FACTORS OF SUMS OF POWERS OF BINOMIAL COEFFICIENTS

NEIL J. CALKIN

ABSTRACT. We prove divisibility properties for sums of powers of binomial coefficients and of q-binomial coefficients.

Dedicated to the memory of Paul Erdős

1. INTRODUCTION

It is well known that if

$$f_{n,a} = \sum_{k=0}^{n} \binom{n}{k}^a$$

then $f_{n,0} = n+1$, $f_{n,1} = 2^n$, $f_{n,2} = \binom{2n}{n}$, and it is possible to show (Wilf, personal communication, using techniques in [8]) that for $3 \le a \le 9$, there is no closed form for $f_{n,a}$ as a sum of a fixed number of hypergeometric terms. Similarly, using asymptotic techniques, de Bruijn has shown [2] that if $a \ge 4$, then $h_{2n,a}$ has no closed form, where

$$h_{n,a} = \sum_{k=0}^{n} (-1)^k \binom{n}{k}^a$$

(clearly, $h_{2n+1,a} = 0$.) In this paper we will prove that while no closed form may exist, there are interesting divisibility properties of $f_{n,2a}$ and $h_{2n,a}$. We will illustrate some of the techniques which may be applied to prove these sorts of results.

Our main results are:

Theorem 1. *for all positive n and a,*

$$\binom{2n}{n} \quad \Big| \quad \sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^a .$$

Theorem 2. *For all positive integers a, m, j*

$$t(n,q) \quad \Big| \quad \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^a (-1)^k q^{jk},$$

where the $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are the q-binomial coefficients, and $t(n,q)$ is an integer polynomial in q with the property that $t(n,1)$ is the odd part of $\binom{n}{k}$.

1991 *Mathematics Subject Classification.* 05A10,05A30,11B65.

2. BACKGROUND

In attempting to extend the results of previous work [1], we were led to consider factorizations of sums of powers of binomial coefficients. It quickly became clear that for even exponents, small primes occurred as divisors in a regular fashion (Proposition 3), and that this result could be extended (Proposition 7) to odd exponents and alternating sums. Further investigation revealed (Proposition 8) that for all alternating sums, the primes dividing $h_{2n,a}$ coincided with those dividing $\binom{2n}{n}$. This led us to conjecture, and subsequently to prove, Theorem 1: as part of our proof we obtain (Theorem 2) a corresponding result for q-binomial coefficients.

3. NON-ALTERNATING SUMS

Proposition 3. *For every integer $m \geq 1$, if p is a prime in the interval*

$$\frac{n}{m} < p < \frac{2a(n+1)-1}{2ma-1} = \frac{n+1}{m} + \frac{n+1-m}{m(2ma-1)}$$

then $p | f_{n,2a}$. In particular, $f_{n,2a}$ is divisible by all primes p for which

$$n < p < \frac{2a(n+1)-1}{2a-1} = n+1+\frac{n}{2a-1}.$$

The following lemma will enable us to convert information about divisors of $f_{n,a}$ which are greater than n into information about divisors less than n.

Lemma 4. *Let $n = n_s n_{s-1} ... n_2 n_1 n_0$ be the expansion of n in base p (and similarly for $k = k_s k_{s-1} ... k_2 k_1 k_0$). Then*

$$f_{n,a} \equiv \prod_{i=0}^{s} f_{n_i,a} \ (\text{mod } p).$$

Proof: By Lucas' Theorem (see for example Granville [6]),

$$\binom{n}{k} \equiv \prod_{i=0}^{s} \binom{n_i}{k_i} \pmod{p}$$

where as usual, $\binom{n_i}{k_i} \equiv 0 \pmod{p}$ if $k_i > n_i$. Hence all the terms in the sum over k for which $k_i > n_i$ for some i disappear, giving

$$\begin{aligned} f_{n,a} &= \sum_{k=0}^{n} \binom{n}{k}^a \\ &\equiv \sum_{k_s=0}^{n_s} \sum_{k_{s-1}=0}^{n_{s-1}} \cdots \sum_{k_0=0}^{n_0} \prod_{i=0}^{s} \binom{n_i}{k_i}^a \pmod{p} \\ &\equiv \prod_{i=0}^{s} \sum_{k_i=0}^{n_i} \binom{n_i}{k_i}^a \pmod{p} \\ &\equiv \prod_{i=0}^{s} f_{n_i,a} \pmod{p} \end{aligned}$$

as claimed. □

Corollary 5. *If $l < p$ and $p | f_{l,a}$ then $p | f_{l+jp,a}$ for all positive integers j.*

