Chapter 36

The Power of a Prime That Divides a Generalized Binomial Coefficient

[Written with Herbert S. Wilf. Originally published in Journal für die reine und angewandte Mathematik **396** *(1989), 212–219.]*

The purpose of this note is to generalize the following result of Kummer [8, page 116]:

Theorem. *The highest power of a prime p that divides the binomial coefficient $\binom{m+n}{m}$ is equal to the number of "carries" that occur when the integers m and n are added in p-ary notation.*

For example, $\binom{88}{50}$ is divisible by exactly the 3rd power of 3, because exactly 3 carries occur during the ternary addition

$$(38)_{10} + (50)_{10} = (1102)_3 + (1212)_3 = (10021)_3 = (88)_{10}.$$

The main idea is to consider generalized binomial coefficients that are formed from an arbitrary sequence $\mathcal{C}$, as shown in (3) below. We will isolate a property of the sequence $\mathcal{C}$ that guarantees the existence of a theorem like Kummer's, relating divisibility by prime powers to carries in addition.

A special case of the theorem we shall prove describes the prime power divisibility of Gauss's generalized binomial coefficients [5, §5],

$$\binom{m+n}{m}_q = \frac{(1-q^{m+n})(1-q^{m+n-1})\dots(1-q^{m+1})}{(1-q^n)(1-q^{n-1})\dots(1-q)}, \tag{1}$$

a result that was found first by Fray [4].

Another special case gives a characterization of the highest power to which a given prime divides the "Fibonomial coefficients" of Lucas [9, §9],

$$\binom{m+n}{m}_{\mathcal{F}} = \frac{F_{m+n}F_{m+n-1}\dots F_{m+1}}{F_nF_{n-1}\dots F_1}, \tag{2}$$

where $\langle F_1, F_2, \ldots \rangle = \langle 1, 1, 2, 3, 5, 8, \ldots \rangle$ is the Fibonacci sequence. These coefficients are integers that satisfy the recurrence

$$\binom{m+n}{m}_{\mathcal{F}} = F_{m+1}\binom{m+n-1}{m}_{\mathcal{F}} + F_{n-1}\binom{m+n-1}{n}_{\mathcal{F}}.$$

Generalized Binomial Coefficients

Let $\mathcal{C} = \langle C_1, C_2, \ldots \rangle$ be a sequence of positive integers. We define $\mathcal{C}$-nomial coefficients by the rule

$$\binom{m+n}{m}_{\mathcal{C}} = \frac{C_{m+n}C_{m+n-1}\ldots C_{m+1}}{C_n C_{n-1}\ldots C_1} \tag{3}$$

for all nonnegative integers m and n.

Generalized coefficients of this kind have been studied by several authors. Bachmann [1, page 81], Carmichael [2, page 40], and Jarden and Motzkin [6] have given proofs that if the sequence $\mathcal{C}$ is formed from a three term recurrence

$$C_{j+1} = aC_j + bC_{j-1},$$

with starting values $C_1 = C_2 = 1$, and with integer a, b, then the $\mathcal{C}$-nomial coefficients are integers.

We are interested in the following questions: For a fixed prime p, what is the highest power of p that divides $\binom{m+n}{m}_{\mathcal{C}}$? And under what conditions on the sequence $\mathcal{C}$ is there an analog of Kummer's theorem?

Given integers m and n, let $d_m(n)$ be the number of positive indices $j \le n$ such that C_j is divisible by m. If p is prime and $x \ne 0$ is rational, let $\varepsilon_p(x)$ be the power by which p enters x, that is, the highest power by which p divides the numerator of x minus the highest power by which p divides the denominator. (Thus, x is an integer if and only if $\varepsilon_p(x) \ge 0$ for all p.)

