in (2.2) we see that  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences, as needed.

$\Leftarrow$ : Suppose that  $\{a_n(q)\}_{n \geq 1}$  satisfies the  $q$ -Gauss congruences. By Proposition 2.2, it suffices to prove that

$$a_n(\omega_n^i) = a_{(n,i)}(1).$$

for all  $n, i \geq 1$ . In other words, we need to deduce (4.3) from (4.2), but with  $m$  fixed and equal to 1 (and  $S = \mathbb{P}$ ). In Proposition 2.2, it is established that (4.2) implies (4.3), and following the proof we see that in fact  $m$  can be fixed during it, so we are done.  $\square$

### 4.4 Proof of Proposition 2.5

According to Proposition 2.2, we may apply Lemma 4.2 with  $f(q) = a_{nm}(q)$ , which establishes the proposition since  $f(\omega_n^e) = a_{nm}(\omega_n^e) = a_{nm/(n/e)}(1) = a_{em}(1)$  if  $e \mid n$ .  $\square$

## 5 Examples

To verify our examples we need two results. The first is a standard result [Sta97, Ch. 3, Ex. 45(b)] (cf. [Sla08]).

**Lemma 5.1.** *Let  $n, k, d$  be non-negative integers. We have*

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\omega_n^d} = \begin{cases} \binom{(n,d)}{(n,d)k/n} & \text{if } n \mid dk, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* Plugging  $q = \omega_n^d$  in (1.5), we obtain

$$(1 - (-t)^{n/(n,d)})^{(n,d)} = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_{\omega_n^d} t^k \omega_n^{d \binom{k}{2}}. \quad (5.1)$$

Comparing the coefficients of  $t^k$  on both sides of (5.1), we conclude the proof of the lemma.  $\square$

We also need the following lemma.

**Lemma 5.2.** *Let  $n \geq 1$  and let  $\omega$  be a primitive root of unity of order  $n$ . Let*

$$A_\omega(t) = \begin{bmatrix} 1 & \omega^{n-1} \\ t & 0 \end{bmatrix} \begin{bmatrix} 1 & \omega^{n-2} \\ t & 0 \end{bmatrix} \cdots \begin{bmatrix} 1 & 1 \\ t & 0 \end{bmatrix} \in \text{Mat}_2(\mathbb{Z}[\omega][t])$$

and

$$A(t) = \begin{bmatrix} 1 & t \\ 1 & 0 \end{bmatrix} \in \text{Mat}_2(\mathbb{Z}[t]).$$

Then  $A_\omega(t)$ ,  $A(t^n)$  have the same characteristic polynomial.

*Proof.* The characteristic polynomial of  $A(t^n)$  is  $X^2 - X - t^n$ , so it suffices to show that

$$\det(A_\omega(t)) = -t^n, \quad \text{Tr}(A_\omega(t)) = 1.$$

By multiplicativity of the determinant, we have

$$\det(A_\omega(t)) = \prod_{i=0}^{n-1} (-\omega^i t) = t^n (-1)^n \omega^{\binom{n}{2}} = -t^n.$$

Let  $P(t) = \text{Tr}(A_\omega(t))$ . We have

$$P(0) = \text{Tr} \left( \begin{bmatrix} 1 & \omega^{n-1} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & \omega^{n-2} \\ 0 & 0 \end{bmatrix} \cdots \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right) = \text{Tr} \left( \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right) = 1. \quad (5.2)$$

Let  $\omega_2 \in \mu_n$ . By conjugating  $A_\omega(\omega_2)$  with  $\text{Diag}(1, \omega_2)$  and using the property  $\text{Tr}(XY) = \text{Tr}(YX)$ , we see that

$$\begin{aligned} P(\omega_2) &= \text{Tr} \left( \begin{bmatrix} 1 & \omega^{n-1}\omega_2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & \omega^{n-2}\omega_2 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} 1 & \omega_2 \\ 1 & 0 \end{bmatrix} \right) \\ &= \text{Tr} \left( \begin{bmatrix} 1 & \omega^{n-1} \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & \omega^{n-2} \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right) = P(1). \end{aligned} \quad (5.3)$$

Plugging  $q = \omega$  in (1.9), we see that  $P(1) = 1$ . From (5.2) and (5.3), the polynomial  $P$  is of degree  $\leq n$  and assumes the value 1  $n + 1$  times. Thus,  $P$  is the constant polynomial 1, as needed.  $\square$

## 5.1 Simple examples

Here we verify that the examples given in §1.2 satisfy the  $q$ -Gauss congruences. We start with  $a_n(q) = \begin{bmatrix} an \\ bn \end{bmatrix}_q$ . By Corollary 2.3, it suffices to show that

$$\begin{bmatrix} an \\ bn \end{bmatrix}_{\omega_n^i} = \begin{pmatrix} a(n, i) \\ b(n, i) \end{pmatrix}. \quad (5.4)$$



By Lemma 5.1, the left-hand side of (5.4) is equal to  $\begin{bmatrix} an \\ bn \end{bmatrix}_{\omega_n^{ai}} = \binom{(an, ai)}{(an, ai)b/a} = \binom{a(n, i)}{b(n, i)}$ , as needed. We now consider  $b_n(q) = \begin{bmatrix} an-1 \\ bn \end{bmatrix}_q$ , for which we have to show that

$$\begin{bmatrix} an-1 \\ bn \end{bmatrix}_{\omega_n^i} = \binom{a(n, i)-1}{b(n, i)}.$$

This equality can be deduced from (5.4) since

$$\begin{bmatrix} am-1 \\ bm \end{bmatrix}_q = \begin{bmatrix} am \\ bm \end{bmatrix}_q \frac{[(a-b)m]_q}{[am]_q}$$

and if  $\omega^m = 1$  then

$$\lim_{q \rightarrow \omega} \frac{[(a-b)m]_q}{[am]_q} = \frac{a-b}{a}.$$

We continue with  $c_n(q) = [t^{bn}] \prod_{i=0}^{n-1} (1 - tq^i)^a$ . By Corollary 2.3, we need to prove that  $c_n(\omega_n^k) = c_{(n,k)}(1)$ , that is,

$$[t^{bn}] \prod_{i=0}^{n-1} (1 - t\omega_n^{ki})^a = [t^{b(n,k)}] (1-t)^{a(n,k)}. \quad (5.5)$$

The left-hand side of (5.5) may be evaluated as follows:

$$\begin{aligned} [t^{bn}] \prod_{i=0}^{n-1} (1 - t\omega_n^{ki})^a &= [t^{bn}] \left( \prod_{i=0}^{\frac{n}{(n,k)}-1} (1 - t\omega_{n/(n,k)}^{ik/(n,k)}) \right)^{a(n,k)} \\ &= [t^{bn}] (1 - t^{n/(n,k)})^{a(n,k)} \\ &= [t^{b(n,k)}] (1-t)^{a(n,k)}, \end{aligned}$$

as needed.

## 5.2 Proof of Theorem 1.1

We prove both parts using Corollary 2.3. We start with  $d_n(q) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} q^{i(i+b)} \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{bmatrix} n-i \\ i \end{bmatrix}_q$ . We need to prove that  $d_n(\omega_n^k) = d_{(n,k)}(1)$ . By Lemma 5.1,

$$\begin{aligned} d_n(\omega_n^k) &= \sum_{\substack{0 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ n \mid ik}} \omega_n^{ki(i+b)} \binom{(n,k)}{(n,k)i/n} \begin{bmatrix} n-i \\ i \end{bmatrix}_{\omega_n^k} \\ &= \sum_{\substack{0 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ \frac{n}{(n,k)} \mid i}} \binom{(n,k)}{(n,k)i/n} \begin{bmatrix} n-i \\ i \end{bmatrix}_{\omega_{n-i}^{k(n-i)/n}} \\ &= \sum_{\substack{0 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ \frac{n}{(n,k)} \mid i}} \binom{(n,k)}{(n,k)i/n} \binom{(n-i, k(n-i)/n)}{(n-i, k(n-i)/n)i/(n-i)}. \end{aligned}$$

Since  $(n-i, k(n-i)/n) = (\frac{n-i}{n/(n,k)}, \frac{n}{(n,k)}, \frac{n-i}{n/(n,k)}, \frac{k}{(n,k)}) = \frac{n-i}{n/(n,k)}$ , we may simplify the last sum as

$$\begin{aligned} d_n(\omega_n^k) &= \sum_{\substack{0 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ \frac{n}{(n,k)} \mid i}} \binom{(n,k)}{(n,k)i/n} \binom{(n,k)(n-i)/n}{(n,k)i/n} \\ &= \sum_{0 \leq i' \leq \lfloor \frac{n}{2} \rfloor / (n/(n,k))} \binom{(n,k)}{i'} \binom{(n,k)-i'}{i'} = d_{(n,k)}(1). \end{aligned}$$

We now prove the theorem for  $e_n(q)$ . Let

$$B_n(q) = A(q^{n-1})A(q^{n-2}) \cdots A(1).$$

Since  $i \mapsto (\omega_n^k)^i = \omega_{n/(n,k)}^{ik/(n,k)}$  has period  $n/(n,k)$ , we have

$$B_n(\omega_n^k) = B_{n/(n,k)}^{(n,k)}(\omega_{n/(n,k)}^{k/(n,k)}). \quad (5.6)$$

If  $(a, b) = 1$ , then Lemma 5.2 with  $t = 1$ ,  $\omega = \omega_a^b$  and  $n = a$  implies that  $B_a(\omega_a^b)$  and  $B_1(1)$  have the same characteristic polynomial, and so

$$\text{Tr}(B_a^j(\omega_a^b)) = \text{Tr}(B_1^j(1)) \quad (5.7)$$

holds for all  $j$  and  $a, b$  with  $(a, b) = 1$ . By Corollary 2.3, we need to prove that  $e_n(\omega_n^k) = e_{(n,k)}(1)$ , that is,

$$\text{Tr}(B_n(\omega_n^k)) = \text{Tr}(B_1^{(n,k)}(1)). \quad (5.8)$$

From (5.7) with  $a = n/(n, k)$ ,  $b = k/(n, k)$  and  $j = (n, k)$ , we obtain that the right-hand side of (5.8) is  $\text{Tr}(B_{n/(n,k)}^{(n,k)}(\omega_{n/(n,k)}^{k/(n,k)}))$ , which in turn equals the left-hand side of (5.8) according to (5.6).  $\square$

## 6 Proof of Theorem 1.2

We begin with the triple  $(B_{n,k}, \mathbb{Z}/n\mathbb{Z}, \left[ \begin{smallmatrix} n; b; q \\ k \end{smallmatrix} \right]_2)$ . The polynomial  $\left[ \begin{smallmatrix} m_1 \\ m_2 \end{smallmatrix} \right]_q$  has non-negative coefficients for all  $m_1 \geq m_2 \geq 0$  (as follows from (1.5), for instance), and so  $\left[ \begin{smallmatrix} n; b; q \\ k \end{smallmatrix} \right] = \sum_{i=0}^{\lfloor \frac{n-k}{2} \rfloor} q^{i(i+b)} \left[ \begin{smallmatrix} n \\ i \end{smallmatrix} \right]_q \left[ \begin{smallmatrix} n-i \\ i+k \end{smallmatrix} \right]_q$  must also have non-negative coefficients. For any  $0 \leq i \leq n$ , the product  $\binom{n}{i} \binom{n-i}{i+k}$  is the number of words in  $B_{n,k}$  with  $i$  2-s and  $i+k$  0-s, and so

$$\left[ \begin{smallmatrix} n; b; 1 \\ k \end{smallmatrix} \right] = \sum_{i \geq 0} \binom{n}{i} \binom{n-i}{i+k} = |B_{n,k}|. \quad (6.1)$$

Given  $g \in \mathbb{Z}/n\mathbb{Z}$ , the set  $B_{n,k}^g$  consists of elements of  $B_{n,k}$  with period  $(g, n)$ , that is, of words of the form

$$w \overbrace{\left[ \begin{smallmatrix} n \\ (g, n) \end{smallmatrix} \right]} = w \mid \underbrace{w \mid w \mid \cdots \mid w}_{n/(g, n)},$$

where  $\mid$  denotes concatenation, and the length of  $w$  is  $(g, n)$ . For  $w \overbrace{\left[ \begin{smallmatrix} n \\ (g, n) \end{smallmatrix} \right]}$  to be in  $B_{n,k}$ , it is necessary and sufficient that  $w \in B_{(g,n), k(g,n)/n}$  (in particular,  $kg \equiv 0 \pmod{n}$ ). Thus,

$$|B_{n,k}^g| = \begin{cases} B_{(g,n), k(g,n)/n} & \text{if } kg \equiv 0 \pmod{n}, \\ 0 & \text{otherwise.} \end{cases} \quad (6.2)$$

