

# PROOFS OF INTEGRALITY OF BINOMIAL COEFFICIENTS

KEITH CONRAD

## 1. INTRODUCTION

The *binomial coefficients* are the numbers

$$(1.1) \quad \binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

for integers  $n$  and  $k$  with  $0 \leq k \leq n$ . Their name comes from their appearance as coefficients in the binomial theorem

$$(1.2) \quad (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

but we will use (1.1), not (1.2), as their definition. While  $\binom{n}{k}$  is, by (1.1), obviously a positive rational number, it is not at all obvious from (1.1) that  $\binom{n}{k}$  is an integer.

**Theorem 1.1.** *For all integers  $n$  and  $k$  with  $0 \leq k \leq n$ ,  $\binom{n}{k} \in \mathbf{Z}$ .*

We will give six proofs of Theorem 1.1 and then discuss a generalization of binomial coefficients called  $q$ -binomial coefficients, which have an analogue of Theorem 1.1.

## 2. PROOF BY COMBINATORICS

Our first proof will be a proof of the binomial theorem that, at the same time, provides a combinatorial meaning of binomial coefficients. By the distributive law we can write

$$(1+x)^n = \underbrace{(1+x)(1+x)\cdots(1+x)}_{n \text{ terms}} = \sum_{k=0}^n c_{n,k} x^k,$$

where  $c_{n,k}$  is the number of ways of picking  $k$  items out of  $n$  items (in  $k$  of the factors  $1+x$  of  $(1+x)^n$  pick  $x$  and in the other factors pick 1). The numbers  $c_{n,k}$ , by the description we just gave of them (“the number of ways . . .”), are positive integers. Clearly  $c_{n,0} = c_{n,n} = 1$ .

To get a formula for  $c_{n,k}$ , we have

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &= (1+x) \sum_{k=0}^n c_{n,k} x^k \\ &= \sum_{k=0}^n c_{n,k} x^k + \sum_{k=0}^n c_{n,k} x^{k+1} \\ &= 1 + \sum_{k=1}^n (c_{n,k} + c_{n,k-1}) x^k + x^{n+1}, \end{aligned}$$





Now if we *start* with integers  $n \geq k \geq 0$ , let's make  $\binom{n}{k}$  be  $\binom{m+k-1}{k}$  by using  $m = n - k + 1$ . This is a positive integer since  $n \geq k$ . Therefore  $\binom{n}{k} = a_{n-k+1,k} \in \mathbf{Z}^+$ .

## 5. PROOF BY NUMBER THEORY

We observed in the introduction that  $\binom{n}{k}$  is a positive rational number. We will prove it is an integer by showing its denominator is 1 using prime factorizations.

The *multiplicity* of a prime  $p$  in a nonzero rational number  $r$  is the power of  $p$  in the reduced form of  $r$ . For example,

$$\frac{40}{7} = \frac{2^3 \cdot 5}{7} = 2^3 \cdot 5^1 \cdot 7^{-1}$$

so we say  $40/7$  has 2-multiplicity 3, 5-multiplicity 1, 7-multiplicity  $-1$ , and  $p$ -multiplicity 0 for primes  $p$  other than 2, 5, and 7. Denote the  $p$ -multiplicity of  $r$  as  $m_p(r)$ , so the above calculations say  $m_2(40/7) = 3$ ,  $m_5(40/7) = 1$ ,  $m_7(40/7) = -1$ , and  $m_p(40/7) = 0$  for primes  $p$  other than 2, 5, and 7.

Since the  $p$ -multiplicity is an exponent, it behaves like a logarithm:

$$(5.1) \quad m_p(ab) = m_p(a) + m_p(b), \quad m_p(a/b) = m_p(a) - m_p(b).$$

For example,  $m_2(80) = m_2(16 \cdot 5) = 4$  and  $m_2(8) + m_2(10) = 3 + 1 = 4$ , while  $m_2(80/14) = m_2(40/7) = 3$  and  $m_2(80) - m_2(14) = 4 - 1 = 3$ . The rules (5.1) essentially come from unique prime factorization in  $\mathbf{Z}$ .

