$$(20) \qquad 3a^2b + 5b^3 = 40,$$

and

$$(21) \qquad (a^3 + 15ab^2) + (3a^2b + 5b^3) = 80.$$

It is easy to see that (20) has only one solution given by $a = 0$ and $b = 2$. From this solution we find $x = (1/4)/(a^2 - 5b^2) = -5$ and hence $y = 0$. Since, by Theorem 1, (21) has no solution in integers, we have exactly one integral solution for $y^2 - 125 = x^3$, namely

$$x = -5, \; y = 0.$$

## REFERENCES


1. O. Hemer. "On the Diophantine Equation $y^2 - k = x^3$." Unpublished doctoral dissertation, Uppsala, 1952.
2. S. P. Mohanty. "On the Diophantine Equation $y^2 - k = x^3$." Unpublished doctoral dissertation, UCLA, 1971.
3. L. J. Mordell. "The Diophantine Equation $y^2 - k = x^3$." *Proc. London Math. Soc.* (2) 13 (1913):60-80.


*****

# A DIVISIBILITY PROPERTY CONCERNING BINOMIAL COEFFICIENTS


JÁNOS SURÁNYI

*University Eötvös L, H-1088 Budapest, Múzeum krt 6/8*


I

The following observation was made by P. Erdős. The exponent of 2 in the canonical decomposition[1] of

$$\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$$

is $3n$ for $n \geq 2$. He conjectured that this is always true.[2] I succeeded in proving his conjecture, which raised the analogous question for odd primes instead of 2.

For the solution of this problem, I can prove the following.

*Theorem:* The exponent of the prime number $p$ in the canonical decomposition of the difference

$$\binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}}$$

is

(i) $3n$ for $p = 2$,
(ii) $3n + 1$ for $p = 3$,
(iii) at least $3n + 2$ for $p > 3$.

More generally, I will investigate, for integers $K$, $M$ divisible by $p$ ($K = kp$, $M = mp$), the difference

$$A = A_p(K, M) = \binom{K}{M} - \binom{k}{m}.$$

By an algebraic transformation, we will be led to the following question: If $p$ is a prime and $m(p - 1)$ is even, which power of $p$ divides the sum

$$\sum_{j=1,\, p\nmid j}^{m(p-1)/2} \frac{\displaystyle\prod_{\substack{r=1 \\ p\nmid j}}^{(mp-1)/2} r(mp - r)}{j(mp - j)}\,?$$

---

[1] I.e., the decomposition into the product of powers of different prime numbers.

[2] Oral communication, July 1976.

We obtain a fairly good answer to this question. However, the determination of the exact value of the exponent for $p > 3$ seems to me as hopeless at present as deciding for which primes $(p - 1)! + 1$ is divisible by $p^2$.

II

Simplifying the factors divisible by $p$ of the numerator and denominator of $\binom{K}{M}$, we can write $A$ as follows:

$$A = \binom{K}{M} - \binom{k}{m} = \binom{k}{m}\left(\prod_{\substack{j=1\\ p\nmid j}}^{M-1} \frac{K-j}{M-j} - 1\right) = \binom{k}{m}\left\{\prod_{\substack{j=1\\ p\nmid j}}^{M-1} (K-j) - \prod_{\substack{j=1\\ p\nmid j}}^{M-1} j\right\}\Bigg/\prod_{\substack{j=1\\ p\nmid j}}^{M-1} j \tag{1}$$

The difference $D = D_p(K, M)$ within brackets can now be transformed.