To verify that  $(B_{n,k}, \mathbb{Z}/n\mathbb{Z}, \left[ \begin{smallmatrix} n; b; q \\ k \end{smallmatrix} \right])$  exhibits the CSP, we need to prove that for all  $g, g' \in \mathbb{Z}/n\mathbb{Z}$  with  $\gcd(n, g) = \gcd(n, g')$ ,

$$\left[ \begin{smallmatrix} n; b; \omega_n^{g'} \\ k \end{smallmatrix} \right] = |B_{n,k}^g|. \quad (6.3)$$

By (6.1) and (6.2), the right-hand side of (6.3) is  $\left[ \begin{smallmatrix} (g, n); b; 1 \\ k(g, n)/n \end{smallmatrix} \right]$  if  $kg \equiv 0 \pmod{n}$ , and 0 otherwise. Thus, (6.3) is equivalent to

$$\left[ \begin{smallmatrix} n; b; \omega_n^{g'} \\ k \end{smallmatrix} \right] = \begin{cases} \left[ \begin{smallmatrix} (g, n); b; 1 \\ k(g, n)/n \end{smallmatrix} \right] & \text{if } kg \equiv 0 \pmod{n}, \\ 0 & \text{otherwise.} \end{cases}$$

To prove this, we use Lemma 5.1, which implies that

$$\left[ \begin{smallmatrix} n; b; \omega_n^{g'} \\ k \end{smallmatrix} \right] = \sum_{\substack{0 \leq i \leq \lfloor \frac{n-k}{2} \rfloor \\ n/(g', n) \mid i}} \binom{(g', n)}{i/(n/(g', n))} \left[ \begin{smallmatrix} n-i \\ i+k \end{smallmatrix} \right]_{\omega_n^{g'(n-i)/n}}. \quad (6.4)$$

If  $kg \neq 0 \pmod n$ , then  $kg' \neq 0 \pmod n$  also and Lemma 5.1 implies that  $\begin{bmatrix} n-i \\ i+k \end{bmatrix}_{\omega_{n-i}^{g'(n-i)/n}} = 0$  whenever  $n/(g', n) \mid i$  and so  $\begin{bmatrix} n; b; \omega_n^{g'} \\ k \end{bmatrix} = 0$ , as needed. Otherwise, Lemma 5.1 tells us that  $\begin{bmatrix} n-i \\ i+k \end{bmatrix}_{\omega_{n-i}^{g'(n-i)/n}} = \binom{(g', n) - i/(n/(g', n))}{i/(n/(g', n)) + k(g', n)/n}$ , and so the sum in (6.4) is exactly  $\begin{bmatrix} (g', n); b; 1 \\ k(g', n)/n \end{bmatrix} = \begin{bmatrix} (g, n); b; 1 \\ k(g, n)/n \end{bmatrix}$ , as needed.

We turn to the triple  $(C_{n,k}, \mathbb{Z}/n\mathbb{Z}, e_{n,k}(q))$ . The entries of  $A(q^i, t)$  are polynomials in  $q$  and  $t$  with non-negative coefficients, and so  $e_{n,k}(q)$  must also have non-negative coefficients. Set

$$e_n(q, t) = \text{Tr}(A(q^{n-1}, t)A(q^{n-2}, t) \cdots A(1, t)).$$

By definition,  $e_{n,k}(q) = [t^k]e_n(q, t)$ . Let  $S_{n+1,k}$  be the set of words  $w$  of length  $n+1$  on letters  $0, 1$ , with no consecutive 1-s, and with  $k$  indices  $1 \leq i \leq n$  such that  $w_i = 1, w_{i+1} = 0$ . For all  $w \in \cup_{k=0}^n S_{n+1,k}$ , set

$$W_3(w) = \sum_{\substack{1 \leq a \leq n: \\ w_a = 0, w_{a+1} = 1}} (n - a).$$

A direct inductive argument shows that for all  $n \geq 1$  and  $i, j \in \{0, 1\}$ , we have

$$(A(q^{n-1}, t)A(q^{n-2}, t) \cdots A(1, t))_{i,j} = \sum_{k=0}^n t^k \sum_{\substack{w \in S_{n+1,k} \\ w_1 = i, w_{n+1} = j}} q^{W_3(w)}. \quad (6.5)$$

Let  $S'_{n+1,k}$  be the subset of  $S_{n+1,k}$  consisting of words that start and end with the same letter. Then (6.5) implies that

$$e_n(q, t) = \sum_{k=0}^n t^k \sum_{w \in S'_{n+1,k}} q^{W_3(w)}. \quad (6.6)$$

By removing the first letter of each word in  $S'_{n+1,k}$ , we obtain a set of the same size, namely  $C_{n,k}$ . Thus, (6.6) implies that

$$e_{n,k}(q) = \sum_{w \in S'_{n+1,k}} q^{W_3(w)} = \sum_{w \in C_{n,k}} q^{W_1(w)}. \quad (6.7)$$

In particular,

$$e_{n,k}(1) = |C_{n,k}|. \quad (6.8)$$

Given  $g \in \mathbb{Z}/n\mathbb{Z}$ , the set  $C_{n,k}^g$  consists of elements of  $C_{n,k}$  with period  $(g, n)$ , that is, of words of the form

$$w^{\frac{n}{(g,n)}} = \underbrace{w \mid w \mid w \mid \cdots \mid w}_{n/(g,n)},$$

where  $\mid$  denotes concatenation, and the length of  $w$  is  $(g, n)$ . For  $w^{\frac{n}{(g,n)}}$  to be in  $C_{n,k}$ , it is necessary and sufficient that  $kg \equiv 0 \pmod n$  and  $w \in C_{(g,n), k(g,n)/n}$ . Thus,

$$|C_{n,k}^g| = \begin{cases} |C_{(g,n), k(g,n)/n}| & \text{if } kg \equiv 0 \pmod n, \\ 0 & \text{otherwise.} \end{cases} \quad (6.9)$$

To verify that  $(C_{n,k}, \mathbb{Z}/n\mathbb{Z}, e_{n,k}(q))$  exhibits the CSP, we need to prove that for all  $g, g' \in \mathbb{Z}/n\mathbb{Z}$  with  $\gcd(n, g) = \gcd(n, g')$ ,

$$e_{n,k}(\omega_n^{g'}) = |C_{n,k}^g|. \quad (6.10)$$

If we set  $\omega = \omega_n^{g'} = \omega_n^{g'/(g', n)}$ , then

$$A(q^{n-1}, t)A(q^{n-2}, t) \cdots A(1, t) \Big|_{q=\omega} = \left( A(\omega^{\frac{n}{(g', n)}} - 1, t) A(\omega^{\frac{n}{(g', n)}} - 2, t) \cdots A(1, t) \right)^{(g', n)}. \quad (6.11)$$

Setting

$$A_\omega(t) = A(\omega^{\frac{n}{(g',n)}-1}, t) A(\omega^{\frac{n}{(g',n)}-2}, t) \cdots A(1, t),$$

we obtain from (6.11) that

$$e_{n,k}(\omega_n^{g'}) = [t^k] \text{Tr}(A_\omega^{(g',n)}(t)) = [t^k] \text{Tr}(A_\omega^{(g,n)}(t)). \quad (6.12)$$

By Lemma 5.2,  $A_\omega(t)$  and  $A(t^{\frac{n}{(g,n)}}, 1)$  have the same characteristic polynomial. Thus, (6.12) implies that

$$e_{n,k}(\omega_n^{g'}) = [t^k] \text{Tr}(A(t^{\frac{n}{(g,n)}}, 1)^{(g,n)}). \quad (6.13)$$

If  $kg \not\equiv 0 \pmod n$ , then (6.13) and (6.9) show that (6.10) holds in this case. If  $kg \equiv 0 \pmod n$ , then (6.8), (6.9) and (6.13) imply that

$$e_{n,k}(\omega_n^{g'}) = [s^{\frac{k(g,n)}{n}}] \text{Tr}(A(s, 1)^{(g,n)}) = e_{(g,n),k(g,n)/n}(1) = |C_{n,k}^g|,$$

that is, (6.10) again holds, as needed.  $\square$

## 7 Criteria for supercongruences and $q$ -Gauss congruences of order $d$

### 7.1 Auxiliary results

We define the degree of the zero polynomial to be  $-\infty$ .

**Lemma 7.1.** *Let  $n$  be a positive integer and let  $\omega \in \mu_n \setminus \{1\}$ .*

1. *Let  $i \in \mathbb{Z}_{\geq 0}$ . We have*

$$[n]_\omega^{(i)} = \frac{P_{n,i}(\omega)}{(\omega - 1)^i \omega^i} \quad (7.1)$$

for

$$P_{n,i}(t) = i! \sum_{0, i-n \leq j \leq i-1} \binom{n}{i-j} (-t)^j (t-1)^{i-j-1} \in \mathbb{Z}[t].$$

2. *Let  $i, j \in \mathbb{Z}_{\geq 0}$ . We have*

$$([n]_\omega^i)^{(j)} = \frac{R_{n,i,j}(\omega)}{(\omega - 1)^j \omega^j}$$

for

$$R_{n,i,j}(t) = \sum_{a_1 + \dots + a_i = j} \binom{j}{a_1, \dots, a_i} \prod_{1 \leq k \leq i} P_{n,a_k}(t) \in \mathbb{Z}[t].$$

Moreover,  $\deg R_{n,i,j} \leq j - i$  if  $j \geq i$  and  $R_{n,i,j} = 0$  otherwise. Also,  $R_{n,i,i} = i!n^i$ .

*Proof.* To prove the first part of the lemma, recall the general Leibniz rule

$$(f_1 f_2 \cdots f_{m_1})^{(m_2)} = \sum_{k_1 + k_2 + \dots + k_{m_1} = m_2} \binom{m_2}{k_1, k_2, \dots, k_{m_1}} \prod_{1 \leq j \leq m_1} f_j^{(k_j)}.$$

Applying this rule with  $f_1 = q^n - 1$ ,  $f_2 = \frac{1}{q-1}$ ,  $m_1 = 2$  and  $m_2 = i$ , we obtain the following identity of rational functions:

$$\begin{aligned} [n]_q^{(i)} &= ((q^n - 1) \frac{1}{q-1})^{(i)} \\ &= \sum_{j=0}^i \binom{i}{j} (q^n - 1)^{(i-j)} \left(\frac{1}{q-1}\right)^{(j)} \\ &= \sum_{j=0}^{i-1} \binom{i}{j} n(n-1) \cdots (n-(i-j-1)) q^{n-(i-j)} \frac{j!(-1)^j}{(q-1)^{j+1}} + \frac{(q^n - 1)i!(-1)^i}{(q-1)^{i+1}}. \end{aligned} \quad (7.2)$$

Plugging  $q = \omega$  in (7.2), we obtain

$$[n]_\omega^{(i)} = \frac{i!}{(\omega-1)^i \omega^i} \sum_{0, i-n \leq j \leq i-1} \binom{n}{i-j} (-\omega)^j (\omega-1)^{i-j-1},$$

as needed. To prove the second part of the lemma, we again apply the general Leibniz rule and obtain

$$([n]_q^i)^{(j)} = \sum_{a_1 + \dots + a_i = j} \binom{j}{a_1, \dots, a_i} \prod_{1 \leq k \leq i} [n]_q^{(a_k)}. \quad (7.3)$$