A nonzero rational number is an integer exactly when its  $p$ -multiplicity is nonnegative for *all* primes  $p$  (a rational number that is not an integer has negative  $p$ -multiplicity for primes  $p$  appearing in its reduced form denominator). We will prove  $\binom{n}{k} \in \mathbf{Z}$  by showing  $m_p\left(\binom{n}{k}\right) \geq 0$  for every prime  $p$ . According to [2, p. 263], this argument is due to André [1, pp. 188-189].

For prime  $p$  and integer  $N \geq 0$ , Legendre [3, p. 10] proved a formula for  $m_p(N!)$ :

$$m_p(N!) = \sum_{i \geq 1} \left\lfloor \frac{N}{p^i} \right\rfloor = \left\lfloor \frac{N}{p} \right\rfloor + \left\lfloor \frac{N}{p^2} \right\rfloor + \left\lfloor \frac{N}{p^3} \right\rfloor + \cdots,$$

where the sum is finite since the  $i$ th term is 0 once  $p^i > N$ .<sup>1</sup> Thus

$$\begin{aligned} m_p\left(\binom{n}{k}\right) &= m_p\left(\frac{n!}{k!(n-k)!}\right) \\ &= m_p(n!) - m_p(k!) - m_p((n-k)!) \\ &= \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor - \sum_{i \geq 1} \left\lfloor \frac{k}{p^i} \right\rfloor - \sum_{i \geq 1} \left\lfloor \frac{n-k}{p^i} \right\rfloor \\ (5.2) \quad &= \sum_{i \geq 1} \left( \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor \right). \end{aligned}$$

Each term in this last sum has the form  $\lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$ , where  $x = k$  and  $y = n - k$ . For all real numbers  $x$  and  $y$ ,  $\lfloor x + y \rfloor$  is either  $\lfloor x \rfloor + \lfloor y \rfloor$  or  $\lfloor x \rfloor + \lfloor y \rfloor + 1$ : if the decimal parts of  $x$  and  $y$  have sum in  $[0, 1)$  then  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ , while if the decimal parts of  $x$  and  $y$  have sum in  $[1, 2)$  then  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1$ .

<sup>1</sup>A second formula for  $m_p(N!)$  is  $(N - s_p(N))/(p - 1)$ , where  $s_p(N)$  is the sum of the base  $p$  digits of  $N$ . This is also due to Legendre [3, p. 12].

Since  $\lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$  is always 0 or 1, the formula (5.2) shows  $m_p \binom{n}{k}$  is a sum of terms that are each 0 or 1. Thus  $m_p \binom{n}{k}$  is a nonnegative integer for every prime  $p$ , so  $\binom{n}{k} \in \mathbf{Z}^+$ .

## 6. PROOF BY GROUP THEORY

For a subgroup  $H$  of a finite group  $G$ ,  $|G|/|H|$  is a positive integer by Lagrange's theorem:  $|G|/|H|$  is the index  $[G : H]$ . We'll use this for  $G = S_n$ , of order  $n!$ . For  $1 \leq k \leq n - 1$ , the permutations of  $\{1, 2, \dots, n\}$  carrying  $\{1, \dots, k\}$  and  $\{k + 1, \dots, n\}$  back to themselves form a subgroup  $H$  isomorphic to  $S_k \times S_{n-k}$ , so  $|H| = k!(n - k)!$  and  $\binom{n}{k} = [G : H]$ .<sup>2</sup>

## 7. PROOF BY POLYNOMIAL FUNCTIONS

For a variable  $x$ , set

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-(k-1))}{k!} = \frac{x(x-1)\cdots(x-k+1)}{k!}.$$

This is a polynomial of degree  $k$  with rational coefficients. For example,

$$\binom{x}{0} = 1, \quad \binom{x}{1} = x, \quad \binom{x}{2} = \frac{x^2 - x}{2}, \quad \binom{x}{3} = \frac{x^3 - 3x^2 + 2x}{6}.$$

We can see that the coefficients are not generally integers.

For an integer  $n \geq k$ , the value of  $\binom{x}{k}$  at  $x = n$  is  $\binom{n}{k}$ . Since we have a polynomial, we can substitute in values of  $x$  that are integers less than  $k$ . When  $k \geq 1$  and  $x = 0, 1, \dots, k - 1$  we have  $\binom{x}{k} = 0$ . At  $x = k$ , the value of  $\binom{x}{k}$  is 1. This information turns out to be enough to deduce that the values of  $\binom{x}{k}$  at larger integers are also in  $\mathbf{Z}$ .