We are now in a position to prove Proposition 3: we proceed in two stages: first, the case when $n < p$.

Lemma 6. *Let p be a prime in the interval $n < p < \frac{2a(n+1)-1}{2a-1}$. Then $p | f_{n,2a}$.*

Proof: Let $p = n + r$ where $r > 0$. Then we have

$$\begin{aligned} f_{n,2a} = \sum_{k=0}^{n} \binom{n}{k}^{2a} &\equiv \sum_{k=0}^{p-r} \binom{p-r}{k}^{2a} \pmod{p} \\ &\equiv \sum_{k=0}^{p-r} \binom{r+k-1}{k}^{2a} (-1)^{2ka} \pmod{p} \\ &\equiv \sum_{k=0}^{p-r} \binom{r+k-1}{k}^{2a} \pmod{p} \\ &\equiv \sum_{k=0}^{p-r} \left(\frac{(k+1)(k+2)\dots(k+r-1)}{(r-1)!} \right)^{2a} \pmod{p}. \end{aligned}$$

Writing $x_{(0)} = 1$ and $x_{(r)}$ for the polynomial $x(x+1)\dots(x+r-1)$ this last sum becomes

$$\sum_{k=0}^{p-r} \left(\frac{(k+1)_{(r-1)}}{(r-1)!} \right)^{2a}.$$

We now observe that the polynomials $x_{(0)}, x_{(1)}, \dots x_{(d)}$ form an integer basis for the space of all integer polynomials of degree at most d. Hence there exist integers $c_0, c_1, \dots c_{(r-1)(2a-1)}$ so that

$$((k+1)_{(r-1)})^{2a-1} = \sum_{j=0}^{(r-1)(2a-1)} c_j (k+r)_{(j)}.$$

Thus

$$\begin{aligned} f_{n,2a} &\equiv \frac{1}{(r-1)!^{2a}} \sum_{k=0}^{p-r} \sum_{j=0}^{(r-1)(2a-1)} c_j \ (k+1)_{(r-1)} \ (k+r)_{(j)} \\ &\equiv \frac{1}{(r-1)!^{2a}} \sum_{j=0}^{(r-1)(2a-1)} \sum_{k=0}^{p-r} c_j \ (k+1)_{(r+j-1)} \\ &\equiv \frac{1}{(r-1)!^{2a}} \sum_{j=0}^{(r-1)(2a-1)} c_j \frac{(p-r+1)_{(r+j)}}{r+j}. \end{aligned}$$

Now, if $r + (r-1)(2a-1) < p$, then each of the terms in the sum is divisible by p, and $(r-1)!$ is not divisible by p: hence $f_{n,2a}$ is divisible by p. But

$$r + (r-1)(2a-1) = 2ra - 2a + 1 = 2pa - 2na - 2a + 1$$

and

$$2pa - 2na - 2a + 1 < p$$

if and only if

$$p < \frac{2a(n+1)-1}{2a-1}$$

completing the proof of the lemma. □

Now, suppose that $n = (m-1)p + l$ with $l > 0$ and

$$l < p < \frac{2a(l+1)-1}{2ma-1}.$$

Then by lemma 6, p divides $f_{l,2a}$ and hence by corollary 5, p divides $f_{n,2a}$. But $l < p$ if and only if $n < mp$, and