Using the first part of the lemma, (7.3) may be written as follows when we substitute  $q = \omega$ :

$$\begin{aligned} ([n]_\omega^i)^{(j)} &= \sum_{a_1 + \dots + a_i = j} \binom{j}{a_1, \dots, a_i} \prod_{1 \leq k \leq i} \frac{P_{n, a_k}(\omega)}{(\omega-1)^{a_k} \omega^{a_k}} \\ &= \frac{\sum_{a_1 + \dots + a_i = j} \binom{j}{a_1, \dots, a_i} \prod_{1 \leq k \leq i} P_{n, a_k}(\omega)}{(\omega-1)^j \omega^j} = \frac{R_{n, i, j}(\omega)}{(\omega-1)^j \omega^j}, \end{aligned}$$

as needed. We now bound the degree of  $R_{n, i, j}(t)$ . By definition,  $\deg P_{n, i} \leq i-1$  if  $i \geq 1$  and  $P_{n, 0} = 0$ , and so

$$\deg R_{n, i, j} \leq \max_{a_1 + \dots + a_i = j} \sum_{k=1}^i \deg P_{n, a_k} \leq \max_{a_1 + \dots + a_i = j} \sum_{k=1}^i (a_k - 1) = j - i,$$

which in particular shows that  $R_{n, i, j} = 0$  if  $j < i$ . Finally, we compute  $R_{n, i, i}$ . We have just established that  $R_{n, i, i}$  is a constant polynomial, and in particular  $R_{n, i, i} = R_{n, i, i}(\omega_n)$ . From the values  $P_{n, 1}(\omega_n) = n$  and  $P_{n, 0}(\omega_n) = 0$ , and from the fact that  $a_1 + \dots + a_i = i$  implies that either  $a_k = 1$  for all  $1 \leq k \leq i$  or  $a_k = 0$  for some  $k$ , it follows that

$$\begin{aligned} R_{n, i, i} &= R_{n, i, i}(\omega_n) = \sum_{a_1 + \dots + a_i = i} \binom{i}{a_1, \dots, a_i} \prod_{1 \leq k \leq i} P_{n, a_k}(\omega_n) \\ &= \underbrace{\binom{i}{1, \dots, 1}}_i P_{n, 1}(\omega_n)^i + \sum_{a_1 + \dots + a_i = i, a_k = 0 \text{ for some } k} \binom{i}{a_1, \dots, a_i} \prod_{1 \leq k \leq i} P_{n, a_k}(\omega_n) \\ &= i! n^i, \end{aligned}$$

as needed.  $\square$

**Proposition 7.1.** *Let  $f(q) \in \mathbb{C}[q]$ ,  $n \geq 2$  and  $r \geq 1$ . Assume that for any  $0 \leq i \leq r-1$ , the function  $g_i: \mu_n \rightarrow \mathbb{C}$ ,  $\omega \mapsto \omega^i f^{(i)}(\omega)$  depends only on the order of  $\omega$ . Then the following hold.*

1. For  $0 \leq i \leq r-1$ , define  $f_i(q)$  recursively by

$$f_i(q) = \frac{1}{i! n^i} \left( (q-1)^i G_{h_i, n}(q) - \sum_{m_1=0}^{i-1} \sum_{m_2=m_1}^i \binom{i}{m_2} f_{m_1}^{(i-m_2)}(q) R_{n, m_1, m_2}(q) (q-1)^{i-m_2} q^{i-m_2} \right), \quad (7.4)$$

where

$$h_i: D_n \rightarrow \mathbb{C}, \quad h_i(d) = (\omega_n^d)^i f^{(i)}(\omega_n^d)$$

and  $R_{n, m_1, m_2}(t) \in \mathbb{Z}[t]$  are defined in Lemma 7.1. Then for

$$r(q) = \sum_{i=0}^{r-1} f_i(q) [n]_q^i \quad (7.5)$$

we have

$$f^{(i)}(\omega) = r^{(i)}(\omega) \quad (7.6)$$

for all  $0 \leq i \leq r-1$  and  $\omega \in \mu_n \setminus \{1\}$ .

2. Let  $p$  be the smallest prime divisor of  $n$ . For all  $0 \leq i \leq r-1$  we have

$$\deg f_i \leq n - p + i. \quad (7.7)$$

3. For all  $0 \leq i \leq \min\{p-2, r-1\}$ , the  $i$ -th  $[n]_q$ -digit of  $f$  is  $f_i$ .

4. For all  $1 \leq i \leq r-1$ ,  $f_i(q)$  is a multiple of  $q-1$ .

*Proof.* We prove (7.6), (7.7) by induction on  $i$ . For  $i=0$ , this is an application of Lemma 4.2. Suppose now that (7.6), (7.7) hold for all  $i \leq k-1$ . To prove that (7.6) holds for  $k$  in place of  $i$  (assuming that  $k \leq r-1$ ), we note that the induction hypothesis implies that

$$f(q) - \sum_{i=0}^{k-1} f_i(q)[n]_q^i = f(q) - r(q) + [n]_q^k \left( \sum_{i=k}^r f_i(q)[n]_q^{i-k} \right)$$

is divisible by  $[n]_q^k$ . By  $k$  successive applications of L'Hôpital's rule and by Lemma 7.1, we have for all  $\omega \in \mu_n \setminus \{1\}$

$$\begin{aligned} \lim_{q \rightarrow \omega} \frac{f(q) - \sum_{i=0}^{k-1} f_i(q)[n]_q^i}{[n]_q^k} &= \lim_{q \rightarrow \omega} \frac{f^{(k)}(q) - \sum_{i=0}^{k-1} (f_i(q)[n]_q^i)^{(k)}}{([n]_q^k)^{(k)}} \\ &= \frac{f^{(k)}(\omega) - \sum_{i=0}^{k-1} \sum_{j=0}^k \binom{k}{j} f_i^{(k-j)}(\omega) R_{n,i,j}(\omega) (\omega-1)^{-j} \omega^{-j}}{k! n^k / (\omega^k (\omega-1)^k)} \\ &= \frac{1}{k! n^k} \left( (\omega-1)^k \omega^k f^{(k)}(\omega) - \sum_{i=0}^{k-1} \sum_{j=i}^k \binom{k}{j} f_i^{(k-j)}(\omega) R_{n,i,j}(\omega) (\omega-1)^{k-j} \omega^{k-j} \right). \end{aligned} \quad (7.8)$$

By Lemma 4.2,  $\omega^k f^{(k)}(\omega) = G_{h_k, n}(\omega)$  for all  $\omega \in \mu_n \setminus \{1\}$ , which together with (7.8) shows that

$$\lim_{q \rightarrow \omega} \frac{f(q) - \sum_{i=0}^{k-1} f_i(q)[n]_q^i}{[n]_q^k} = f_k(\omega).$$

This shows that  $(f(q) - \sum_{i=0}^k f_i(q)[n]_q^i)/([n]_q^k)$  vanishes on the roots of  $[n]_q$ , and so  $f(q) - \sum_{i=0}^k f_i(q)[n]_q^i$  is divisible by  $[n]_q^{k+1}$ , thus implying that (7.5) holds for  $k$  in place of  $i$ .

To prove that (7.7) holds for  $k$  in place of  $i$ , note that  $\deg f_k(q) \leq \max\{S_1, S_2\}$  where

$$S_1 = \deg((q-1)^k G_{h_k, n}(q)) \leq k + \max_{d \in D_n} \deg \frac{[n]_q}{[n/d]_q} = n - p + k$$

and

$$\begin{aligned} S_2 &= \deg \sum_{i=0}^{k-1} \sum_{j=i}^k \binom{k}{j} f_i^{(k-j)}(q) R_{n,i,j}(q) (q-1)^{k-j} q^{k-j} \\ &\leq \max_{0 \leq i \leq k-1, i \leq j \leq k} (\deg f_i^{(k-j)} + \deg R_{n,i,j} + 2(k-j)) \\ &\leq \max_{0 \leq i \leq k-1, i \leq j \leq k} (\deg(f_i) - (k-j) + j - i + 2(k-j)) \\ &\leq \max_{0 \leq i \leq k-1, i \leq j \leq k} (n - p + i + (k-i)) = n - p + k, \end{aligned}$$

by Lemma 7.1 and our inductive assumption on  $\deg f_i$ . Thus  $\deg f_k(q) \leq n - p + k$ , as needed.

Let  $\tilde{f}(q) = \sum_{i=0}^{\min\{p-2, r-1\}} f_i(q)[n]_q^i$ . By (7.7),  $\deg \tilde{f} < \deg [n]_q^{\min\{p-2, r-1\}+1}$ . By (7.5),  $\tilde{f}(q) - f(q)$  is divisible by  $[n]_q^{\min\{p-2, r-1\}+1}$ . Thus,  $\tilde{f}(q)$  is the remainder of  $f(q)$  upon division by  $[n]_q^{\min\{p-2, r-1\}+1}$ , which proves that  $f_i$  is the  $i$ -th  $[n]_q$ -digit of  $f(q)$  for  $0 \leq i \leq \min\{p-2, r-1\}$ .

We turn to prove, by induction on  $i$ , that the  $f_i$ -s are divisible by  $q-1$  when  $1 \leq i \leq r-1$ . For  $i=1$ , as  $R_{n,0,1} = 0$ , (7.4) shows that  $f_1$  is a multiple of  $(q-1)^1$  by construction. We now assume that  $f_i$  is divisible

by  $q-1$  for all  $1 \leq i \leq c$  for some  $1 \leq c < r-1$ , and show that  $f_{c+1}$  is also divisible by  $q+1$ . For  $i = c+1$ , all the summands in (7.4) are multiples of  $q-1$ , except possibly the summands corresponding to  $(m_1, m_2)$  with  $m_2 = c+1$ , which look like  $f_{m_1}(q)R_{n, m_1, c+1}(q)$ . Note that we may assume that  $m_1 \geq 1$  since  $R_{n, 0, c+1} = 0$ . Since  $1 \leq m_1 < i$ , we can use the induction hypothesis to deduce that these summands are also divisible by  $q-1$ , and so  $f_{c+1}$  is divisible by  $q-1$ , as needed.  $\square$

## 7.2 Proof of Theorem 2.4

Formula (2.4) follows from applying Proposition 7.1 with  $f(q) = a_{nm}(q)$ , which also tells us that the  $f_i$ -s are divisible by  $q-1$  for  $1 \leq i \leq \min\{p-2, r-1\}$ . After substituting  $q = 1$  in

$$a_{nm}(q) \equiv \sum_{i=0}^{\min\{p-2, r-1\}} (q-1) \frac{f_i(q)}{q-1} [n]_q^i \bmod [n]_q^{1+\min\{p-2, r-1\}}$$

we obtain

$$\begin{aligned} a_{nm}(1) &\equiv f_0(1) = G_{g_0}(1) = \sum_{d \in D_n} \sum_{e|d} \mu\left(\frac{d}{e}\right) a_{me}(1) \\ &= \sum_{e|n} a_{me}(1) \sum_{d: e|d|n, d \neq n} \mu\left(\frac{d}{e}\right) \bmod n^{1+\min\{p-2, r-1\}}. \end{aligned} \quad (7.9)$$

By Lemma 4.1, the inner sum in (7.9) is  $1_{e=n} - \mu\left(\frac{n}{e}\right)$ , and so (7.9) becomes (2.5), as needed.  $\square$

## 8 Examples (II)

### 8.1 Derivatives of $q$ -binomial coefficients at roots of unity

**Lemma 8.1.** *[RSW04, Prop. 4.2] Let  $n, k$  be non-negative integers. Let  $\omega \in \mu_n$ . We have*

$$\left[ \begin{matrix} n+k \\ k \end{matrix} \right]_{\omega} = \left( \frac{n}{\text{ord}(\omega)} + \left\lfloor \frac{k}{\text{ord}(\omega)} \right\rfloor \right).$$

In the following propositions we use the convention that  $\binom{a}{-1} = 0$  for any integer  $a$ .

**Proposition 8.1.** *Let  $n, k$  be integers with  $n \geq k \geq 0$ . Let  $i \in \mathbb{Z}$  and set  $d = (n, i)$ . If  $n \nmid dk$ , we have*

$$\omega_n^i \left[ \begin{matrix} n \\ k \end{matrix} \right]_{\omega_n^i}' = \binom{n}{2} \binom{d-1}{\frac{kd}{n}-1} - \binom{k}{2} \binom{d}{\frac{kd}{n}}.$$

If  $n \nmid dk$ , we have

$$\omega_n^{i\binom{k}{2}+i} \left[ \begin{matrix} n \\ k \end{matrix} \right]_{\omega_n^i}' = \frac{n}{\omega_n^{ik}-1} (-1)^{k+\lfloor (k-1)d/n \rfloor + 1} \binom{d-1}{\lfloor (k-1)d/n \rfloor}.$$

*Proof.* We start by differentiating (1.5) with respect to  $q$ :

$$\prod_{j=0}^{n-1} (1+tq^j) \cdot \sum_{j=0}^{n-1} \frac{j q^{j-1} t}{1+tq^j} = \sum_{r=0}^n q^{\binom{r}{2}-1} t^r \left( \binom{r}{2} \left[ \begin{matrix} n \\ r \end{matrix} \right]_q + q \left[ \begin{matrix} n \\ r \end{matrix} \right]_q' \right). \quad (8.1)$$

We plug  $q = \omega_n^i$  in (8.1) and obtain

$$\prod_{j=0}^{n-1} (1+t\omega_n^{ij}) \cdot \sum_{j=0}^{n-1} \frac{j \omega_n^{i(j-1)} t}{1+t\omega_n^{ij}} = \sum_{r=0}^n \omega_n^{i\binom{r}{2}-1} t^r \left( \binom{r}{2} \left[ \begin{matrix} n \\ r \end{matrix} \right]_{\omega_n^i} + \omega_n^i \left[ \begin{matrix} n \\ r \end{matrix} \right]_{\omega_n^i}' \right). \quad (8.2)$$