**Theorem 7.1.** *If  $f(x)$  is a polynomial with rational coefficients of degree  $k$  and  $f(0), f(1), \dots, f(k)$  are in  $\mathbf{Z}$  then  $f(n) \in \mathbf{Z}$  for every integer  $n \geq 0$ .*

*Proof.* We induct on  $\deg f(x)$ . The result is obvious if  $k = 0$ . For  $k = 1$ ,  $f(x) = ax + b$  for  $a$  and  $b$  in  $\mathbf{Q}$ , so  $f(0) = b$  and  $f(1) = a + b$ . Thus  $a = f(1) - b = f(1) - f(0)$ , and  $b = f(0)$  are in  $\mathbf{Z}$ , so  $f(n) = an + b$  is in  $\mathbf{Z}$  when  $n$  is a nonnegative integer (or an arbitrary integer).

Now suppose  $\deg f = k \geq 2$  and the theorem is proved for polynomials with rational coefficients of degree less than  $k$ . Set  $g(x) = f(x + 1) - f(x)$ . What does this look like?

Writing  $f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$ , we have

$$\begin{aligned} g(x) &= f(x + 1) - f(x) \\ &= (a_k(x + 1)^k + a_{k-1}(x + 1)^{k-1} + \dots + a_0) - (a_k x^k + a_{k-1} x^{k-1} + \dots + a_0) \\ &= a_k((x + 1)^k - x^k) + a_{k-1}((x + 1)^{k-1} - x^{k-1}) + \dots + a_1(x + 1 - x) \\ &= k a_k x^{k-1} + \text{lower-degree terms,} \end{aligned}$$

where the last formula is due to  $(x + 1)^k = x^k + kx^{k-1} + \text{lower-degree terms}$ . (This is a weak form of the binomial theorem.) Since  $a_k \neq 0$ ,  $g(x)$  has degree  $k - 1$ .

From  $f(0), f(1), \dots, f(k)$  being in  $\mathbf{Z}$ , the values  $g(0) = f(1) - f(0)$ ,  $g(1) = f(2) - f(1)$ ,  $\dots$ ,  $g(k - 1) = f(k) - f(k - 1)$  are in  $\mathbf{Z}$  since each one is a difference of integers. By induction on polynomial degrees,  $g(n) \in \mathbf{Z}$  for all nonnegative integers  $n$ . Then for integers  $n \geq 1$ ,

$$\begin{aligned} f(n) &= (f(n) - f(n - 1)) + (f(n - 1) - f(n - 2)) + \dots + (f(1) - f(0)) + f(0) \\ (7.1) \quad &= g(n - 1) + g(n - 2) + \dots + g(0) + f(0), \end{aligned}$$

<sup>2</sup>Also  $\frac{n!}{k!(n-k)!} \in \mathbf{Z}^+$  since the  $k$ -element subsets of  $\{1, \dots, n\}$  are an orbit of  $S_n$  with stabilizer  $S_k \times S_{n-k}$ .

which is a sum of integers, so  $f(n) \in \mathbf{Z}$ .  $\square$

**Remark 7.2.** The theorem admits a slightly stronger conclusion than we have shown:  $f(n) \in \mathbf{Z}$  for all  $n \in \mathbf{Z}$ , not just when  $n \geq 0$ .

This approach to the integrality of binomial coefficients shares a lot in common with the proof by recursion. Indeed, for  $k \geq 1$  the polynomial  $\binom{x}{k}$  satisfies  $\binom{x+1}{k} = \binom{x}{k-1} + \binom{x}{k}$ , so if  $f(x) = \binom{x}{k}$  then  $g(x) := f(x+1) - f(x)$  is  $\binom{x}{k-1}$ . In this case, (7.1) says

$$\begin{aligned} \binom{n}{k} &= g(n-1) + g(n-2) + \cdots + g(0) + f(0) \\ &= \binom{n-1}{k-1} + \binom{n-2}{k-1} + \cdots + \binom{0}{k-1} + \binom{0}{k}. \end{aligned}$$

The term  $f(0)$  is 0, and also  $g(j) = 0$  for  $j = 0, \dots, k-2$ , so (7.1) for  $f(x) = \binom{x}{k}$  says

$$\binom{n}{k} = g(n-1) + g(n-2) + \cdots + g(k-1) = \sum_{j=k-1}^{n-1} \binom{j}{k-1},$$

which is exactly (3.2).