Proposition 1. *The maximum power of a prime p that divides the $\mathcal{C}$-nomial coefficient $\binom{m+n}{m}_{\mathcal{C}}$ is*

$$\varepsilon_p\left(\binom{m+n}{m}_{\mathcal{C}}\right) = \sum_{k\ge 1}\bigl(d_{p^k}(m+n) - d_{p^k}(m) - d_{p^k}(n)\bigr). \tag{4}$$

Proof. We can write $\binom{m+n}{m}_{\mathcal{C}} = \Pi(m+n)/(\Pi(m)\Pi(n))$, where $\Pi(n) = C_1 C_2 \ldots C_n$. Now

$$\begin{aligned} \varepsilon_p\bigl(\Pi(n)\bigr) &= \sum_{j=1}^{n} \varepsilon_p(C_j) \\ &= \sum_{j=1}^{n} \sum_{k=1}^{\infty} [p^k \backslash C_j] \\ &= \sum_{k=1}^{\infty} \sum_{j=1}^{n} [p^k \backslash C_j] = \sum_{k \ge 1} d_{p^k}(n), \end{aligned}$$

where $[p^k \backslash C_j]$ denotes 1 if p^k divides C_j, otherwise 0. The result follows since

$$\varepsilon_p\left(\binom{m+n}{m}_{\mathcal{C}}\right) = \varepsilon_p\bigl(\Pi(m+n)\bigr) - \varepsilon_p\bigl(\Pi(m)\bigr) - \varepsilon_p\bigl(\Pi(n)\bigr). \qquad \square$$

Corollary 1. *If $d_k(m+n) \ge d_k(m) + d_k(n)$ for all positive k, m, and n, the $\mathcal{C}$-nomial coefficients are all integers.* $\square$

Regularly Divisible Sequences

We say that the sequence $\mathcal{C}$ is *regularly divisible* if it has the following property for each integer $m > 0$: Either there exists an integer $r(m)$ such that C_j is divisible by m if and only if j is divisible by $r(m)$, or C_j is never divisible by m for any $j > 0$. In the latter case we let $r(m) = \infty$. Notice that the d functions for a regularly divisible sequence have the simple form

$$d_m(n) = \left\lfloor \frac{n}{r(m)} \right\rfloor, \tag{5}$$

which satisfies the condition of Corollary 1. Therefore,

Corollary 2. *The $\mathcal{C}$-nomial coefficients corresponding to a regularly divisible sequence are all integers.* $\square$

Regularly divisible sequences can be characterized in another interesting way:

Proposition 2. *The sequence $\langle C_1, C_2, C_3, \ldots \rangle$ is regularly divisible if and only if*

$$\gcd(C_m, C_n) = C_{\gcd(m,n)}, \quad \text{for all } m, n > 0. \tag{6}$$

Proof. Assume first that $\mathcal{C}$ is regularly divisible, and let m and n be positive integers. If $g = \gcd(C_m, C_n)$, we know that m and n are divisible by $r(g)$, hence $\gcd(m,n)$ is divisible by $r(g)$, hence $C_{\gcd(m,n)}$ is divisible by g. Also $\gcd(m,n)$ is divisible by $r(C_{\gcd(m,n)})$, hence m and n are divisible by $r(C_{\gcd(m,n)})$, hence C_m and C_n are divisible by $C_{\gcd(m,n)}$, hence g is divisible by $C_{\gcd(m,n)}$. Therefore (6) holds.

Conversely, assume that (6) holds and that m is a positive integer. If some C_j is divisible by m, let $r(m)$ be the smallest such j. Then $\gcd(C_j, C_{r(m)})$ is divisible by m, hence $C_{\gcd(j,r(m))}$ is divisible by m, hence $\gcd(j, r(m)) = r(m)$ by minimality; we have shown that C_j is a multiple of m only if j is a multiple of $r(m)$. And if j is a multiple of $r(m)$ we have $\gcd(C_j, C_{r(m)}) = C_{r(m)}$, hence C_j is a multiple of m. Therefore $\mathcal{C}$ is regularly divisible. $\square$

The number $r(m)$ is traditionally called the *rank of apparition* of m in the sequence $\mathcal{C}$. If m' is a multiple of m, the rank $r(m')$ must be a multiple of $r(m)$ in any regularly divisible sequence. Thus, in particular, every prime p defines a sequence of positive integers

$$a_1(p) = r(p), \quad a_2(p) = r(p^2)/r(p), \quad a_3(p) = r(p^3)/r(p^2), \quad \ldots,$$

which either terminates with $a_k(p) = \infty$ for some k or continues indefinitely with $a_k(p) > 1$ for infinitely many k. Conversely, every collection of such sequences, defined for each prime p, defines a regularly divisible sequence $\mathcal{C}$.