We can simplify the left-hand side of (8.2) by using  $\prod_{j=0}^{n-1} (1 + t\omega_n^{ij}) = (1 - (-t)^{n/d})^d$ , and the right-hand side by using Lemma 5.1. We obtain

$$(1 - (-t)^{n/d})^d \cdot \sum_{j=0}^{n-1} \frac{j\omega_n^{i(j-1)}t}{1 + t\omega_n^{ij}} = \sum_{r=0}^n \omega_n^{i\binom{r}{2}-1} t^r \left( 1_{n|dr} \cdot \binom{r}{2} \binom{d}{dr/n} + \omega_n^i \left[ r \right]_{\omega_n^i}' \right). \quad (8.3)$$

Writing  $\frac{1}{1+t\omega_n^{ij}}$  as  $\sum_{m \geq 0} t^m (-\omega_n^{ij})^m$ , we compare the coefficients of  $t^k$  on both sides of (8.3) and multiply the result by  $\omega_n^i$ :

$$\sum_{0 \leq s \leq (k-1)d/n} \binom{d}{s} (-1)^{\binom{n}{d}+1}s \sum_{j=0}^{n-1} (-j)(-\omega_n^{ij})^{k-\frac{n}{d}s} = \omega_n^{i\binom{k}{2}} \left( 1_{n|dk} \cdot \binom{k}{2} \binom{d}{dk/n} + \omega_n^i \left[ k \right]_{\omega_n^i}' \right). \quad (8.4)$$

We can simplify the left-hand side of (8.4) by noting that  $\omega_n^{ij\frac{n}{d}} = 1$ , which leads to

$$(-1)^{k+1} \sum_{0 \leq s \leq (k-1)d/n} \binom{d}{s} (-1)^s \sum_{j=0}^{n-1} j\omega_n^{ikj} = \omega_n^{i\binom{k}{2}} \left( 1_{n|dk} \cdot \binom{k}{2} \binom{d}{dk/n} + \omega_n^i \left[ k \right]_{\omega_n^i}' \right). \quad (8.5)$$

The formal identity  $\sum_{j=0}^{n-1} jx^j = x(\sum_{j=0}^{n-1} x^j)' = x(\frac{1-x^n}{1-x})' = x \frac{(n-1)x^n - nx^{n-1} + 1}{(1-x)^2}$  shows that

$$\sum_{j=0}^{n-1} j(\omega_n^m)^j = \begin{cases} \binom{n}{2} & \text{if } n \mid m, \\ \frac{n}{\omega_n^m - 1} & \text{otherwise.} \end{cases} \quad (8.6)$$

Applying (8.6) with  $m = ik$ , we simplify (8.5) as follows. If  $n \mid dk$ , we have

$$\binom{n}{2} (-1)^{k+1} \sum_{0 \leq s \leq (k-1)d/n} \binom{d}{s} (-1)^s = \omega_n^{i\binom{k}{2}} \left( \binom{k}{2} \binom{d}{dk/n} + \omega_n^i \left[ k \right]_{\omega_n^i}' \right). \quad (8.7)$$

Otherwise, we have

$$\frac{n}{\omega_n^{ik} - 1} (-1)^{k+1} \sum_{0 \leq s \leq (k-1)d/n} \binom{d}{s} (-1)^s = \omega_n^{i\binom{k}{2}+i} \left[ n \right]_{\omega_n^i}' . \quad (8.8)$$

The identity

$$\sum_{s=0}^r \binom{d}{s} (-1)^s = (-1)^r \binom{d-1}{r}, \quad (8.9)$$

which may be proved comparing coefficients in  $\frac{(1-x)^d}{1-x} = (1-x)^{d-1}$ , together with the observation that  $\omega_n^{i\binom{k}{2}} = (-1)^{k+\frac{kd}{n}}$  when  $n \mid dk$ , allow us to simplify (8.7), (8.8) and to obtain the result of the proposition.  $\square$

**Proposition 8.2.** *Let  $n, k$  be integers with  $n \geq k \geq 0$ . Let  $i \in \mathbb{Z}$  and set  $d = (n, i)$ . If  $n \mid dk$ , we have*

$$\begin{aligned} \omega_n^{2i} \left[ n \right]_{\omega_n^i}'' &= \left( n \frac{(3d^2 + 1)n^2 - 6d^2n + 2d^2}{12d} - 2 \binom{n}{3} \right) \left( n \binom{d-2}{\frac{kd}{n}-2} - k \binom{d-1}{\frac{kd}{n}-1} \right) \\ &\quad - \binom{n}{2} \left( n \binom{d-2}{\frac{kd}{n}-2} - (k-1) \binom{d-1}{\frac{kd}{n}-1} \right) + \binom{n}{2}^2 \binom{d-1}{\frac{kd}{n}-1} \\ &\quad - \left( \binom{k}{2} - 1 \right) \binom{k}{2} \binom{d}{\frac{kd}{n}} - k(k-1) \left( \binom{n}{2} \binom{d-1}{\frac{kd}{n}-1} - \binom{k}{2} \binom{d}{\frac{kd}{n}} \right). \end{aligned} \quad (8.10)$$

**Remark 8.3.** *Although the expression in the right-hand side of (8.10) can be simplified (see Corollary 8.2), as currently written it constitutes a proof that  $\omega_n^{2i} \left[ n \right]_{\omega_n^i}'' \in \mathbb{Z}$  when  $n \mid ik$ .*



*Proof.* We start by differentiating (1.5) twice with respect to  $q$ , which is the same as differentiating (8.1) once with respect to  $q$ , and the result is

$$\begin{aligned} \prod_{j=0}^{n-1} (1 + tq^j) \cdot \left( \sum_{j=0}^{n-1} \frac{jq^{j-2}t(j-1-q^jt)}{(1+tq^j)^2} + \left( \sum_{j=0}^{n-1} \frac{jq^{j-1}t}{1+tq^j} \right)^2 \right) \\ = \sum_{r=0}^n q^{\binom{r}{2}-2} t^r \left( \left( \binom{r}{2} - 1 \right) \binom{r}{2} \begin{bmatrix} n \\ r \end{bmatrix}_q + qr(r-1) \begin{bmatrix} n \\ r \end{bmatrix}_q' + q^2 \begin{bmatrix} n \\ r \end{bmatrix}_q'' \right). \end{aligned} \quad (8.11)$$

We plug  $q = \omega_n^i$  in (8.11) and obtain

$$\begin{aligned} (1 - (-t)^{n/d})^d \cdot \left( \sum_{j=0}^{n-1} \frac{j\omega_n^{i(j-2)}t(j-1-\omega_n^{ij}t)}{(1+t\omega_n^{ij})^2} + \left( \sum_{j=0}^{n-1} \frac{j\omega_n^{i(j-1)}t}{1+t\omega_n^{ij}} \right)^2 \right) \\ = \sum_{r=0}^n \omega_n^{i(\binom{r}{2}-2)} t^r \left( \left( \binom{r}{2} - 1 \right) \binom{r}{2} \begin{bmatrix} n \\ r \end{bmatrix}_{\omega_n^i} + \omega_n^i r(r-1) \begin{bmatrix} n \\ r \end{bmatrix}_{\omega_n^i}' + \omega_n^{2i} \begin{bmatrix} n \\ r \end{bmatrix}_{\omega_n^i}'' \right). \end{aligned} \quad (8.12)$$

Let

$$S_1(t, q) = \sum_{j=0}^{n-1} \frac{jq^{j-2}t(j-1)}{(1+tq^j)^2}, \quad S_2(t, q) = - \sum_{j=0}^{n-1} \frac{jq^{2j-2}t^2}{(1+tq^j)^2}, \quad S_3(t, q) = \left( \sum_{j=0}^{n-1} \frac{jq^{j-1}t}{1+tq^j} \right)^2.$$

Comparing the coefficient of  $t^k$  in (8.12), multiplying the result by  $\omega_n^{2i}$  and using Lemma 5.1 and Proposition 8.1 to simplify it, we obtain

$$\begin{aligned} \omega_n^{2i} \sum_{0 \leq s \leq \frac{dk}{n}-1} \binom{d}{s} (-1)^{(\frac{n}{d}+1)s} [t^{k-\frac{n}{d}s}] (S_1(t, \omega_n^i) + S_2(t, \omega_n^i) + S_3(t, \omega_n^i)) \\ = (-1)^{k+\frac{kd}{n}} \left( \left( \binom{k}{2} - 1 \right) \binom{k}{2} \binom{d}{\frac{kd}{n}} + k(k-1) \left( \binom{n}{2} \binom{d-1}{\frac{kd}{n}-1} - \binom{k}{2} \binom{d}{\frac{kd}{n}} \right) + \omega_n^{2i} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega_n^i}'' \right). \end{aligned} \quad (8.13)$$

We now compute the coefficient of  $t^r$  in  $S_i(t, \omega_n^i)$ , assuming that  $\frac{n}{d} \mid r$ ,  $r \geq 1$ . We begin with  $S_1(t, q)$ . Since  $\frac{1}{(1+t)^2} = \sum_{r \geq 0} (r+1)(-t)^r$  in  $\mathbb{C}[[t]]$ , we have

$$\begin{aligned} S_1(t, q) &= -\frac{1}{q^2} \sum_{j=0}^{n-1} j(j-1) \sum_{r \geq 1} r(-tq^j)^r \\ &= -\frac{1}{q^2} \sum_{r \geq 1} r(-t)^r \sum_{j=0}^{n-1} j(j-1)q^{jr} \implies \\ \omega_n^{2i} [t^r] S_1(t, \omega_n^i) &= -r(-1)^r \sum_{j=0}^{n-1} j(j-1) = -2 \binom{n}{3} r(-1)^r. \end{aligned} \quad (8.14)$$

We proceed with  $S_2(t, q)$ :

$$\begin{aligned} S_2(t, q) &= -\frac{1}{q^2} \sum_{j=0}^{n-1} j \sum_{r \geq 1} (r-1)(-tq^j)^r \\ &= -\frac{1}{q^2} \sum_{r \geq 1} (r-1)(-t)^r \sum_{j=0}^{n-1} jq^{jr} \implies \\ \omega_n^{2i} [t^r] S_2(t, \omega_n^i) &= -(r-1)(-1)^r \sum_{j=0}^{n-1} j = -\binom{n}{2} (r-1)(-1)^r. \end{aligned} \quad (8.15)$$

We now treat  $S_3(t, q)$ .

$$\begin{aligned}
S_3(t, q) &= \left( \sum_{j=0}^{n-1} j q^{j-1} t \sum_{m \geq 0} (-t q^j)^m \right)^2 \\
&= \frac{1}{q^2} \sum_{r \geq 2} (-t)^r \sum_{\substack{r_1+r_2=r \\ r_i \geq 1}} \sum_{0 \leq j_1, j_2 \leq n-1} j_1 j_2 q^{j_1 r_1 + j_2 r_2} \implies \\
\omega_n^{2i}[t^r] S_3(t, \omega_n^i) &= (-1)^r \sum_{0 \leq j_1, j_2 \leq n-1} j_1 j_2 \sum_{r_1=1}^{r-1} \omega_n^{i r_1 (j_1 - j_2)} = (-1)^r \sum_{0 \leq j_1, j_2 \leq n-1} j_1 j_2 (-1 + r \cdot 1_{j_1 \equiv j_2 \pmod{\frac{n}{d}}}) \\
&= (-1)^r \left( -\binom{n}{2}^2 + r \sum_{0 \leq j_1, j_2 \leq n-1, j_1 \equiv j_2 \pmod{\frac{n}{d}}} 1 \right).
\end{aligned} \tag{8.16}$$

Since

$$\begin{aligned}
\sum_{0 \leq j_1, j_2 \leq n-1, j_1 \equiv j_2 \pmod{\frac{n}{d}}} 1 &= \sum_{m=0}^{\frac{n}{d}-1} \left( \sum_{0 \leq j \leq n-1, j \equiv m \pmod{\frac{n}{d}}} 1 \right)^2 = \sum_{m=0}^{\frac{n}{d}-1} \left( \sum_{s=0}^{d-1} \left( m + \frac{n}{d} s \right) \right)^2 \\
&= \sum_{m=0}^{\frac{n}{d}-1} \left( dm + \frac{n}{d} \binom{d}{2} \right)^2 = n \frac{(3d^2 + 1)n^2 - 6d^2 n + 2d^2}{12d},
\end{aligned}$$

we obtain from (8.16) that

$$\omega_n^{2i}[t^r] S_3(t, \omega_n^i) = (-1)^r \left( -\binom{n}{2}^2 + r n \frac{(3d^2 + 1)n^2 - 6d^2 n + 2d^2}{12d} \right). \tag{8.17}$$