If the number of factors $M - m = m(p - 1)$ is even, we arrange the "symmetrical" factors corresponding to values $j$ and $M - j$ in pairs and get

$$\begin{aligned} D &= \prod_{j=1,\, p\nmid j}^{(M-1)/2} (K-j)(K-M+j) - \prod_{j=1,\, p\nmid j}^{(M-1)/2} j(M-j) \\ &= \prod_{j=1,\, p\nmid j}^{(M-1)/2} (K(K-M) + j(M-j)) - \prod_{j=1,\, p\nmid j}^{(M-1)/2} j(M-j) \\ &= \sum_{r=1}^{m(p-1)/2} (K(K-M))^r B_r, \end{aligned} \tag{2}$$

where $B_r = B_r(p, M)$ denotes the following expression:

$$\sum_{\substack{1\le j_1<\cdots<j_\mu\le \frac{M-1}{2}\\ p\nmid j_s}} \prod_{s=1}^{\mu} j_s(M-j_s) \qquad \left(1 \le r \le \frac{m(p-1)}{2} - 1\right)$$

with $\mu = \frac{m(p-1)}{2} - r$; finally,

$$B_{\frac{m(p-1)}{2}} = 1.$$

III

If $m(p - 1)$ is odd, then the prime $p$ must be 2 and $m$ must be odd. In this case, we can proceed similarly after separating the middle factor corresponding to $j = m$ and obtain

$$\begin{aligned} D &= (K-m) \prod_{j=1,\, 2\nmid j}^{m-1} (K-j)(K-M+j) - m \prod_{j=1,\, 2\nmid j}^{m-1} j(M-j) \\ &= (K-m) \prod_{j=1,\, 2\nmid j}^{m-1} (K(K-M) + j(M-j)) - m \prod_{j=1,\, 2\nmid j}^{m-1} j(M-j) \\ &= (K-m) \sum_{r=1}^{(m-1)/2} (K(K-M)^r B_r \ + 2(k-m)) \prod_{j=1,\, 2\nmid j}^{m-1} j(M-j) \end{aligned}$$

where $B_r = B_r(2, M)$ denotes the expression:

$$\sum_{\substack{1\le j_1<\cdots<j_\mu\le m-1\\ 2\nmid j_s}} \prod_{s=1}^{\mu} j_s(M-j_s) \qquad \left(1 \le r \le \frac{m-1}{2} - 1\right)$$

with $\mu = \frac{m-1}{2} - r$; finally,

$$B_{\frac{m-1}{2}} = 1.$$

Here $K - m = 2k - m$ is odd because $m$ is now odd and each term of the sum is divisible by $K(K - M) = 4k(k - m)$, whereas the last term is an odd multiple of $2(k - m)$.

Returning to the expression (1), the denominator in the last form is odd for $p = 2$ (and for every prime $p$ relatively prime to $p$), so that the exponent of 2 in the canonical decomposition of $A$ is the sum of its exponent in the binomial coefficient $\binom{k}{m}$ and in $2(k - m)$.

IV

In the case when $m(p - 1)$ is even we are led to the determination of the exponent of $p$ in the canonical decomposition of $B_1(p, M)$, as indicated at the beginning. Let us write $M$ in the form $M = m_1 p$ where $a \geq 1$ and $p \nmid m_1$.

Each factor $j_s(m_1 p^a - j_s)$ of $B_1$ is congruent to the opposite of a square mod $p^a$, so each term of the sum is congruent to $(-1)^{\frac{m(p-1)}{2} - 1}$ times a square.

V

First we consider the case $p = 2$, $a \geq 2$. For $a = 2$, $B_1(2, 4) = 1$, by definition, and if $m_1 > 1$, then $B_1$ is the sum of $m_1$ odd integers; thus, $B_1$ is also odd.

Let us have $a \geq 3$ and $j_1$, $j_2$ be two odd integers with

$$0 \leq u2^{a-2} < j_1 < j_2 < (u + 1)2^{a-2}(\leq m_1 2^{a-1}).$$

The terms of $B_1$ belonging to $j_1$ and $j_2$ are incongruent mod $p^a$. Their difference is the product of a common odd factor of the two terms and of

(3) $$j_2(M - j_2) - j_1(M - j_1) = (j_2 - j_1)(M - j_1 - j_2).$$

(The common factor for any other prime $p$ is always coprime with $p$.)