$$p < \frac{2a(l+1)-1}{2a-1}$$

if and only if

$$p < \frac{2a(n-(m-1)p)-1}{2a-1}$$

that is if

$$p < \frac{2a(n+1)-1}{2ma-1}.$$

Thus, if

$$\frac{n}{m} < p < \frac{2a(n+1)-1}{2ma-1}$$

then p divides $f_{n,2a}$, completing the proof of Proposition 3. $\square$

4. Alternating Sums

We note that no similar result holds for the case of odd powers of binomial coefficients (with the trivial exception of a=1). Indeed, except for the power of 2 dividing $f_{n,2a+1}$ (which we discuss in Lemma 12), the factorizations of sums of odd powers seem to exhibit no structure: for example,

$$f_{28,3} = 2^6.661.3671.5153.313527009031.$$

However, for alternating sums of odd powers, we have

Proposition 7. *p divides $h_{2n,2a+1}$ for primes in the intervals*

$$\frac{n}{m} < p < \frac{(2a+1)(n+1)-1}{m(2a+1)-1} = \frac{n+1}{m} + \frac{n+1-m}{m(2a+1)-1}$$

Proof: indeed by examining the proof of Proposition 3, we see that if we define

$$g_{n,a} = \sum_{k=0}^{n} \left((-1)^k \binom{n}{k} \right)^a$$

so that $g_{n,2a} = f_{n,2a}$ and $g_{n,2a+1} = h_{n,2a+1}$, then $g_{n,a}$ is divisible by all primes in each of the intervals

$$\frac{n}{m} < p < \frac{(n+1)a-1}{ma-1}$$

so Propositions 3 and 7 are really the same result. $\square$

For all alternating sums we have

Proposition 8. *If $p|\binom{2n}{n}$ then $p|h_{2n,a}$.*

Proof: Clearly 2 divides $h_{2n,a}$ if and only if 2 divides the middle term, $\binom{2n}{n}^a$, as all of the other terms cancel (mod 2). Since 2 divides $\binom{2n}{n}$, 2 divides $h_{2n,a}$.

Now let p be an odd prime dividing $\binom{2n}{n}$: we will show that p divides $h_{2n,a}$. By Kummer's theorem, at least one of the "digits" of $2n$ written in base p is odd (since if all are even, then there are no carries in computing $n+n=2n$ in base p). Let the digits of $2n$ in base p be $(2n)_s, (2n)_{s-1}, \ldots (2n)_1, (2n)_0$. Then as in Lemma 4

$$\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}^a \equiv \prod_{i=0}^{s}\left(\sum_{k_i=0}^{(2n)_i}(-1)^{k_i}\binom{(2n)_i}{k_i}^a\right)$$

(since p is odd, $(-1)^k=(-1)^{k_0+k_1+\ldots k_s}$). Now, since $p|\binom{2n}{n}$, at least one of the digits of $2n$ in base p is odd: but then the corresponding term in the product is zero, and so $p|h_{2n,a}$, completing the proof of Proposition 8. □

After computing some examples, it is natural to conjecture (and then, of course, to prove!) Theorem 1.

5. THE MAIN THEOREMS

We will prove Theorem 1 by considering $q-$binomial coefficents.

Definitions: Let n be a positive integer: throughout we will denote the number of 1's in the binary expansion of n by $l(n)$ (so that $2^{l(n)}||\binom{2n}{n}$): we further define the following polynomials in an indeterminate q:

$$\theta_n(q)=\frac{1-q^n}{1-q}=1+q+q^2+\cdots+q^{n-1}$$

(the q-equivalent of n)

$$\phi_n(q)=\prod_{d|n}(1-q^d)^{\mu(\frac{n}{d})}$$

(the n^{th} cyclotomic polynomial in q),

$$n!_q=\prod_{i=1}^{n}\theta_i(q)$$

(the q-equivalent of $n!$), and

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{n!_q}{k!_q(n-k)!_q}$$

(the q-equivalent of $\binom{n}{k}$).