## 8. $q$ -BINOMIAL COEFFICIENTS

For a real number  $q > 0$  with  $q \neq 1$ , or an indeterminate  $q$ , the positive integer  $n$  can be generalized to the polynomial

$$(n)_q = \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1}.$$

This polynomial is called the  $q$ -analogue of  $n$ , and at  $q = 1$  its value is  $n$ . For example,

$$(1)_q = 1, \quad (2)_q = 1 + q, \quad (3)_q = 1 + q + q^2.$$

The expression of  $(n)_q$  as the ratio  $(q^n - 1)/(q - 1)$  does not make direct sense at  $q = 1$ , but its limit as  $q \rightarrow 1$  is  $n$ . The product

$$(n)_q! = (n)_q(n-1)_q \cdots (2)_q(1)_q,$$

is called the  $q$ -factorial of  $n$ , and we set  $(0)_q! = 1$  (analogous to setting  $0! = 1$ ). The ratio

$$(8.1) \quad \binom{n}{k}_q := \frac{(n)_q!}{(k)_q!(n-k)_q!} = \frac{(n)_q(n-1)_q \cdots (n-k+1)_q}{(k)_q!}$$

is called a  $q$ -binomial coefficient. Each  $(j)_q$  is a polynomial in  $q$ , so  $\binom{n}{k}_q$  is a rational function of  $q$ . Since  $(n)_q! = n!$  at  $q = 1$ , we have  $\binom{n}{k}_q = \binom{n}{k}$  at  $q = 1$ .

The second defining formula for  $\binom{n}{k}_q$  in (8.1) has an equal number of factors in the numerator and denominator (the first defining formula in (8.1) does as well), so writing  $(j)_q = (q^j - 1)/(q - 1)$  gives us a third formula for  $q$ -binomial coefficients:

$$(8.2) \quad \binom{n}{k}_q := \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

**Example 8.1.** Since  $(0)_q! = 1$  and  $(1)_q! = 1$ , we have  $\binom{n}{0}_q = \binom{n}{n}_q = 1$  for  $n \geq 0$  and  $\binom{n}{1}_q = \binom{n}{n-1}_q = (n)_q = 1 + q + \cdots + q^{n-1}$  for  $n \geq 1$ , which generalize  $\binom{n}{0} = \binom{n}{n} = 1$  for  $n \geq 0$  and  $\binom{n}{1} = \binom{n}{n-1} = n$  for  $n \geq 1$ .

**Example 8.2.** The first  $q$ -binomial coefficient  $\binom{n}{k}_q$  with  $k \neq 0, 1, n-1$ , or  $n$  is

$$\binom{4}{2}_q = \frac{(4)_q(3)_q}{(2)_{q!}} = \frac{(1+q+q^2+q^3)(1+q+q^2)}{(1+q)} = (1+q^2)(1+q+q^2),$$

where the last formula comes from the factorization  $1+q+q^2+q^3 = (1+q)(1+q^2)$ . Setting  $q = 1$ , we recover the value  $\binom{4}{2} = 2 \cdot 3 = 6$ .

The calculation in Example 8.2 is a special case of the following general theorem.

**Theorem 8.3.** For integers  $n \geq k \geq 0$ ,  $\binom{n}{k}_q$  is a polynomial in  $q$  with coefficients that are nonnegative integers.

Theorem 8.3 implies the integrality of binomial coefficients by setting  $q = 1$  in the conclusion of Theorem 8.3. We will show how the ideas in most of the proofs of integrality of  $\binom{n}{k}$  can be adapted to give a proof of Theorem 8.3, sometimes in the weaker form that the coefficients are in  $\mathbf{Z}$  rather than being nonnegative in  $\mathbf{Z}$ . That weaker form suffices to see that  $\binom{n}{k} = \binom{n}{k}_1$  is an integer, and it is clearly positive from its definition.