Using (8.14), (8.15) and (8.17), the left-hand side of (8.13) becomes

$$\begin{aligned}
&(-1)^k \left( n \frac{(3d^2 + 1)n^2 - 6d^2 n + 2d^2}{12d} - 2 \binom{n}{3} \right) \sum_{0 \leq s \leq \frac{kd}{n}-1} \binom{d}{s} (-1)^s \left( k - \frac{n}{d} s \right) \\
&- (-1)^k \binom{n}{2} \sum_{0 \leq s \leq \frac{kd}{n}-1} \binom{d}{s} \left( k - \frac{n}{d} s - 1 \right) (-1)^s \\
&- (-1)^k \binom{n}{2}^2 \sum_{0 \leq s \leq \frac{kd}{n}-1} \binom{d}{s} (-1)^s.
\end{aligned} \tag{8.18}$$

Using (8.9) and its variant

$$\sum_{s=0}^r (-1)^s \binom{d}{s} s = -d \sum_{s=1}^r (-1)^{s-1} \binom{d-1}{s-1} = d(-1)^r \binom{d-2}{r-1},$$

we can simplify (8.18) as

$$\begin{aligned}
&(-1)^{k+\frac{kd}{n}} \left( \left( n \frac{(3d^2 + 1)n^2 - 6d^2 n + 2d^2}{12d} - 2 \binom{n}{3} \right) \left( n \binom{\frac{d-2}{n}}{\frac{kd}{n}-2} - k \binom{\frac{d-1}{n}}{\frac{kd}{n}-1} \right) \right. \\
&\quad \left. - \binom{n}{2} \left( n \binom{\frac{d-2}{n}}{\frac{kd}{n}-2} - (k-1) \binom{\frac{d-1}{n}}{\frac{kd}{n}-1} \right) + \binom{n}{2}^2 \binom{\frac{d-1}{n}}{\frac{kd}{n}-1} \right).
\end{aligned} \tag{8.19}$$

Replacing the left-hand side of (8.13) with (8.19), dividing by  $(-1)^{k+\frac{kd}{n}}$  and isolating the term  $\omega_n^{2i} [k]_{\omega_n^i}^{[n]}$ , we conclude the proof.  $\square$

We can simplify the expressions in Propositions 8.1 and 8.2 using the relations  $\binom{d-1}{\frac{kd}{n}-1} = \binom{d}{\frac{kd}{n}} \frac{k}{n}$  for  $\frac{kd}{n} \geq 1$  and  $\binom{d-2}{\frac{kd}{n}-2} = \binom{d-1}{\frac{kd}{n}-1} \frac{\frac{kd}{n}-1}{d-1}$  for  $\frac{kd}{n} \geq 2$ , and obtain the following corollary from Lemma 5.1 and these propositions.

**Corollary 8.2.** *Fix  $n \geq k \geq 0$ . For every  $0 \leq j \leq 2$ , the function  $\omega^j \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_{\omega}^{(j)}$ , as a function of  $\omega \in \mu_{\gcd(n,k)}$ , depends only on the order of  $\omega$  and assumes integer values. In fact, for any primitive root of unity  $\omega \in \mu_{\gcd(n,k)}$  of order  $d$ , we have*

$$\begin{aligned} \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_{\omega} &= \binom{n/d}{k/d}, \\ \omega \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_{\omega}' &= \binom{n/d}{k/d} \frac{k(n-k)}{2}, \\ \omega^2 \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_{\omega}'' &= \binom{n/d}{k/d} k(n-k) \left( \frac{k(n-k)}{4} + \frac{nd-5}{12} \right). \end{aligned}$$

If  $\omega \in \mu_n \setminus \mu_k$  is a primitive root of unity of order  $d$ , we have

$$\begin{aligned} \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_{\omega} &= 0, \\ \omega^{\binom{k}{2}+1} \left[ \begin{smallmatrix} n \\ k \end{smallmatrix} \right]_{\omega}' &= \frac{n}{\omega^k - 1} (-1)^{k+\lfloor (k-1)/d \rfloor + 1} \binom{\frac{n}{d}-1}{\lfloor (k-1)/d \rfloor}. \end{aligned}$$

## 8.2 Sums of roots of unity

The following lemma was essentially proved by Shi and Pan [SP07]. We provide a different proof.

**Lemma 8.3.** *Let  $n \geq 1$ . Let  $\omega$  be a primitive root of unity of order  $n$ . Then*

$$\begin{aligned} \sum_{i=1}^{n-1} \frac{1}{\omega^i - 1} &= -\frac{n-1}{2}, \\ \sum_{i=1}^{n-1} \frac{1}{(\omega^i - 1)^2} &= -\frac{(n-1)(n-5)}{12}. \end{aligned}$$

*Proof.* Substituting  $q+1$  in place of  $q$  in  $\prod_{i=1}^{n-1} (q - \omega^i) = \frac{q^n - 1}{q - 1}$ , we obtain

$$\prod_{i=1}^{n-1} (q+1 - \omega^i) = \frac{(q+1)^n - 1}{q} = q^{n-1} + \dots + \binom{n}{3} q^2 + \binom{n}{2} q + n. \quad (8.20)$$

By equating coefficients in (8.20), we see that

$$\begin{aligned} \sigma_{n-1} &:= \prod_{i=1}^{n-1} (\omega^i - 1) = n(-1)^{n-1}, \\ \sigma_{n-2} &:= \sum_{i=1}^{n-1} \prod_{1 \leq j \leq n-1, j \neq i} (\omega^j - 1) = \binom{n}{2} (-1)^{n-2}, \\ \sigma_{n-3} &:= \sum_{1 \leq i < j \leq n-1} \prod_{1 \leq k \leq n-1, k \neq i, j} (\omega^k - 1) = \binom{n}{3} (-1)^{n-3}. \end{aligned}$$

Thus,

$$\sum_{i=1}^{n-1} \frac{1}{\omega^i - 1} = \frac{\sigma_{n-2}}{\sigma_{n-1}} = -\frac{n-1}{2}$$

and

$$\sum_{i=1}^{n-1} \frac{1}{(\omega^i - 1)^2} = \left( \frac{\sigma_{n-2}}{\sigma_{n-1}} \right)^2 - 2 \frac{\sigma_{n-3}}{\sigma_{n-1}} = \left( -\frac{n-1}{2} \right)^2 - 2 \frac{\binom{n}{3}}{n} = -\frac{(n-1)(n-5)}{12},$$

as needed.  $\square$

### 8.3 Proof of Theorem 2.6

Let  $a \geq b \geq 1$  and define  $a_n(q) = \left[ \frac{an}{bn} \right]_q$ . Corollary 8.2 implies that (2.7)–(2.9) hold for any  $n \geq 1$  and  $\omega \in \mu_n$ .  $\square$

### 8.4 Proof of Theorem 2.7

We show that (2.14) holds by using Lemma 5.1, which tells us in particular that  $\left[ \frac{n}{k} \right]_\omega$  vanishes for  $\omega \in \mu_n \setminus \mu_k$ . For any  $\omega \in \mu_n$ ,

$$\begin{aligned} a_n(\omega) &= \sum_{k=0}^n \left[ \frac{n}{k} \right]_\omega^2 \left[ \frac{n+k}{k} \right]_\omega^2 \omega^{f(n,k)} \\ &= \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{n/\text{ord}(\omega)}{k/\text{ord}(\omega)} \right)^2 \left[ \frac{n+k}{k} \right]_\omega^2 \omega^{f(n,k)} \\ &= \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{n/\text{ord}(\omega)}{k/\text{ord}(\omega)} \right)^2 \left( \frac{(n+k)/\text{ord}(\omega)}{k/\text{ord}(\omega)} \right)^2 = a_{n/\text{ord}(\omega)}(1). \end{aligned}$$

We show that (2.15) holds. The derivative of  $a_n(q)$ , times  $q$ , is given by

$$qa'_n(q) = \sum_{k,\ell} \left[ \frac{n}{k} \right]_q \left[ \frac{n+k}{k} \right]_q q^{f(n,k)} \left( 2q \left[ \frac{n}{k} \right]_q' \left[ \frac{n+k}{k} \right]_q + 2q \left[ \frac{n}{q} \right]_q \left[ \frac{n+k}{k} \right]_q' + f(n,k) \left[ \frac{n}{k} \right]_q \left[ \frac{n+k}{k} \right]_q \right),$$

and Corollary 8.2 allows us to evaluate it at  $q = \omega \in \mu_n$ :

$$\begin{aligned} \omega a'_n(\omega) &= \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) \\ &\quad \cdot \left( 2\omega \left[ \frac{n}{k} \right]_\omega' \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) + 2\omega \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) \left[ \frac{n+k}{k} \right]_\omega' + f(n,k) \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) \right) \\ &= \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 (k(n-k) + kn + f(n,k)) \\ &= \text{ord}(\omega)^2 \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( 2 \frac{k}{\text{ord}(\omega)} \frac{n}{\text{ord}(\omega)} - \left( \frac{k}{\text{ord}(\omega)} \right)^2 \right. \\ &\quad \left. + f\left( \frac{n}{\text{ord}(\omega)}, \frac{k}{\text{ord}(\omega)} \right) \right) = \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}}(2xy - y^2 + f(x,y)). \end{aligned}$$

We show that (2.16) holds. The second derivative of  $a_n(q)$ , times  $q^2$ , is given by

$$q^2 a''_n(q) = S_{n,1}(q) + S_{n,2}(q),$$

where

$$\begin{aligned}
S_{n,1}(q) = & \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q q^{f(n,k)} \left( 2 \begin{bmatrix} n \\ k \end{bmatrix}_q'' \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2 q^2 + 8 \begin{bmatrix} n \\ k \end{bmatrix}_q' \begin{bmatrix} n+k \\ k \end{bmatrix}_q \begin{bmatrix} n+k \\ k \end{bmatrix}_q' q^2 + 4f(n,k) \begin{bmatrix} n \\ k \end{bmatrix}_q' \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2 q \right. \\
& + 2 \begin{bmatrix} n \\ k \end{bmatrix}_q \left( \begin{bmatrix} n+k \\ k \end{bmatrix}_q' \right)^2 q^2 + 2 \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n+k \\ k \end{bmatrix}_q \begin{bmatrix} n+k \\ k \end{bmatrix}_q'' q^2 + 4f(n,k) \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n+k \\ k \end{bmatrix}_q \begin{bmatrix} n+k \\ k \end{bmatrix}_q' q \\
& \left. + f(n,k)(f(n,k) - 1) \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2 \right)
\end{aligned}$$

and

$$S_{n,2}(q) = 2 \sum_{k=0}^n q^2 \left( \begin{bmatrix} n \\ k \end{bmatrix}_q' \right)^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_q^2 q^{f(n,k)}. \quad (8.21)$$

Since  $\begin{bmatrix} n \\ k \end{bmatrix}_q$  vanishes on  $\mu_n \setminus \mu_k$ , Corollary 8.2 allows us to evaluate  $S_{n,1}(q)$  at  $q = \omega \in \mu_n$  similarly to the evaluation of  $a'_n(\omega)$  and  $a_n(\omega)$ :

$$\begin{aligned}
S_{n,1}(\omega) = & \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( 2k(n-k) \left( \frac{k(n-k)}{4} + \frac{n \cdot \text{ord}(\omega) - 5}{12} \right) + 8 \frac{k(n-k)}{2} \frac{kn}{2} \right. \\
& + 4f(n,k) \frac{k(n-k)}{2} + 2 \left( \frac{kn}{2} \right)^2 + 2kn \left( \frac{kn}{4} + \frac{(n+k) \cdot \text{ord}(\omega) - 5}{12} \right) \\
& \left. + 4f(n,k) \frac{kn}{2} + f(n,k)(f(n,k) - 1) \right) \\
= & \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n+k}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 (3.5n^2k^2 + 0.5k^4 - 3nk^3 - \frac{5}{6}k(2n-k) + 2f(n,k)k(2n-k) \\
& + f(n,k)(f(n,k) - 1) + \frac{n^2k}{3} \text{ord}(\omega)) \\
= & \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, 3.5x^2y^2 + 0.5y^4 - 3xy^3 + \frac{x^2y}{3} + 2f(x,y)y(2x-y) + f(x,y)^2} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, -\frac{5}{6}y(2x-y) - f(x,y)}. \quad (8.22)
\end{aligned}$$