Further, define

$$r(x,q)=\prod_{j\le x}\left(1-q^j\right)=(1-q)^n n!_q$$

$$s(x,q)=\prod_{2j+1\le x}\left(1-q^{2j+1}\right)$$

and

$$t(n,q)=\frac{s(n,q)}{s(\frac{n}{2},q)s(\frac{n}{4},q)s(\frac{n}{8},q)\ldots}.$$

Note that the apparently infinite product in the denominator is in fact finite, since $s(x, q) = 1$ if $x < 1$. We now make some useful observations about $t(n, q)$. First,

$$s(n, q) = \frac{r(n, q)}{r(\frac{n}{2}, q^2)}$$

so

$$\begin{aligned} t(n, q) &= \frac{s(n, q)}{s(\frac{n}{2}, q)^2} \; \frac{s(\frac{n}{2}, q)}{s(\frac{n}{4}, q)^2} \; \frac{s(\frac{n}{4}, q)}{s(\frac{n}{8}, q)^2} \; \frac{s(\frac{n}{8}, q)}{s(\frac{n}{16}, q)^2} \quad \cdots \\ &= \frac{\dfrac{r(n, q)}{r(\frac{n}{2}, q)^2} \; \dfrac{r(\frac{n}{2}, q)}{r(\frac{n}{4}, q)^2} \; \dfrac{r(\frac{n}{4}, q)}{r(\frac{n}{8}, q)^2}}{\dfrac{r(\frac{n}{2}, q^2)}{r(\frac{n}{4}, q^2)^2} \; \dfrac{r(\frac{n}{4}, q^2)}{r(\frac{n}{8}, q^2)^2} \; \dfrac{r(\frac{n}{8}, q^2)}{r(\frac{n}{16}, q^2)^2}} \cdots \\ &= \frac{r(n, q)}{r(\frac{n}{2}, q)^2} \; \frac{\dfrac{r(\frac{n}{2}, q)}{r(\frac{n}{4}, q)^2}}{\dfrac{r(\frac{n}{2}, q^2)}{r(\frac{n}{4}, q^2)^2}} \; \frac{\dfrac{r(\frac{n}{4}, q)}{r(\frac{n}{8}, q)^2}}{\dfrac{r(\frac{n}{4}, q^2)}{r(\frac{n}{8}, q^2)^2}} \; \frac{\dfrac{r(\frac{n}{8}, q)}{r(\frac{n}{16}, q)^2}}{\dfrac{r(\frac{n}{8}, q^2)}{r(\frac{n}{16}, q^2)^2}} \quad \cdots \end{aligned}$$

where again, the apparently infinite product is in fact finite.

Now, since

$$\frac{\dfrac{r(x, q)}{r(\frac{x}{2}, q)^2}}{\dfrac{r(x, q^2)}{r(\frac{x}{2}, q^2)^2}} \longrightarrow \begin{cases} 1 & \lfloor x \rfloor \text{ even} \\ \frac{1}{2} & \lfloor x \rfloor \text{ odd} \end{cases}$$

as $q \longrightarrow 1$, we see that

$$\lim_{q \to 1} t(2n, q) = \frac{\binom{2n}{n}}{2^l}.$$

Further, $t(2n + 1, q)$ has a factor $(q - 1)$, so

$$\lim_{q \to 1} t(2n + 1, q) = 0.$$

In other words, since $2^l || \binom{2n}{n}$, we may regard $t(2n, q)$ as the q-equivalent of the largest odd factor of $\binom{2n}{n}$.

Lemma 9.

$$t(n, q) \quad = \quad \prod_m{}' \phi_m(q)$$

where the product is over those odd m for which $\lfloor \frac{n}{m} \rfloor$ is odd.