Proof of Theorem 8.3 by combinatorics:

The  $q$ -analogue of  $(1+x)^n$  is  $(1+x)(1+qx)(1+q^2x) \cdots (1+q^{n-1}x)$ . By distributivity,

$$(8.3) \quad (1+x)(1+qx) \cdots (1+q^{n-1}x) = \sum_{k=0}^n c_{n,k}(q)x^k$$

where  $c_{n,k}(q)$  is a polynomial in  $q$  with nonnegative integer coefficients. Clearly  $c_{n,0}(q) = 1$  and  $c_{n,n}(q) = q^{0+1+2+\cdots+(n-1)} = q^{n(n-1)/2}$ . For  $q \neq 1$  we will get a formula for  $c_{n,k}(q)$  by computing the left side of (8.3) in two ways. First,

$$\begin{aligned} (1+x)(1+qx) \cdots (1+q^n x) &= (1+x)(1+qx) \cdots (1+q^{n-1}x) \cdot (1+q^n x) \\ &= \left( \sum_{k=0}^n c_{n,k}(q)x^k \right) (1+q^n x) \\ &= \sum_{k=0}^n c_{n,k}(q)x^k + \sum_{k=0}^n q^n c_{n,k}(q)x^{k+1} \\ &= 1 + \sum_{k=1}^n c_{n,k}(q)x^k + \sum_{k=1}^n q^n c_{n,k-1}(q)x^k + q^{n+n(n-1)/2}x^{n+1} \\ &= 1 + \sum_{k=1}^n (c_{n,k}(q) + q^n c_{n,k-1}(q))x^k + q^{n+n(n-1)/2}x^{n+1}. \end{aligned}$$

Second,

$$\begin{aligned} (1+x)(1+qx) \cdots (1+q^n x) &= (1+x) \cdot (1+qx) \cdots (1+q^{n-1}x)(1+q^n x) \\ &= (1+x) \left( \sum_{k=0}^n c_{n,k}(q)(qx)^k \right) \\ &= 1 + \sum_{k=1}^n \left( q^k c_{n,k}(q) + q^{k-1} c_{n,k-1}(q) \right) x^k + q^{n(n-1)/2+n}x^{n+1} \end{aligned}$$

Equating coefficients of  $x^k$  in both formulas, for  $1 \leq k \leq n$ ,

$$c_{n,k}(q) + q^n c_{n,k-1}(q) = q^k c_{n,k}(q) + q^{k-1} c_{n,k-1}(q) \implies c_{n,k}(q) = \frac{q^n - q^{k-1}}{q^k - 1} c_{n,k-1}(q).$$

(If we take the limit as  $q \rightarrow 1$ , this recursive formula becomes (2.1).) Iterating this recursion  $k - 1$  more times,

$$\begin{aligned} c_{n,k}(q) &= \frac{(q^n - q^{k-1})(q^n - q^{k-2}) \cdots (q^n - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)} c_{n,0}(q) \\ &= \frac{q^{k-1}(q^{n-(k-1)} - 1)q^{k-2}(q^{n-(k-2)} - 1) \cdots q^0(q^n - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)} \\ &= \frac{q^{(k-1)+(k-2)+\cdots+1}(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)} \\ &= q^{k(k-1)/2} \binom{n}{k}_q, \end{aligned}$$

where the last formula comes from (8.2). This proves  $q^{k(k-1)/2} \binom{n}{k}_q$  is a polynomial in  $q$  with nonnegative integer coefficients when  $q \neq 1$ . To conclude that  $\binom{n}{k}_q$  is also a polynomial in  $q$ , here are two approaches. Each one treats the previous calculations as if  $q$  is an indeterminate.

- (1) In the expansion (8.3),  $c_{n,k}(q)$  is a sum of products of distinct  $q$ -powers  $k$  at a time, and each of those products has exponent at least  $0 + 1 + \cdots + (k - 1) = k(k - 1)/2$ . Therefore  $c_{n,k}(q)$  is a polynomial in  $q$  that's divisible by  $q^{k(k-1)/2}$ , so  $\binom{n}{k}_q$  is a polynomial in  $q$ .
- (2) By (8.2),  $\binom{n}{k}_q$  is a rational function of  $q$  with no  $q$ -power in its denominator, so when its product with a power of  $q$  is a polynomial in  $q$ ,  $\binom{n}{k}_q$  is also a polynomial in  $q$ .