Ideal Primes

We say that the prime p is *ideal* for a sequence $\mathcal{C}$ if $\mathcal{C}$ is regularly divisible and there is a number $s(p)$ such that the multipliers $a_2(p)$, $a_3(p)$, ... defined in the previous paragraph are

$$a_k(p) = \begin{cases} 1, & \text{if } 2 \le k \le s(p); \\ p, & \text{if } k > s(p). \end{cases} \tag{7}$$

Thus

$$r(p^k) = \begin{cases} r(p), & \text{if } 1 \le k \le s(p); \\ p^{k-s(p)} r(p), & \text{if } k \ge s(p). \end{cases} \tag{8}$$

Such primes lead to a Kummer-like theorem for generalized binomial coefficients:

Proposition 3. *Let p be an ideal prime for a sequence $\mathcal{C}$. Then the exponent of the highest power of p that divides the $\mathcal{C}$-nomial coefficient $\binom{m+n}{m}_{\mathcal{C}}$ is equal to the number of carries that occur to the left of the radix point when the rational numbers $m/r(p)$ and $n/r(p)$ are added in p-ary notation, plus an extra $s(p)$ if a carry occurs across the radix point itself.*

Proof. We use Proposition 1 and formula (5). If $1 \le k \le s(p)$ we have

$$d_{p^k}(m+n) - d_{p^k}(m) - d_{p^k}(n) = \left\lfloor \frac{m+n}{r(p)} \right\rfloor - \left\lfloor \frac{m}{r(p)} \right\rfloor - \left\lfloor \frac{n}{r(p)} \right\rfloor,$$

and this is 1 if and only if a carry occurs across the radix point when $m/r(p)$ is added to $n/r(p)$; otherwise it is 0. Similarly if $k > s(p)$,

$$\begin{aligned} &d_{p^k}(m+n) - d_{p^k}(m) - d_{p^k}(n) \\ &\qquad = \left\lfloor \frac{m+n}{p^{k-s(p)}r(p)} \right\rfloor - \left\lfloor \frac{m}{p^{k-s(p)}r(p)} \right\rfloor - \left\lfloor \frac{n}{p^{k-s(p)}r(p)} \right\rfloor, \end{aligned}$$

which is 1 if and only if a carry occurs $k - s(p)$ positions to the left of the radix point. □

Proposition 3 can be generalized in a straightforward way to multinomial coefficients (see Dickson [3]), in which case we count the carries that occur when more than two numbers are added.

If p is not ideal, a similar result holds, but we must use a mixed-radix number system with radices $a_2(p)$, $a_3(p)$, $a_4(p)$, $\ldots$.

Gaussian Coefficients

Fix an integer $q > 1$, and let $\mathcal{C}$ be the sequence

$$\langle q-1, q^2-1, q^3-1, \ldots \rangle.$$

Then the $\mathcal{C}$-nomial coefficients (3) are the Gaussian coefficients (1). It is well known that this sequence $\mathcal{C}$ is regularly divisible; the integer $r(m)$ is called the order of q modulo m, namely the smallest power j such that $q^j \equiv 1$ (modulo m). We denote this quantity $r(m)$ by $r_q(m)$.