We turn to evaluate  $S_{n,2}(q)$  at  $q = \omega \in \mu_n$ . We separate  $S_{n,2}(q)$  into two sums – one with the summands corresponding to  $k$  divisible by  $\text{ord}(\omega)$ , and another with the rest:

$$S_{n,2}(q) = T_1(q) + T_2(q),$$

where

$$\begin{aligned}
T_1(q) = & 2 \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} q^2 \left( \begin{bmatrix} n \\ k \end{bmatrix}_q' \right)^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_\omega^2 q^{f(n,k)}, \\
T_2(q) = & 2 \sum_{0 \leq k \leq n, \text{ord}(\omega) \nmid k} q^2 \left( \begin{bmatrix} n \\ k \end{bmatrix}_q' \right)^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_\omega^2 q^{f(n,k)}.
\end{aligned}$$

We use Lemma 8.1 and Corollary 8.2 to evaluate  $T_1(\omega)$ :

$$\begin{aligned}
T_1(\omega) = & 2 \sum_{0 \leq k \leq n, \text{ord}(\omega) | k} \left( \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right) \frac{k(n-k)}{2} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} + \frac{k}{\text{ord}(\omega)} \right)^2 \\
= & \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, \frac{y^2(x-y)^2}{2}}. \quad (8.23)
\end{aligned}$$

We turn to  $T_2(\omega)$ . By Lemma 8.1 and Corollary 8.2, we may evaluate  $T_2(\omega)$  as follows:

$$T_2(\omega) = 2 \sum_{0 \leq k \leq n, \text{ord}(\omega) \nmid k} \left( \omega^{-\binom{k}{2}} \frac{n}{\omega^k - 1} \left( \frac{\frac{n}{\text{ord}(\omega)} - 1}{\lfloor \frac{k-1}{\text{ord}(\omega)} \rfloor} \right) \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)} + \lfloor \frac{k}{\text{ord}(\omega)} \rfloor}{\lfloor \frac{k}{\text{ord}(\omega)} \rfloor} \right)^2 \omega^{f(n,k)}. \quad (8.24)$$

We write every  $0 \leq k \leq n$  with  $\text{ord}(\omega) \nmid k$  as  $k = \text{ord}(\omega)j + i$  with  $1 \leq i \leq \text{ord}(\omega) - 1$  and  $0 \leq j \leq \frac{n}{\text{ord}(\omega)} - 1$ . Now we have  $\omega^k = \omega^i$ ,  $\omega^{f(n,k)} = \omega^{k^2} = \omega^{i^2}$ ,  $\lfloor \frac{k}{\text{ord}(\omega)} \rfloor = \lfloor \frac{k-1}{\text{ord}(\omega)} \rfloor = j$ . We express (8.24) as

$$\begin{aligned} T_2(\omega) &= 2n^2 \sum_{i=1}^{\text{ord}(\omega)-1} \sum_{j=0}^{\frac{n}{\text{ord}(\omega)}-1} \frac{\omega^{-i^2+i}}{(\omega^i - 1)^2} \left( \frac{\frac{n}{\text{ord}(\omega)} - 1}{j} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)} + j}{j} \right)^2 \omega^{i^2} \\ &= 2 \left( \sum_{i=1}^{\text{ord}(\omega)-1} \frac{\omega^i}{(\omega^i - 1)^2} \right) \left( \sum_{j=0}^{\frac{n}{\text{ord}(\omega)}-1} \left( \frac{\frac{n}{\text{ord}(\omega)}}{j} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)} + j}{j} \right)^2 (n - j\text{ord}(\omega))^2 \right). \end{aligned} \quad (8.25)$$

The sum  $\sum_{i=1}^{\text{ord}(\omega)-1} \frac{\omega^i}{(\omega^i - 1)^2}$  is evaluated in Lemma 8.3. From (8.23)–(8.25) and Lemma 8.3, we obtain

$$S_{n,2}(\omega) = \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, \frac{y^2(x-y)^2}{2} - \frac{(x-y)^2}{6}} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, \frac{(x-y)^2}{6}}. \quad (8.26)$$

From (8.22) and (8.26), we obtain (2.16), as needed.  $\square$

## 8.5 Proof of Theorem 2.8

We show that (2.20) holds by using Lemma 5.1, which tells us in particular that  $\left[ \frac{n}{m} \right]_\omega$  vanishes for  $\omega \in \mu_n \setminus \mu_m$ . For any  $\omega \in \mu_n$ ,

$$\begin{aligned} a_n(\omega) &= \sum_{k,\ell} \left[ \frac{n}{k} \right]_\omega^2 \left[ \frac{n}{\ell} \right]_\omega \left[ \frac{k}{\ell} \right]_\omega \left[ \frac{k+\ell}{n} \right]_\omega \omega^{f(n,k,\ell)} \\ &= \sum_{\text{ord}(\omega) \mid k,\ell} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k+\ell}{\text{ord}(\omega)}}{\frac{n}{\text{ord}(\omega)}} \right) \omega^{f(n,k,\ell)} = a_{n/\text{ord}(\omega)}(1). \end{aligned}$$

We show that (2.21) holds. The derivative of  $a_n(q)$ , times  $q$ , is given by

$$\begin{aligned} qa'_n(q) &= \sum_{k,\ell} \left[ \frac{n}{k} \right]_q q^{f(n,k,\ell)} \left( \left[ \frac{n}{k} \right]_q \left( \left[ \frac{n}{\ell} \right]_q \left[ \frac{k}{\ell} \right]_q \left[ \frac{k+\ell}{n} \right]_q \right)' \right. \\ &\quad \left. + \left( \left[ \frac{n}{k} \right]_q f(n,k,\ell) + 2 \left[ \frac{n}{k} \right]_q' q \left[ \frac{n}{\ell} \right]_q \left[ \frac{k}{\ell} \right]_q \left[ \frac{k+\ell}{n} \right]_q \right). \end{aligned} \quad (8.27)$$

After substituting  $q = \omega \in \mu_n$  in (8.27), we claim that only the terms with  $\text{ord}(\omega) \mid k, \ell$  contribute. Indeed, since each summand contains  $\left[ \frac{n}{k} \right]_q$ , it follows by Lemma 5.1 that each summand vanishes on  $\omega$  if  $\text{ord}(\omega) \nmid k$ . Similarly, since each summand contains either  $\left[ \frac{n}{\ell} \right]_q$  or  $\left[ \frac{k}{\ell} \right]_q$ , Lemma 5.1 again implies that each summand vanishes on  $\omega$  if  $\text{ord}(\omega) \nmid \ell$ . Thus, Corollary 8.2 allows us to evaluate (8.27) at  $q = \omega \in \mu_n$  as follows:

$$\begin{aligned} \omega a'_n(\omega) &= \sum_{\text{ord}(\omega) \mid k,\ell} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k+\ell}{\text{ord}(\omega)}}{\frac{n}{\text{ord}(\omega)}} \right) \left( \frac{\ell(n-\ell) + \ell(k-\ell) + n(k+\ell-n)}{2} \right. \\ &\quad \left. + f(n,k,\ell) + k(n-k) \right) = \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, xz - y^2 - z^2 + \frac{3xy + yz - x^2}{2} + f(x,y,z)}. \end{aligned}$$

Thus, (2.21) holds. We show that (2.22) holds. The second derivative of  $a_n(q)$ , times  $q^2$ , is given by

$$q^2 a''_n(q) = S_{n,1}(q) + S_{n,2}(q) + S_{n,3}(q),$$

where

$$\begin{aligned}
S_{n,1}(q) &= \sum_{k,\ell} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{f(n,k,\ell)} \\
&\quad \cdot \left( \left( \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q \right) \left( 2q^2 \begin{bmatrix} n \\ k \end{bmatrix}_q'' + \begin{bmatrix} n \\ k \end{bmatrix}_q f(n,k,\ell)(f(n,k,\ell)-1) + 4q \begin{bmatrix} n \\ k \end{bmatrix}_q' f(n,k,\ell) \right) \right. \\
&\quad + \begin{bmatrix} n \\ k \end{bmatrix}_q q^2 \left( \begin{bmatrix} n \\ \ell \end{bmatrix}_q'' \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q + \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q'' \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q + \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q'' \right. \\
&\quad + 2 \begin{bmatrix} n \\ \ell \end{bmatrix}_q' \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q' + 2 \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q' \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q' \left. \right) \\
&\quad + \left( 2 \begin{bmatrix} n \\ k \end{bmatrix}_q' f(n,k,\ell)q + 4 \begin{bmatrix} n \\ k \end{bmatrix}_q' q^2 \right) \left( \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q \right)' \Big), \\
S_{n,2}(q) &= 2 \sum_{k,\ell} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^{f(n,k,\ell)} q^2 \begin{bmatrix} n \\ \ell \end{bmatrix}_q' \begin{bmatrix} k \\ \ell \end{bmatrix}_q' \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q, \quad S_{n,3}(q) = 2 \sum_{k,\ell} \left( q \begin{bmatrix} n \\ k \end{bmatrix}_q' \right)^2 q^{f(n,k,\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q.
\end{aligned}$$

Let

$$\begin{aligned}
P_1(x, y, z) &= \frac{1}{4} (x^4 - 6x^3y + 11x^2y^2 - 8xy^3 + 2y^4 - 4x^3z + 10x^2yz - 2xy^2z - 4y^3z + 8x^2z^2 \\
&\quad - 10xyz^2 + 9y^2z^2 - 6xz^3 - 2yz^3 + 2z^4) + f \cdot (-x^2 + 3xy - 2y^2 + 2xz + yz - 2z^2) \\
&\quad + f^2 + \frac{x^2y - xy^2 + 2xyz + y^2z - yz^2}{12}
\end{aligned}$$

and

$$P_2(x, y, z) = \frac{5}{12} (x^2 - 3xy + 2y^2 - 2xz - yz + 2z^2) - f.$$

Corollary 8.2 allows us to evaluate  $S_{n,1}(q)$  at  $q = \omega \in \mu_n$  similarly to the evaluation of  $a'_n(\omega)$  and  $a_n(\omega)$ :

$$\begin{aligned}
S_{n,1}(\omega) &= \sum_{k,\ell \mid \text{ord}(\omega)} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k+\ell}{\text{ord}(\omega)}}{\frac{n}{\text{ord}(\omega)}} \right) \left( k(n-k) \left( \frac{k(n-k)}{2} + \frac{n \cdot \text{ord}(\omega) - 5}{6} \right) \right. \\
&\quad + f(n,k,\ell)(f(n,k,\ell)-1) + 2k(n-k)f(n,k,\ell) + \ell(n-\ell) \left( \frac{\ell(n-\ell)}{4} + \frac{n \cdot \text{ord}(\omega) - 5}{12} \right) \\
&\quad + \ell(k-\ell) \left( \frac{\ell(k-\ell)}{4} + \frac{k \cdot \text{ord}(\omega) - 5}{12} \right) + n(k+\ell-n) \left( \frac{n(k+\ell-n)}{4} + \frac{(k+\ell) \cdot \text{ord}(\omega) - 5}{12} \right) \\
&\quad + \frac{\ell(n-\ell)n(k+\ell-n) + \ell(k-\ell)n(k+\ell-n)}{2} \\
&\quad \left. + (f(n,k,\ell) + k(n-k))(\ell(n-\ell) + \ell(k-\ell) + n(k+\ell-n)) \right) \\
&= \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, P_1} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, P_2}.
\end{aligned} \tag{8.28}$$

We turn to evaluate  $S_{n,2}(q)$  at  $q = \omega \in \mu_n$ . We separate  $S_{n,2}(q)$  into two sums – one with the summands corresponding to  $\ell$  divisible by  $\text{ord}(\omega)$ , and another with the rest:

$$S_{n,2}(q) = T_1(q) + T_2(q),$$

where

$$\begin{aligned}
T_1(q) &= 2 \sum_{k,\ell, \text{ord}(\omega) \mid \ell} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^{f(n,k,\ell)} q^2 \begin{bmatrix} n \\ \ell \end{bmatrix}_q' \begin{bmatrix} k \\ \ell \end{bmatrix}_q' \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q, \\
T_2(q) &= 2 \sum_{k,\ell, \text{ord}(\omega) \nmid \ell} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^{f(n,k,\ell)} q^2 \begin{bmatrix} n \\ \ell \end{bmatrix}_q' \begin{bmatrix} k \\ \ell \end{bmatrix}_q' \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q.
\end{aligned}$$

We use Lemma 8.1 and Corollary 8.2 to evaluate  $T_1(\omega)$ , a sum that is supported on  $k$ -s and  $\ell$ -s divisible by  $\text{ord}(\omega)$ :

$$\begin{aligned} T_1(\omega) &= 2 \sum_{\text{ord}(\omega) | k, \ell} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k+\ell}{\text{ord}(\omega)}}{\frac{n}{\text{ord}(\omega)}} \right) \frac{\ell(n-\ell)}{2} \frac{\ell(k-\ell)}{2} \\ &= \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, \frac{1}{2}(z^2(x-z)(y-z))}. \end{aligned} \quad (8.29)$$