Proof of Theorem 8.3 by recursion:

A recursion for  $q$ -binomial coefficients that generalizes the Pascal's triangle recursion for binomial coefficients is

$$\binom{n}{k}_q = q^{n-k} \binom{n-1}{k-1}_q + \binom{n-1}{k}_q.$$

Iterating this enough times, we get

$$\binom{n}{k}_q = \sum_{j=0}^{n-k} q^{n-k-j} \binom{n-1-j}{k-1}_q = \sum_{j=k-1}^{n-1} q^{j-(k-1)} \binom{j}{k-1}_q,$$

which generalizes (3.2). If all  $q$ -binomial coefficients with denominator  $k - 1$  are polynomials in  $q$  with nonnegative integer coefficients then so is each  $\binom{n}{k}_q$  by the above formula.

Therefore starting from the value  $\binom{0}{0}_q = 1$ , Theorem 8.3 is proved by induction on  $k$ .

Proof of Theorem 8.3 by calculus:

A  $q$ -analogue of the series identity

$$\frac{1}{(1-x)^m} = \sum_{k \geq 0} \binom{m+k-1}{k} x^k$$

for  $|x| < 1$  and  $m \geq 1$  is

$$\frac{1}{(1-x)(1-qx)\cdots(1-q^{m-1}x)} = \sum_{k \geq 0} \binom{m+k-1}{k}_q x^k$$

for  $|x| < 1$ ,  $0 < q < 1$ , and  $m \geq 1$ . Since each  $1/(1-q^i x)$  for  $|x| < 1$  and  $0 < q < 1$  can be expanded into a geometric series  $\sum_{k \geq 0} q^{ik} x^k$ , the product of these series is a power series in  $x$  having coefficients that are polynomials in  $q$  with nonnegative integer coefficients. Therefore  $\binom{m+k-1}{k}_q$  is a polynomial in  $q$  with nonnegative integer coefficients, at least when  $0 < q < 1$ . A polynomial and rational function in  $q$  that agree for  $0 < q < 1$  must agree for all  $q$ , so we get Theorem 8.3 using  $m = n - k + 1$ .

Proof of Theorem 8.3 by number theory:

Treat  $q$  as an indeterminate. By (8.2),  $\binom{n}{k}_q$  is a ratio of products of polynomials of the form  $q^i - 1$ , so the irreducible factors in the numerator and denominator of (8.2) are cyclotomic polynomials  $\Phi_j(q)$  for various  $j$ . We will show every cyclotomic polynomial  $\Phi_j(q)$  has nonnegative multiplicity in  $\binom{n}{k}_q$ , so  $\binom{n}{k}_q$  is a product of cyclotomic polynomials and therefore is a polynomial with integral coefficients. (This will not tell us the coefficients of that polynomial in  $q$  are nonnegative.) For positive integers  $i$  and  $j$ ,  $\Phi_j(q)$  is a factor of  $q^i - 1$  if and only if  $j \mid i$ , so the multiplicity of  $\Phi_j(q)$  as a factor of the polynomial  $(n)_q!$  is  $|\{i \leq n : j \mid i\}| = \lfloor n/j \rfloor$ . Therefore the multiplicity of  $\Phi_j(q)$  in  $\binom{n}{k}_q = (n)_q! / (k)_q! (n-k)_q!$  is  $\lfloor n/j \rfloor - \lfloor k/j \rfloor - \lfloor (n-k)/j \rfloor$ , which has the form  $\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$ , so it is 0 or 1. (Thus no  $\binom{n}{k}_q$  has a repeated irreducible factor, which is a contrast to ordinary binomial coefficients  $\binom{n}{k}$  since they often have repeated prime factors. In fact, the largest  $n$  for which all  $\binom{n}{k}$  are squarefree is 23. See <http://oeis.org/A048278>.)