If p is a prime that divides q, we have $r_q(p) = \infty$. On the other hand, every odd prime p that does not divide q is ideal for the sequence $\mathcal{C}$. (A proof of this well-known fact can be found, for example, in [7, Lemma 3.2.1.2P].) Therefore Proposition 3 leads to

Theorem 1. *Let $q > 1$ be an integer, and let p be an odd prime. If p divides q, it does not divide the Gaussian coefficient $\binom{m+n}{m}_q$ for any nonnegative m and n. Otherwise $\varepsilon_p\bigl(\binom{m+n}{m}_q\bigr)$ is equal to the number of carries that occur to the left of the radix point when $m/r_q(p)$ is added to $n/r_q(p)$ in p-ary notation, plus an additional $s_q(p) = \varepsilon_p(q^{r(p)} - 1)$ if there is a carry across the radix point itself.* □

For example, if $q = 2$ and $p = 7$ we have $r_2(7) = 3$ and $s_2(7) = 1$. If $m = 2$ and $n = 5$ we have $m/3 = (0.444\ldots)_7$ and $n/3 = (1.444\ldots)_7$. The sum is $(m+n)/3 = (2.222\ldots)_7$; a single carry has occurred at the radix point, and we ignore the (infinitely many) carries that occur to the right of the point. Sure enough, $\binom{7}{2}_2 = 2667$ is divisible by 7 but not by 7^2.

The fractions $m/r_q(p)$ and $n/r_q(p)$ are always of the repeating form $(\alpha.ddd\ldots)_p$, where $0 \le d < p - 1$, because $r_q(p)$ is a divisor of $p - 1$.

The case $p = 2$ is slightly special, but it can be handled by almost the same methods. Suppose $q > 1$ is odd. Then there is a unique $f > 1$ such that

$$q \equiv 2^f \pm 1 \pmod{2^{f+1}}.$$

If $q \equiv 2^f + 1$ we have $r_q(2) = r_q(2^2) = \cdots = r_q(2^f) = 1$, and $r_q(2^k) = 2^{k-f}$ for $k \ge f$; but if $q \equiv 2^f - 1$ we have $r_q(2) = 1$, $r_q(2^2) = \cdots = r_q(2^{f+1}) = 2$, and $r_q(2^k) = 2^{k-f}$ for $k > f$.

It follows that the highest power of 2 dividing $\binom{m+n}{m}_q$ is the number of carries when m is added to n in binary notation, plus $f - 1$ if m and n are both odd and if $q \equiv 2^f - 1 \pmod{2^{f+1}}$.

For example, if $q = 23$ we have $f = 3$, so we add $m + n$ in binary and count the carries, throwing in an extra $f - 1 = 2$ if there's a carry out of the rightmost bit position. If $q = 25$ again $f = 3$; but in this case $q \equiv 2^f + 1 \pmod{2^{f+1}}$, so the highest power of 2 dividing $\binom{m+n}{m}_{25}$ is the same as for the ordinary binomial coefficient $\binom{m+n}{m}$.

Fibonacci Coefficients

Now let's turn to the case where the generating sequence $\mathcal{C}$ is the sequence of Fibonacci numbers. This sequence satisfies (6), by a well-known theorem of Lucas [9, page 206]; so it is regularly divisible.

Let $r(p)$ be the least positive integer such that $p \backslash F_{r(p)}$. Then F_j is divisible by p if and only if j is divisible by $r(p)$; indeed it is well known [10] that the period of the Fibonacci sequence modulo p is either $r(p)$, $2r(p)$, or $4r(p)$. It is also well known (see, for example, exercise 3.2.2–11 in [7]) that every odd prime is ideal for the Fibonacci sequence. Special consideration of the prime 2 leads to our second main result:

Theorem 2. *The highest power of the odd prime p that divides the Fibonomial coefficient $\binom{m+n}{m}_{\mathcal{F}}$ is the number of carries that occur to the left of the radix point when $m/r(p)$ is added to $n/r(p)$ in p-ary notation, plus $\varepsilon_p(F_{r(p)})$ if a carry occurs across the radix point. The highest power of 2 that divides $\binom{m+n}{m}_{\mathcal{F}}$ is the number of carries that occur when $m/3$ is added to $n/3$ in binary notation, not counting carries to the right of the binary point, plus 1 if there is a carry from the 1's to the 2's position.* $\square$

A Cyclotomic Approach

Let us sketch one more proof of Kummer's theorem. This one uses a more powerful apparatus than necessary, but it also sheds additional light on the problem.