We turn to  $T_2(\omega)$ . By Lemma 8.1 and Corollary 8.2, we may evaluate  $T_2(\omega)$  as follows:

$$T_2(\omega) = 2 \sum_{\text{ord}(\omega) | k, \text{ord}(\omega) \nmid \ell} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \frac{\omega^{f(n,k,\ell)-\ell^2+\ell}}{(\omega^\ell - 1)^2} n k \binom{\frac{n}{\text{ord}(\omega)} - 1}{\lfloor \frac{\ell-1}{\text{ord}(\omega)} \rfloor} \binom{\frac{k}{\text{ord}(\omega)} - 1}{\lfloor \frac{\ell-1}{\text{ord}(\omega)} \rfloor} \binom{\frac{k}{\text{ord}(\omega)} + \lfloor \frac{\ell}{\text{ord}(\omega)} \rfloor}{\frac{n}{\text{ord}(\omega)}}. \quad (8.30)$$

We write every  $0 \leq \ell \leq n$  with  $\text{ord}(\omega) \nmid \ell$  as  $\ell = \text{ord}(\omega)j + i$  with  $1 \leq i \leq \text{ord}(\omega) - 1$  and  $0 \leq j \leq \frac{n}{\text{ord}(\omega)} - 1$ . Now we have, for  $\omega \in \mu_n$  and  $\text{ord}(\omega) \mid k$ , the equalities  $\omega^\ell = \omega^i$ ,  $\omega^{f(n,k,\ell)} = \omega^{\ell^2} = \omega^{i^2}$ ,  $\lfloor \frac{\ell}{\text{ord}(\omega)} \rfloor = \lfloor \frac{\ell-1}{\text{ord}(\omega)} \rfloor = j$ . Letting  $k' = \frac{k}{\text{ord}(\omega)}$ , we express (8.30) as

$$T_2(\omega) = 2 \text{ord}(\omega) n \sum_{k'=0}^{\frac{n}{\text{ord}(\omega)}} \sum_{j=0}^{\frac{n}{\text{ord}(\omega)}-1} \left( \frac{\frac{n}{\text{ord}(\omega)}}{k'} \right)^2 k' \binom{\frac{n}{\text{ord}(\omega)} - 1}{j} \binom{k' - 1}{j} \binom{k' + j}{\frac{n}{\text{ord}(\omega)}} \sum_{i=1}^{\frac{n}{\text{ord}(\omega)}-1} \frac{\omega^i}{(\omega^i - 1)^2}. \quad (8.31)$$

The relation  $\binom{a-1}{b} = \binom{a}{b} \frac{a-b}{a}$  and Lemma 8.3 allow us to simplify (8.31) as

$$T_2(\omega) = -\frac{\text{ord}(\omega)^2}{6} (\text{ord}(\omega)^2 - 1) a_{\frac{n}{\text{ord}(\omega)}, (x-z)(y-z)}. \quad (8.32)$$

From (8.29) and (8.32), we obtain

$$S_{n,2}(\omega) = \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, (\frac{z^2}{2} - \frac{1}{6})(x-z)(y-z)} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, \frac{(x-z)(y-z)}{6}}. \quad (8.33)$$

We turn to evaluate  $S_{n,3}(q)$  at  $q = \omega \in \mu_n$ . We separate  $S_{n,3}(q)$  into two sums – one with the summands corresponding to  $k$  divisible by  $\text{ord}(\omega)$ , and another with the rest:

$$S_{n,3}(q) = U_1(q) + U_2(q),$$

where

$$\begin{aligned} U_1(q) &= 2 \sum_{k, \ell, \text{ord}(\omega) | k} (q \begin{bmatrix} n \\ k \end{bmatrix}_q)^2 q^{f(n,k,\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q, \\ U_2(q) &= 2 \sum_{k, \ell, \text{ord}(\omega) \nmid k} (q \begin{bmatrix} n \\ k \end{bmatrix}_q)^2 q^{f(n,k,\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q. \end{aligned}$$

We use Lemma 8.1 and Corollary 8.2 to evaluate  $U_1(\omega)$ , a sum that is supported on  $k$ -s and  $\ell$ -s divisible by  $\text{ord}(\omega)$ :

$$\begin{aligned} U_1(\omega) &= 2 \sum_{\text{ord}(\omega) | k, \ell} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{k}{\text{ord}(\omega)}} \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \left( \frac{\frac{k+\ell}{\text{ord}(\omega)}}{\frac{n}{\text{ord}(\omega)}} \right) \left( \frac{k(n-k)}{2} \right)^2 \\ &= \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, \frac{1}{2}(y^2(x-y)^2)}. \end{aligned} \quad (8.34)$$

We turn to  $U_2(\omega)$ . By Lemma 8.1 and Corollary 8.2, we may evaluate  $U_2(\omega)$  as follows:

$$U_2(\omega) = 2 \sum_{\text{ord}(\omega) \nmid \ell, \text{ord}(\omega) \nmid k} \left( n \frac{\omega^{-\binom{k}{2}}}{\omega^k - 1} \binom{\frac{n}{\text{ord}(\omega)} - 1}{\lfloor \frac{k-1}{\text{ord}(\omega)} \rfloor} \right)^2 \omega^{f(n,k,\ell)} \left( \frac{\frac{n}{\text{ord}(\omega)}}{\frac{\ell}{\text{ord}(\omega)}} \right) \binom{\frac{k}{\text{ord}(\omega)}}{\lfloor \frac{k}{\text{ord}(\omega)} \rfloor} \binom{\frac{k}{\text{ord}(\omega)}}{\lfloor \frac{k}{\text{ord}(\omega)} \rfloor + \frac{\ell}{\text{ord}(\omega)}}. \quad (8.35)$$



We write every  $0 \leq k \leq n$  with  $\text{ord}(\omega) \nmid k$  as  $k = \text{ord}(\omega)j + i$  with  $1 \leq i \leq \text{ord}(\omega) - 1$  and  $0 \leq j \leq \frac{n}{\text{ord}(\omega)} - 1$ . Now we have, for  $\omega \in \mu_n$  and  $\text{ord}(\omega) \mid \ell$ , the equalities  $\omega^k = \omega^i$ ,  $\omega^{f(n,k,\ell)} = \omega^{k^2} = \omega^{i^2}$ ,  $\lfloor \frac{k}{\text{ord}(\omega)} \rfloor = \lfloor \frac{k-1}{\text{ord}(\omega)} \rfloor = j$ . Letting  $\ell' = \frac{\ell}{\text{ord}(\omega)}$ , we express (8.35) as

$$U_2(\omega) = 2n^2 \sum_{\ell'=0}^{\frac{n}{\text{ord}(\omega)}} \sum_{j=0}^{\frac{n}{\text{ord}(\omega)}-1} \left( \frac{\frac{n}{\text{ord}(\omega)}}{j} - 1 \right)^2 \left( \frac{\frac{n}{\text{ord}(\omega)}}{\ell'} \right) \binom{j}{\ell'} \binom{j+\ell'}{\frac{n}{\text{ord}(\omega)}} \sum_{i=1}^{\frac{n}{\text{ord}(\omega)}-1} \frac{\omega^i}{(\omega^i - 1)^2}. \quad (8.36)$$

The relation  $\binom{a-1}{b} = \binom{a}{b} \frac{a-b}{a}$  and Lemma 8.3 allow us to simplify (8.36) as

$$U_2(\omega) = -\frac{\text{ord}(\omega)^2}{6} (\text{ord}(\omega)^2 - 1) a_{\frac{n}{\text{ord}(\omega)}, (x-y)^2}. \quad (8.37)$$

From (8.34) and (8.37), we obtain

$$S_{n,3}(\omega) = \text{ord}(\omega)^4 a_{\frac{n}{\text{ord}(\omega)}, \frac{1}{2}y^2(x-y)^2 - \frac{(x-y)^2}{6}} + \text{ord}(\omega)^2 a_{\frac{n}{\text{ord}(\omega)}, \frac{1}{6}(x-y)^2}. \quad (8.38)$$

From (8.28), (8.33) and (8.38), we obtain (2.22), as needed.  $\square$

## 8.6 Alternative form

In Theorems 2.6–2.8 we have calculated the first three  $[n]_q$ -digits of several sequences, which allowed us to obtain supercongruences modulo  $n^3$ . For  $n = p$  a prime we describe below an alternative way to deduce the supercongruences, which seems more elegant, although it is not as general as Corollary 2.5.

**Proposition 8.4.** *Let  $\{a_n(q)\}_{n \geq 1} \subseteq \mathbb{Z}[q]$  be a sequence satisfying the  $q$ -Gauss congruences. Suppose that for any  $n \geq 1$  and  $\omega \in \mu_n$ , we have*

$$\omega a'_n(\omega) = \text{ord}(\omega)^2 a'_{\frac{n}{\text{ord}(\omega)}}(1). \quad (8.39)$$

Moreover, suppose that there are sequences  $b_n, c_n$  such that for any  $n \geq 1$  and  $\omega \in \mu_n$ , we have

$$\omega^2 a''_n(\omega) = \text{ord}(\omega)^4 b_{\frac{n}{\text{ord}(\omega)}} + \text{ord}(\omega)^2 c_{\frac{n}{\text{ord}(\omega)}}. \quad (8.40)$$

Then for any  $m, n \geq 1$  with  $(m, 6) = 1$  we have

$$a_{nm}(q) - a_n(q^{m^2}) \equiv -(q^m - 1)^2 \frac{m^2 - 1}{2} (c_n + a'_n(1)) \pmod{\Phi_m(q)^3}. \quad (8.41)$$

In particular for  $m = p \geq 5$  a prime we have

$$a_{np}(1) \equiv a_n(1) \pmod{p^3}. \quad (8.42)$$

*Proof.* Using (8.40) with  $\omega = 1$ , it follows that  $b_n + c_n$  is an integer. Using (8.40) with  $\omega = -1$  and  $2n$  in place of  $n$ , we find that  $16b_n + 4c_n$  is an integer. These two integrality conditions imply that  $b_n, c_n$  are rational numbers with denominator dividing 12. In particular, the right-hand side of (8.41) has integer coefficients since  $24 \mid m^2 - 1$  if  $(m, 6) = 1$ .

Let  $g_1(q) = a_{nm}(q) - a_n(q^{m^2})$  and  $g_2(q) = -(q^m - 1)(m^2 - 1)(c_n + a'_n(1))/2$ . As  $a_n(q)$  satisfies the  $q$ -Gauss congruences, Corollary 2.3 implies that  $g_1(\omega)$  vanishes on the zeros of  $\Phi_m(q)$ , and (8.39) ensures that  $g'_1(\omega)$  vanishes on these zeros again. We also have that  $g_2$  vanishes twice on the zeros of  $\Phi_m(q)$  by construction. Using (8.39) and (8.40), we have

$$\begin{aligned} g''_1(\omega) &= a''_{nm}(\omega) - (m^2 \omega^{m^2-1})^2 a''_n(\omega^{m^2}) - (m^2(m^2 - 1)\omega^{m^2-2}) a'_n(\omega^{m^2}) \\ &= \frac{m^4 b_n + m^2 c_n}{\omega^2} - \frac{m^4 (b_n + c_n)}{\omega^2} - \frac{m^2(m^2 - 1) a'_n(1)}{\omega^2} = \frac{-m^2(m^2 - 1)(c_n + a'_n(1))}{\omega^2} \end{aligned} \quad (8.43)$$

for any  $\omega$  which is a primitive root of unity of order  $m$ , and similarly

$$g_2''(\omega) = \frac{-m^2(m^2 - 1)(c_n + a'_n(1))}{\omega^2}. \quad (8.44)$$

Thus,  $(g_1 - g_2)''(\omega) = 0$  for every zero of  $\Phi_m$ , which establishes (8.41). To establish (8.42), we apply (8.41) with  $m = p$  and plug  $q = 1$ .  $\square$

For  $a_n(q) = \begin{bmatrix} an \\ bn \end{bmatrix}_q$ , Corollary 8.2 shows that the conditions of Proposition 8.4 hold with  $a'_n(1) = \begin{pmatrix} an \\ bn \end{pmatrix} \frac{b(a-b)}{2} n^2$ ,  $b_n = \begin{pmatrix} an \\ bn \end{pmatrix} \frac{b(a-b)n^2}{4} (b(a-b)n^2 + \frac{an}{3})$ ,  $c_n = -\frac{5}{12} \begin{pmatrix} an \\ bn \end{pmatrix} b(a-b)n^2$ . Applying the proposition with  $n = 1$ , we obtain (2.13).