Proof: Clearly, if m is even then $\phi_m(q)$ doesn't divide $t(n, q)$. Suppose m is odd: then $\phi_m(q)$ divides $s(n, q)$ exactly $\lceil \lfloor \frac{n}{m} \rfloor / 2 \rceil$ times, and hence $\phi_m(q)$ divides $t(n, q)$

$$\left\lceil \left\lfloor \frac{n}{m} \right\rfloor /2 \right\rceil - \left\lceil \left\lfloor \frac{n}{2m} \right\rfloor /2 \right\rceil - \left\lceil \left\lfloor \frac{n}{4m} \right\rfloor /2 \right\rceil - \cdots - \left\lceil \left\lfloor \frac{n}{2^j m} \right\rfloor /2 \right\rceil - \cdots$$

times. Now, by considering the binary expansion of $\lfloor \frac{n}{m} \rfloor$, it is immediate that this is 0 if $\lfloor \frac{n}{m} \rfloor$ is even, and 1 if $\lfloor \frac{n}{m} \rfloor$ is odd. □

Lemma 10. *Let m, n, k be non-negative integers: and write*

$$n = n''m + n'$$
$$k = k''m + k'$$
$$(n-k) = (n-k)''m + (n-k)'$$

where n', k' are the least non-negative residues of n, k (mod m). Then

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \equiv \begin{bmatrix} n' \\ k' \end{bmatrix}_q \binom{n''}{k''} \quad \textit{(mod } \phi_m(q)\textit{)}$$

where $\left[\begin{smallmatrix} n' \\ k' \end{smallmatrix}\right]_q$ is taken to be 0 if $n' < k'$.

Proof: We consider polynomials modulo $\theta_n(q)$ and $\phi_n(q)$. First, observe that

$$m \equiv m' \pmod{n}$$

if and only if

$$1 - q^m \equiv 1 - q^{m'} \pmod{1 - q^n},$$

that is,

$$\theta_m(q) \equiv \theta_{m'}(q) \pmod{\theta_n(q)},$$

if and only if

$$\theta_m(q) \equiv \theta_{m'}(q) \pmod{\phi_n(q)}.$$

Now,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{r(n,q)}{r(k,q)r(n-k,q)}$$

and reducing those terms which are coprime to $\phi_m(q)$ we obtain

$$r(m-1,q)^{n''-k''-(n-k)''} \frac{r(n',q)}{r(k',q)r((n-k)',q)} \frac{r(n'',q^m)}{r(k'',q^m)r((n-k)'',q^m)}.$$

Now, $n' = k' + (n-k)'$ then $n'' - k'' - (n-k)'' = 0$, and

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \equiv \begin{bmatrix} n' \\ k' \end{bmatrix}_q \frac{r(n'',q^m)}{r(k'',q^m)r((n-k)'',q^m)} \pmod{\phi_m(q)}$$
$$\equiv \begin{bmatrix} n' \\ k' \end{bmatrix}_q \binom{n''}{k''} \pmod{\phi_m(q)}$$

since $\theta_{jm}(q) \equiv j \pmod{(1 - q^m)}$, and hence $\pmod{\phi_m(q)}$.

If $n' + m = k' + (n-k)'$, then $n'' - k'' - (n-k)'' = 1$, and

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \equiv 0 \pmod{\phi_m(q)},$$

and since $k' > n'$, we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \equiv \begin{bmatrix} n' \\ k' \end{bmatrix}_q \binom{n''}{k''} \pmod{\phi_m(q)}$$

as required. □

We note that evaluating $\begin{bmatrix} n \\ k \end{bmatrix}_q$ at $q = 1$ immediately implies Kummer's theorem, since $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is a product of cyclotomic polynomials, and since $\phi_m(1) = p$ if $m = p^i$ and 1 otherwise, we have a factor of p corresponding to each position for which there is a carry in $n = k + (n - k)$ base p.

We are grateful to Professor Ira Gessel for informing us that Lemma 10 appears without proof as a property of q-binomial coefficients in [7], as Proposition 2.2 in [4] and as Remark 2.4 in [3].