If we write $q^n - 1$ in factored form as a product of cyclotomic polynomials,

$$q^n - 1 = \prod_{d \backslash n} \Psi_d(q), \tag{9}$$

we obtain a factorization of Gaussian coefficients by substituting into the right side of (1) and cancelling common factors:

$$\binom{m+n}{m}_q = \prod_{h \in H(m,n)} \Psi_h(q), \tag{10}$$

where

$$H(m,n) = \{\, h \geq 1 \mid m \bmod h + n \bmod h \geq h \,\}.$$

If we now let $q \to 1$, the left side becomes the ordinary binomial coefficient. The right side becomes a product of well-known cyclotomic values,

$$\Psi_h(1) = \begin{cases} p, & \text{if } h = p^k \text{ is a prime power;} \\ 1, & \text{if } h \text{ is not a prime power.} \end{cases} \tag{11}$$

Thus each factor is either 1 or a single prime, and p occurs as often as there are powers of p in the set $H(m,n)$; this is easily seen to be the number of carries in the p-ary addition $m + n$.

A corollary of (10), obtained by matching the degrees, is an identity for Euler's function that we can state as follows: *Fix integers $m, n \geq 0$. The product mn is the sum of $\varphi(h)$, over all integers h for which a carry occurs out of the units position when adding $m + n$ in radix h.*

Some Determinants

The special properties of regularly divisible sequences allow us to evaluate some striking determinants. The genesis of these ideas was in the well-known result that

$$\det\bigl(\gcd(i,j)\bigr)_{i,j=1}^{n} = \varphi(1)\varphi(2)\ldots\varphi(n).$$

This identity was generalized in [12] to a theorem about determinants in semi-lattices, which we will quote here in just enough generality to cover the situation at hand. If f is any function of the positive integers, we have

$$\det\Bigl(f\bigl(\gcd(i,j)\bigr)\Bigr)_{i,j=1}^{n} = \prod_{m=1}^{n}\Biggl(\sum_{d\backslash m}\mu\Bigl(\frac{m}{d}\Bigr)f(d)\Biggr).$$

In view of (6), we find the following evaluation.

Proposition 4. *Let* $\langle C_1, C_2, \ldots\rangle$ *be a regularly divisible sequence. Then*

$$\det\bigl(\gcd(C_i,C_j)\bigr)_{i,j=1}^{n} = \prod_{m=1}^{n}\Biggl(\sum_{d\backslash m}\mu\Bigl(\frac{m}{d}\Bigr)C_d\Biggr). \qquad \square \tag{12}$$

If apply this result to the sequence $\langle q^j-1\rangle_{j=1}^{\infty}$, we encounter, on the right side for $m>1$, the quantity

$$M(m,q) = \sum_{d\backslash m}\mu\Bigl(\frac{m}{d}\Bigr)q^d, \tag{13}$$

which is well known to be the number of nonperiodic words of m letters, over an alphabet of q letters. Thus we have the remarkable identity

$$\det\bigl(\gcd(q^i-1,q^j-1)\bigr)_{i,j=1}^{n} = (q-1)\prod_{m=2}^{n}M(m,q). \tag{14}$$

Similarly we can apply (12) to the Fibonacci sequence, to find that

$$\det\bigl(\gcd(F_{qi},F_{qj})\bigr)_{i,j=1}^{n} = \prod_{m=1}^{n}\Biggl(\sum_{d\backslash m}\mu\Bigl(\frac{m}{d}\Bigr)F_{qd}\Biggr). \tag{15}$$

Is there a “natural” interpretation of the factors of this product?