Proof of Theorem 8.3 by group theory:

Let  $q = p$  be an arbitrary prime number. We will use group theory to show  $\binom{n}{k}_p$  is a positive integer and then explain why this implies  $\binom{n}{k}_q$  is a polynomial in  $q$  for general  $q$ .

The group  $\mathrm{GL}_n(\mathbf{F}_p)$  is all the automorphisms of the additive group  $\mathbf{F}_p^n$ . Using linear algebra (counting bases of  $\mathbf{F}_p^n$ ), the order of this group is

$$\begin{aligned} (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) &= (p^n - 1)(p^{n-1} - 1)p \cdots (p - 1)p^{n-1} \\ &= (p^n - 1)(p^{n-1} - 1) \cdots (p - 1)p^{n(n-1)/2} \\ &= (n)_p! p^{n(n-1)/2}. \end{aligned}$$

Inside  $\mathrm{GL}_n(\mathbf{F}_p)$ , the matrices  $A$  that preserve the direct sum decomposition  $\mathbf{F}_p^k \oplus \mathbf{F}_p^{n-k}$  (this means  $A$  carries  $\mathbf{F}_p^k \oplus \mathbf{0}$  to itself and  $\mathbf{0} \oplus \mathbf{F}_p^{n-k}$  to itself) is a subgroup. This subgroup is isomorphic to  $\mathrm{GL}_k(\mathbf{F}_p) \times \mathrm{GL}_{n-k}(\mathbf{F}_p)$ , so its order is  $(k)_p! p^{k(k-1)/2} (n-k)_p! p^{(n-k)(n-k-1)/2}$ . By Lagrange's theorem, the ratio

$$\begin{aligned} \frac{|\mathrm{GL}_n(\mathbf{F}_p)|}{|\mathrm{GL}_k(\mathbf{F}_p) \times \mathrm{GL}_{n-k}(\mathbf{F}_p)|} &= \frac{(n)_p! p^{n(n-1)/2}}{(k)_p! p^{k(k-1)/2} (n-k)_p! p^{(n-k)(n-k-1)/2}} \\ &= \frac{(n)_p!}{(k)_p! (n-k)_p!} p^{k(n-k)} \\ &= \binom{n}{k}_p p^{k(n-k)} \end{aligned}$$

is an integer. Since  $(n)_p!$  and  $(k)_p!(n-k)_p!$  are integers that are not divisible by  $p$ , we can conclude from  $\binom{n}{k}_p p^{k(n-k)} \in \mathbf{Z}$  that  $\binom{n}{k}_p \in \mathbf{Z}$ .

If a rational function in an indeterminate  $q$  has numerator and denominator that are polynomials in  $q$  with coefficients in  $\mathbf{Z}$ , and its values are in  $\mathbf{Z}$  as  $q$  runs through the prime numbers, then the rational function is a polynomial in  $q$  with coefficients in  $\mathbf{Q}$ . This is a special case of Theorem A.1 below, and it tells us  $\binom{n}{k}_q$  is a polynomial in  $q$ . But watch out: a polynomial with coefficients in  $\mathbf{Q}$  that has integral values at primes need not have coefficients in  $\mathbf{Z}$ . For example,  $\frac{1}{2}(q^2 - q)$  has values in  $\mathbf{Z}$  when  $q$  runs through  $\mathbf{Z}$  (not just primes) but its coefficients are not in  $\mathbf{Z}$ . To show  $\binom{n}{k}_q$  has coefficients in  $\mathbf{Z}$ , we can use more information about  $q$ -binomial coefficients: they are a ratio of monic polynomials with integer coefficients, by (8.2). It can be shown (see Theorem A.1) that a polynomial with coefficients in  $\mathbf{Q}$  that is equal to a ratio of monic polynomials with coefficients in  $\mathbf{Z}$  must itself have coefficients in  $\mathbf{Z}$ . This is why  $\binom{n}{k}_q$  has coefficients in  $\mathbf{Z}$ , but we don't learn why the coefficients are nonnegative.