For  $a_n(q) = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \begin{bmatrix} n+k \\ k \end{bmatrix}_q q^{f(n,k)}$  with  $f(x, y)$  as in Theorem 2.7, then the proof of Theorem 2.7 shows that the conditions of Proposition 8.4 hold with  $a'_n(1) = a_{n, 2xy-y^2+f(x,y)}$ ,  $b_n = a_{n, (2xy-y^2+f(x,y))^2 + \frac{x^2y}{3} - \frac{(x-y)^2}{6}}$  and  $c_n = a_{n, \frac{x^2}{6} - 2xy + y^2 - f(x,y)}$ . Applying the proposition we obtain (2.18).

Finally, for  $a_n(q) = \sum_{k,\ell} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \begin{bmatrix} n \\ \ell \end{bmatrix}_q \begin{bmatrix} k \\ \ell \end{bmatrix}_q \begin{bmatrix} k+\ell \\ n \end{bmatrix}_q q^{f(n,k,\ell)}$  with  $f(x, y, z)$  as in Theorem 2.8, the proof of Theorem 2.8 shows that the conditions of Proposition 8.4 hold with  $a'_n(1) = a_{n, xz-y^2-z^2 + \frac{3xy+yz-x^2}{2} + f(x,y,z)}$ ,  $b_n = a_{n, Q_1}$  and  $c_n = a_{n, Q_2}$ , where  $Q_1, Q_2$  are given in Theorem 2.8. Applying the proposition we obtain (2.24).

## Acknowledgments

The author would like to thank Ira Gessel and Richard Stanley for the references in §3, and the referee for valuable suggestions. He is also grateful to Wadim Zudilin for discussions on  $q$ -congruences and useful suggestions regarding the paper. He is especially thankful to Armin Straub for careful suggestions that improved an earlier draft.

## References

- [AB87] George E. Andrews and R. J. Baxter. Lattice gas generalization of the hard hexagon model. III.  $q$ -trinomial coefficients. *J. Statist. Phys.*, 47(3-4):297–330, 1987.
- [ABDJ17] B. Adamczewski, J. P. Bell, É. Delaygue, and F. Jouhet. Congruences modulo cyclotomic polynomials and algebraic independence for  $q$ -series. *Sém. Lothar. Combin.*, 78B:Art. 54, 12, 2017.
- [And90a] George E. Andrews. Euler’s “exemplum memorabile inductionis fallacis” and  $q$ -trinomial coefficients. *J. Amer. Math. Soc.*, 3(3):653–669, 1990.
- [And90b] George E. Andrews.  $q$ -trinomial coefficients and Rogers-Ramanujan type identities. In *Analytic number theory (Allerton Park, IL, 1989)*, volume 85 of *Progr. Math.*, pages 1–11. Birkhäuser Boston, Boston, MA, 1990.
- [And94] George E. Andrews. Schur’s theorem, Capparelli’s conjecture and  $q$ -trinomial coefficients. In *The Rademacher legacy to mathematics (University Park, PA, 1992)*, volume 166 of *Contemp. Math.*, pages 141–154. Amer. Math. Soc., Providence, RI, 1994.
- [And99] George E. Andrews.  $q$ -analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher. *Discrete Math.*, 204(1-3):15–25, 1999.
- [And04] George E. Andrews. Fibonacci numbers and the Rogers-Ramanujan identities. *Fibonacci Quart.*, 42(1):3–19, 2004.
- [Apé79] Roger Apéry. Irrationalité de  $\zeta(2)$  et  $\zeta(3)$ . *Astérisque*, 61:11–13, 1979.
- [AT16] Tewodros Amdeberhan and Roberto Tauraso. Supercongruences for the Almkvist-Zudilin numbers. *Acta Arith.*, 173(3):255–268, 2016.

- [AvSZ11] Gert Almkvist, Duco van Straten, and Wadim Zudilin. Generalizations of Clausen’s formula and algebraic transformations of Calabi-Yau differential equations. *Proc. Edinb. Math. Soc.* (2), 54(2):273–295, 2011.
- [AZ06] Gert Almkvist and Wadim Zudilin. Differential equations, mirror maps and zeta values. In *Mirror symmetry. V*, volume 38 of *AMS/IP Stud. Adv. Math.*, pages 481–515. Amer. Math. Soc., Providence, RI, 2006.
- [Beu85] F. Beukers. Some congruences for the Apéry numbers. *J. Number Theory*, 21(2):141–155, 1985.
- [Beu87] F. Beukers. Another congruence for the Apéry numbers. *J. Number Theory*, 25(2):201–210, 1987.
- [BSF<sup>+</sup>52] Viggo Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, and E. Jacobsthal. On the divisibility of the difference between two binomial coefficients. In *Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949*, pages 42–54. Johan Grundt Tanums Forlag, Oslo, 1952.
- [Car74] L. Carlitz. Fibonacci notes. III.  $q$ -Fibonacci numbers. *Fibonacci Quart.*, 12:317–322, 1974.
- [Car75] L. Carlitz. Fibonacci notes. IV.  $q$ -Fibonacci polynomials. *Fibonacci Quart.*, 13:97–102, 1975.
- [CCC80] S. Chowla, J. Cowles, and M. Cowles. Congruence properties of Apéry numbers. *J. Number Theory*, 12(2):188–190, 1980.
- [CGP01] Tianxin Cai and Gilberto García-Pulgarín. Two Wolstenholme’s type theorems on  $q$ -binomial coefficients. *Rev. Colombiana Mat.*, 35(2):61–65, 2001.
- [Cha11] Hei-Chi Chan. *An invitation to  $q$ -series*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2011. From Jacobi’s triple product identity to Ramanujan’s “most beautiful identity”.
- [Cig03] Johann Cigler.  $q$ -Fibonacci polynomials. *Fibonacci Quart.*, 41(1):31–40, 2003.
- [Cig04] Johann Cigler.  $q$ -Fibonacci polynomials and the Rogers-Ramanujan identities. *Ann. Comb.*, 8(3):269–285, 2004.
- [Cig16] Johann Cigler. Some divisibility properties of  $q$ -Fibonacci numbers. *arXiv preprint arXiv:1604.07977*, 2016.
- [Cla95] W. Edwin Clark.  $q$ -analogue of a binomial coefficient congruence. *Internat. J. Math. Math. Sci.*, 18(1):197–200, 1995.
- [Coh04] Henry Cohn. Projective geometry over  $F_1$  and the Gaussian binomial coefficients. *Amer. Math. Monthly*, 111(6):487–495, 2004.
- [Coo12] Shaun Cooper. Sporadic sequences, modular forms and new series for  $1/\pi$ . *Ramanujan J.*, 29(1-3):163–183, 2012.
- [Cos88] Matthijs Johannes Coster. *Supercongruences*. PhD thesis, University of Leiden, 1988.
- [DHL03] Bau-Sen Du, Sen-Shan Huang, and Ming-Chia Li. Generalized Fermat, double Fermat and Newton sequences. *J. Number Theory*, 98(1):172–183, 2003.
- [DS06] Emeric Deutsch and Bruce E. Sagan. Congruences for Catalan and Motzkin numbers and related sequences. *J. Number Theory*, 117(1):191–215, 2006.
- [Ges80] Ira Gessel. A noncommutative generalization and  $q$ -analogue of the Lagrange inversion formula. *Trans. Amer. Math. Soc.*, 257(2):455–482, 1980.
- [Ges82] Ira Gessel. Some congruences for Apéry numbers. *J. Number Theory*, 14(3):362–368, 1982.
- [Gil89] Frank S. Gillespie. A generalization of Fermat’s little theorem. *Fibonacci Quart.*, 27(2):109–115, 1989.

- [GZ18] Victor J. W. Guo and Wadim Zudilin. A  $q$ -microscope for supercongruences. *arXiv preprint arXiv:1803.01830*, 2018.
- [IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.
- [JM06] Jerzy Jezierski and Waclaw Marzantowicz. *Homotopy methods in topological fixed and periodic points theory*, volume 3 of *Topological Fixed Point Theory and Its Applications*. Springer, Dordrecht, 2006.
- [KRZ06] C. Krattenthaler, T. Rivoal, and W. Zudilin. Séries hypergéométriques basiques,  $q$ -analogues des valeurs de la fonction zêta et séries d'Eisenstein. *J. Inst. Math. Jussieu*, 5(1):53–79, 2006.
- [Mim83] Yoshio Mimura. Congruence properties of Apéry numbers. *J. Number Theory*, 16(1):138–146, 1983.
- [Min14] Gregory T. Minton. Linear recurrence sequences satisfying congruence conditions. *Proc. Amer. Math. Soc.*, 142(7):2337–2352, 2014.
- [MS16] Amita Malik and Armin Straub. Divisibility properties of sporadic Apéry-like numbers. *Res. Number Theory*, 2:Art. 5, 26, 2016.
- [OS13] Robert Osburn and Brundaban Sahu. A supercongruence for generalized Domb numbers. *Funct. Approx. Comment. Math.*, 48(part 1):29–36, 2013.
- [OSS16] Robert Osburn, Brundaban Sahu, and Armin Straub. Supercongruences for sporadic sequences. *Proc. Edinb. Math. Soc. (2)*, 59(2):503–518, 2016.
- [Pan06] Hao Pan. Arithmetic properties of  $q$ -Fibonacci numbers and  $q$ -Pell numbers. *Discrete Math.*, 306(17):2118–2127, 2006.
- [Pan08] Hao Pan.  $q$ -analogue of Gauss’ divisibility theorem. *arXiv preprint arXiv:0804.0834*, 2008.
- [Pan13] Hao Pan. Congruences for  $q$ -Lucas numbers. *Electron. J. Combin.*, 20(2):Paper 29, 8, 2013.
- [Rob00] Alain M. Robert. *A course in  $p$ -adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [RSW04] V. Reiner, D. Stanton, and D. White. The cyclic sieving phenomenon. *J. Combin. Theory Ser. A*, 108(1):17–50, 2004.
- [Sag11] Bruce E. Sagan. The cyclic sieving phenomenon: a survey. In *Surveys in combinatorics 2011*, volume 392 of *London Math. Soc. Lecture Note Ser.*, pages 183–233. Cambridge Univ. Press, Cambridge, 2011.
- [Sch17] I. Schur. Ein Beitrag zur additiven Zahlentheorie und zur Theorie der Kettenbrüche. *Berl. Ber.*, 1917:302–321, 1917.
- [Sla08] Keith R. Slavin.  $q$ -binomials and the greatest common divisor. *Integers*, 8:A05, 10, 2008.
- [SP07] Ling-Ling Shi and Hao Pan. A  $q$ -analogue of Wolstenholme’s harmonic series congruence. *Amer. Math. Monthly*, 114(6):529–531, 2007.
- [Sta97] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.
- [Sta99] Richard P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

- [Ste17] Heinrich Steinlein. Fermat’s Little Theorem and Gauss Congruence: Matrix Versions and Cyclic Permutations. *Amer. Math. Monthly*, 124(6):548–553, 2017.
- [Str11] Armin Straub. A  $q$ -analog of Ljunggren’s binomial congruence. In *Proceedings of the 23rd international conference on formal power series and algebraic combinatorics, FPSAC 2011, Reykjavik, Iceland, June 13–17, 2011*, pages 897–902. Nancy: The Association. Discrete Mathematics & Theoretical Computer Science (DMTCS), 2011.
- [Str19] Armin Straub. Supercongruences for polynomial analogs of the Apéry numbers. *Proceedings of the American Mathematical Society*, 147:1023–1036, 2019.
- [War01] S. Ole Warnaar. Refined  $q$ -trinomial coefficients and character identities. In *Proceedings of the Baxter Revolution in Mathematical Physics (Canberra, 2000)*, volume 102, pages 1065–1081, 2001.
- [War03] S. Ole Warnaar. The generalized Borwein conjecture. II. Refined  $q$ -trinomial coefficients. *Discrete Math.*, 272(2-3):215–258, 2003.
- [Zag09] Don Zagier. Integral solutions of Apéry-like recurrence equations. In *Groups and symmetries*, volume 47 of *CRM Proc. Lecture Notes*, pages 349–366. Amer. Math. Soc., Providence, RI, 2009.
- [Zar08] A. V. Zarelua. On congruences for the traces of powers of some matrices. *Proceedings of the Steklov Institute of Mathematics*, 263(1):78–98, 2008.
- [Zhe11] De-Yin Zheng. An algebraic identity on  $q$ -Apéry numbers. *Discrete Math.*, 311(23-24):2708–2710, 2011.
- [Zud19] Wadim Zudilin. Congruences for  $q$ -binomial coefficients. *arXiv preprint arXiv:1901.07843*, 2019.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 6997801, Israel. E-mail address: ofir.goro@gmail.com