Additional Remarks

We have derived our theorems for $\mathcal{C}$-nomial coefficients belonging to regularly divisible sequences, but similar theorems apply in more general situations. For example, we obtain a sequence satisfying the condition of Corollary 1 if we let

$$d_{p^k}(n) = \lfloor \alpha_p n / p^k \rfloor \tag{16}$$

for all primes p and all $k \geq 1$, where α_p is any real number such that $0 \leq \alpha_p \leq p$. Such sequences $\mathcal{C}$ are not regularly divisible, unless each α_p is either zero or p times the reciprocal of an integer. The highest power of p that divides $\binom{m+n}{m}_{\mathcal{C}}$ in such cases is the number of carries that occur to the left of the radix point when $\alpha_p m$ is added to $\alpha_p n$ in p-ary notation.

One special case of this construction occurs when $\alpha_p = 2$ for all p; then it turns out that $C_j = 2j(2j-1)$, and $\binom{m+n}{m}_{\mathcal{C}} = \binom{2m+2n}{2m}$.

Another interesting (and remarkable) case occurs when $\alpha_p = \phi^{-1} = (\sqrt{5}-1)/2$ for all p; then it turns out that $C_{\lceil \phi n \rceil} = n$ and $C_{\lceil \phi^2 n \rceil} = 1$ for all $n \geq 1$.

An ideal prime p is called *simple* if $s(p) = 1$; in such cases Proposition 3 reduces to counting the number of carries to the left of and at the radix point. Nonsimple primes exist for sequences of the form $q^j - 1$; for example $r_3(11) = 10$, and $3^{10} - 1 = 2^3 \cdot 11^2 \cdot 61$. Another example [11] is $q = 2$, $p = 1093$, $r_q(p) = 364$, $s_q(p) = 2$. But in the case of the Fibonacci sequence, calculations by Wall [11] have shown that all primes < 10000 are simple. Does the Fibonacci sequence have any nonsimple primes? Can one prove that it has infinitely many simple primes?

This research was supported in part by the National Science Foundation under grant CCR-86-10181 and in part by Office of Naval Research contracts N00014-87-K-0502 and N00014-85-K-0320.

References

[1] Paul Bachmann, *Niedere Zahlentheorie*, Volume 2 (Leipzig: Teubner, 1910).

[2] R. D. Carmichael, "On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$," *Annals of Mathematics* **15** (1913–1914), 30–70.

[3] L. E. Dickson, "Theorems on the residues of multinomial coefficients with respect to a prime modulus," *Quarterly Journal of Pure and Applied Mathematics* **33** (1902), 378–384.

[4] Robert D. Fray, “Congruence properties of ordinary and q-binomial coefficients,” *Duke Mathematical Journal* **34** (1967), 467–480.

[5] Carolo Friderico Gauß, “Summatio quarumdam serierum singularium,” *Commentationes societatis regiæ scientiarum Gottingensis recentiores* **1** (1808), 147–186. [The page numbers are taken from the Kraus reprint of 1970; in the original publication, each paper had its own page numbers beginning with page 1.] Reprinted in Gauss's *Werke* **2** (1863), 9–45.

[6] Dov Jarden and Theodor Motzkin, “The product of sequences with a common linear recursion formula of order 2,” *Riveon Lematematika* **3** (1949), 25–27, 38. Reprinted in Dov Jarden, *Recurring Sequences* (Jerusalem: Riveon Lematematika, 1958).

[7] Donald E. Knuth, *Seminumerical Algorithms*, Volume 2 of *The Art of Computer Programming* (Reading, Massachusetts: Addison–Wesley, 1969).

[8] E. E. Kummer, “Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen,” *Journal für die reine und angewandte Mathematik* **44** (1852), 93–146.

[9] Edouard Lucas, “Théorie des fonctions numériques simplement périodiques,” *American Journal of Mathematics* **1** (1878), 184–240.

[10] D. W. Robinson, “The Fibonacci matrix modulo m,” *Fibonacci Quarterly* **1**, 2 (April 1963), 29–36.

[11] D. D. Wall, “Fibonacci series modulo m,” *American Mathematical Monthly* **67** (1960), 525–532.

[12] Herbert S. Wilf, “Hadamard determinants, Möbius functions, and the chromatic number of a graph,” *Bulletin of the American Mathematical Society* **74** (1968), 960–964.