**Remark 8.4.** The proof of integrality of  $\binom{n}{k}$  in Section 7, using polynomial functions and the discrete difference operation  $f(x+1) - f(x)$  to reduce degrees, has a  $q$ -analogue: there are  $q$ -discrete difference operations that reduce “ $q$ -degrees” (e.g., the sequence  $f(n) = q^{kn}$  for each  $k \geq 0$  has  $q$ -degree  $k$ ). We have already given enough other proofs of Theorem 8.3 that we omit the proof analogous to the method in Section 7.

#### APPENDIX A. A CRITERION FOR A RATIONAL FUNCTION TO BE A POLYNOMIAL

We used the theorem below in the proof of Theorem 8.3 by group theory.

**Theorem A.1.** *If  $A(x)$  and  $B(x)$  are polynomials with coefficients in  $\mathbf{Z}$  and  $A(n)/B(n) \in \mathbf{Z}$  for infinitely many integers  $n$ , then  $A(x)/B(x)$  is a polynomial with rational coefficients.*

*If  $B(x)$  has leading coefficient 1 then  $A(x)/B(x)$  is a polynomial with integral coefficients.*

This is *not* saying  $B(x)$  is constant, since  $A(x)/B(x)$  may not be reduced at first. For example,  $(x^4 - 1)/(x^2 - 1)$  and  $(x^4 - 1)/(x^2 + 1)$  fit the conditions of the theorem.

*Proof.* The result is obvious if  $A(x)$  is 0, so assume  $A(x) \neq 0$ . Polynomials with integral coefficients have unique factorization, so we can suppose  $A(x)/B(x)$  is in reduced form. Then  $A(x)$  and  $B(x)$  have no nonconstant common factor in  $\mathbf{Q}[x]$ , so  $\gcd(A(x), B(x)) = 1$  in  $\mathbf{Q}[x]$ . By Bezout's identity,  $A(x)U(x) + B(x)V(x) = 1$  for some  $U(x), V(x) \in \mathbf{Q}[x]$ . Multiplying through by a common denominator of the coefficients of  $U(x)$  and  $V(x)$ , there are  $\tilde{U}(x)$  and  $\tilde{V}(x)$  in  $\mathbf{Z}[x]$  and  $c \in \mathbf{Z} - \{0\}$  such that

$$(A.1) \quad A(x)\tilde{U}(x) + B(x)\tilde{V}(x) = c.$$

Let  $S$  be the set of  $n \in \mathbf{Z}$  such that  $A(n)/B(n) \in \mathbf{Z}$ , so  $S$  is infinite. Thus  $S$  contains  $n$  with  $|n| \rightarrow \infty$ . For  $n \in S$  we have  $B(n) \mid A(n)$ , so (A.1) implies  $B(n) \mid c$ . If  $B(x)$  is nonconstant, then  $|B(n)| \rightarrow \infty$  as  $|n| \rightarrow \infty$ , but a nonzero integer doesn't have factors that have arbitrarily large absolute value. Therefore  $B(x)$  is constant, so  $A(x)/B(x) \in \mathbf{Q}[x]$ .

Suppose now that  $B(x)$  has leading coefficient 1. Then we can divide  $A(x)$  by  $B(x)$  using polynomials with integral coefficients:  $A(x) = B(x)q(x) + r(x)$  where  $q(x)$  and  $r(x)$  have integral coefficients and  $r(x) = 0$  or  $\deg r < \deg B$ . Since  $B(x) \mid A(x)$  in  $\mathbf{Q}[x]$ , the uniqueness of quotient and remainder in  $\mathbf{Q}[x]$  implies  $r(x) = 0$ , so  $A(x)/B(x) = q(x)$  is a polynomial with integral coefficients.  $\square$

## REFERENCES

- [1] D. André, *Sur une formule d'arithmétique*, Nouv. Ann. Math. **13** (1874), 185–189. Online at [http://www.numdam.org/item/NAM\\_1874\\_2\\_13\\_\\_185\\_1/](http://www.numdam.org/item/NAM_1874_2_13__185_1/).
- [2] L. E. Dickson, “History of the Theory of Numbers, Vol. I: Primality and Divisibility,” Chelsea, Bronx, NY, 1971.
- [3] A.-M. Legendre, “Théorie des Nombres, Tome 1,” 3rd ed., Firmin Didot Frères, Paris, 1830. Online at <https://books.google.com/books?id=BTIVAAAQAAJ>.