Proof of Theorem 2: It is enough to show that if m and $n'' = \lfloor \frac{n}{m} \rfloor$ are odd, then

$$\phi_m(q) \quad | \sum_{k=0}^{n} \quad \begin{bmatrix} n \\ k \end{bmatrix}_q^a (-1)^k q^{jk}.$$

But, from Lemma 10,

$$\begin{aligned} \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^a (-1)^k q^{jk} &\equiv \sum_{k'=0}^{n'} \sum_{k''=0}^{n''} \begin{bmatrix} n' \\ k' \end{bmatrix}_q^a \binom{n''}{k''}^a (-1)^{k'+k''} q^{jk'} \pmod{\phi_m(q)} \\ &= \left(\sum_{k'=0}^{n'} \begin{bmatrix} n' \\ k' \end{bmatrix}_q^a (-1)^{k'} q^{jk'} \right) \left(\sum_{k''=0}^{n''} \binom{n''}{k''}^a (-1)^{mj} \right) \end{aligned}$$

and since m and n'' are odd, the second sum is zero, and we are done. $\square$

We observe now that both sides of Theorem 2 are integer polynomials; thus when we evaluate them at $q = 1$, the left hand side (if non-zero) will divide the right hand side. But we have already observed that $t(2n, 1) = \binom{2n}{n}/2^l$, and hence we have proved

Corollary 11.

$$\binom{2n}{n} \quad | \quad 2^{l(n)} \sum_{k=0}^{2n} \binom{2n}{k}^a (-1)^k.$$

$\square$

To prove Theorem 1 it remains to show that

$$2^{l(n)} \quad | \quad \sum_{k=0}^{2n} \binom{2n}{k}^a (-1)^k.$$

We prove a stronger result by induction.

Lemma 12. *For all positive integers a and n,*

$$2^{l(n)} \quad | \quad \sum_{k=0}^{n} \binom{n}{k}^a.$$

and

$$2^{l(n)} \quad | \quad \sum_{k=0}^{n} \binom{n}{k}^a (-1)^k.$$

Proof: The theorem is clearly true when $n = 1$: assume now that it it holds for all values less than n. For each $1 \le i \le l(n)$, let $m = 2^i$ and let $n', n'', k', k'', (n-k)', (n-k)''$ be defined as in Lemma 10: writing

$$w_i(q) = \left(\sum \begin{bmatrix} n' \\ k' \end{bmatrix}_q^a \right) \left(\sum \binom{n''}{k''}^a \right)$$

we have

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^a \equiv w_i(q) \pmod{\phi_{2^i}(q)}$$

By our induction hypothesis, since $l(n) = l(n') + l(n'')$, $2^{l(n)} | w_i(1)$ for each i.

We now wish to combine these equivalences modulo

$$\theta_{2^{l(n)}}(q) = \phi_2(q)\phi_4(q)\phi_8(q)\dots\phi_{2^{l(n)}}(q)$$

and evaluate them at $q = 1$. To do this, define

$$\pi_1 = \frac{1}{2^{l-1}}$$

and

$$\pi_i = \frac{1}{2^{l-i+1}}(1-q)$$

for $i = 2, 3, \dots, l(n)$. Then, setting

$$u_i(q) = \phi_2(q)\phi_4(q)\dots\phi_{2^{i-1}}(q)\pi_i\phi_{2^{i+1}}(q)\dots\phi_{2^{l(n)}}(q)$$

we have

$$u_1(q) = \frac{1}{2^{l-1}}(1+q^2)(1+q^4)\dots(1+q^{2^{l(n)-1}}) \equiv 1 \pmod{(1+q)}$$

and for $i \geq 2$,

$$\begin{aligned} u_i(q) &\equiv \frac{1}{2^{l-i+1}}(1-q^2)(1+q^2)(1+q^4)\dots(1+q^{2^{i-2}})(1+q^{2^i})\dots(1+q^{2^{l(n)-1}}) \\ &\equiv \frac{1}{2^{l-i+1}}(1-q^{2^{i-1}})(1+q^{2^i})(1+q^{2^{i+1}})\dots(1+q^{2^{l(n)-1}}) \\ &\equiv 1 \pmod{(1+q^{2^{i-1}})} \end{aligned}$$

Further, if $i \neq j$,

$$u_i(q) \equiv 0 \ (\text{mod } \phi_{2^j}(q)).$$

Hence,

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^a \equiv \sum_{i=1}^{l(n)} w_i(q)u_i(q) \qquad (\text{ mod } \theta_{2^{l(n)}}(q))$$

that is,

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^a = P(q)\theta_{2^{l(n)}}(q) + \sum_{i=1}^{l(n)} w_i(q)u_i(q)$$

where we wish to conclude that $P(q)$ is an integer polynomial. Observe that it is sufficient to prove that each $w_i(q)u_i(q)$ is an integer polynomial, since $\theta_{2^l}(q)$ is monic.

To do this, consider $w_i(q)$: first, observe that $w_i(q)$ is divisible by $2^{l(n'')}$ by our inductive hypothesis, since $n'' < n$: further, if n is odd, so is n', and hence the q-binomial sum in $w_i(q)$ is symmetric and its coefficients are even: if n is even, then $l(n') \leq i-1$, and in each case, $2^{l-i} | w_i(q)$ (that is, each coefficient of $w_i(q)$ is divisible by 2^{l-i+1}). Thus, for each i, $w_i(q)u_i(q)$ is an integer polynomial.

We have thus proven that

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q^a = P(q)\theta_{2^{l(n)}}(q) + \sum_{i=1}^{l(n)} w_i(q)u_i(q)$$

where $P(q)$ has integer coefficients. Now, setting $q = 1$ in both sides, we observe that $u_i(1)$ is an integer for each i, $2^{l(n)} | w_i(1)$ for each i (indeed, $u_i(1) = 0$ for $i \geq 2$, and $u_1(1) = 1$), and that $\theta_{2^{l(n)}}(1) = 2^{l(n)}$. Hence each term on the right is divisible by $2^{l(n)}$, proving that

$$2^{l(n)} \quad | \quad \sum_{k=0}^{n} \binom{n}{k}^a .$$

To prove that

$$2^{l(n)} \quad | \quad \sum_{k=0}^{n} \binom{n}{k}^a (-1)^k$$

we proceed similarly, setting

$$v_i(q) = \left(\sum \begin{bmatrix} n' \\ k' \end{bmatrix}_q^a (-1)^k \right) \left(\sum \binom{n''}{k''}^a \right),$$

with the only major difference being in the proof that

$$\sum_{i=1}^{l(n)} v_i(q) u_i(q)$$

is an integer polynomial: in this case, if n is even, things work as above, and if n is odd, then we have n' is odd, and $v_i(q)$ is identically equal to 0. Note that we need to have already proven the Lemma for non-alternating sums to prove the alternating case. This completes the proof of Lemma 12 and thus of Theorem 1. $\square$

We gratefully acknowledge many informative discussions with Professors Jonathan M. Borwein, Ira Gessel, Andrew J. Granville and Herbert S. Wilf.

References

[1] *Neil J. Calkin*, A Curious Binomial Identity, Discrete Math 131 (1994), 335-337.

[2] *N. G. DeBruijn*, Asymptotic Methods in Analysis, (Dover, New York 1981).

[3] *Man-Duen Choi, George A. Elliott, and Noriko Yui*, Gauss polynomials and the rotation algebra, Inventiones Mathematicae 99 (1990), 225–246.

[4] *J. Désarménien*, Un analogue des congruences de Kummer pour les q-nombres d'Euler, Europ. J. Combin. 3 (1982), 19–28.

[5] *A. J. Granville*, Zaphod Beeblebrox's Brain and the Fify-ninth Row of Pascal's Triangle, American Math. Monthly 99 (1992), 318–331.

[6] *A. J. Granville*, The Arithmetic Properties of Binomial Coefficients Proceedings of the Organic Mathematics Workshop (1996) `http://www.cecm.sfu.ca/organics/papers/granville/index.html` (URL verified October 10, 1996).

[7] *Gloria Olive*, Generalized Powers, American Math Monthly 72 (1965), 619–627.

[8] *Marko Petkovšek, Herbert S. Wilf and Doron Zeilberger*, A=B, (A. K. Peters, Wellesley, Massachusetts, 1996).

SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GA 30332
E-mail address: `calkin@math.gatech.edu`