Here both factors are even, one of them is not divisible by 4 because of

$$j_1 + j_2 - (j_2 - j_1) = 2j_1,$$

and none of them is divisible by $2^{a-1}$, as we have

$$0 < j_2 - j_1 < 2^{a-2}$$

and

$$u2^{a-1} < j_1 + j_2 < (u + 1)2^{a-1}.$$

Now the squares of the odd numbers of such an interval represent a system of all quadratic residues (coprime with $p^a$) because of

$$c^2 \equiv (2^{a-1} \pm c)^2 \equiv (2^a - c)^2 \pmod{2^a}.$$

The interval $[1, m_1 p^{a-1} - 1]$ consists of $2m_1$ intervals of length $2^{a-2}$; thus, we obtain

$$B_1(2, m_1 2^a) \equiv -2m_1 \left( \sum_{u=1}^{2^{a-2}} u^2 - 4 \sum_{u=1}^{2^{a-3}} u^2 \right) = - \frac{2^{a-2}(2^{a-1} - 1)m_1}{3} \pmod{2^a}.$$

The exponent of 2 in the canonical factorization of $B_1(2, m_1 2^a)$ is therefore $a - 2$, and this holds even for $a = 2$.

VI

In the case of an odd prime $p$, the terms corresponding to intervals of the length $p^a/2$ are pairwise incongruent modulo $p^a$; thus, they give complete systems of quadratic residues modulo $p^a$. Namely, $p > 2$, and

$$(0 \leq)\frac{u}{2} p^a < j_1 < j_2 < \frac{u + 1}{2} p^a \leq \frac{m_1}{2} p, \quad p \nmid j_1, j_2,$$

so both factors of (3) cannot be divisible by $p$ and none is divisible by $p^a$, because of

$$0 < j_2 - j_1 < \frac{1}{2} p^a, \; up^a < j_1 + j_2 < (u + 1)p^a.$$

Thus, we have in this case,

$$B_1(p, M) = (-1)^{\frac{m_1 p^{a-1}(p-1)}{2} - 1} m_1 \left( \sum_{u=1}^{(p^a - 1)/2} u^2 - p^2 \sum_{u=1}^{(p^{a-1} - 1)/2} u^2 \right)$$

*(continued)*

$$= \frac{(-1)^{\frac{m_1 p^{a-1}(p-1)}{2}-1}\, p^a(p^{2a-1}+1)(p-1)m_1}{24}, \qquad (\text{mod } p^a).$$

This means that the exponent of 3 in the canonical expansion of $B_1(3, m_1 3^a)$ $(3 \nmid m_1)$ is $a - 1$, and

$$p^a | B_1(p, m_1 p^a) \ (p \nmid m_1) \quad \text{for} \quad p > 3.$$

In the last case, we do not know, however, the exact exponent of $p$ in the canonical factorization of $B_1$.

VII

Returning to the difference

$$\binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}} = A_p(p^{n+1}, p^n) = \binom{p^n}{p^{n-1}} \left\{ \sum_{r=1}^{m(p-1)/2} \left(p^{2n+1}(p-1)\right)^r B_r \right\} \Bigg/ \prod_{j=1,\, p \nmid j}^{p^n-1} j,$$

we know that

$$\binom{p^n}{p^{n-1}} = p \prod_{j=1}^{p^{n-1}} \frac{p^n - j}{p^{n-j} - j}$$

is divisible by $p$ but not by $p^2$. Thus, the results concerning the divisibility of $B_1$ give immediately the results ennounced in the theorem. More generally, if

$$M = m_1 p^a,\ K = k_1 p^b,\ \min(a, b) = c,\ (p \nmid m_1, k_1), \text{ and } 2/M\left(1 - \frac{1}{p}\right),$$

then

$$p^{a+b+c+d}/D_p(K, M),$$

where

$$d = \begin{cases} -2 & \text{for } p = 2,\ a \geq 2, \\ -1 & \text{for } p = 3, \\ 0 & \text{for } p > 3. \end{cases}$$

As for $A_p(K, M)$, we have to multiply this by the power of $p$ in the factorization of $\binom{K}{M}$ which can be calculated by the theorem of Lagrange.

*****

## FORMATION OF GENERALIZED *F-L* IDENTITIES OF THE FORM $\sum_{r=1}^{n} r^{\bar{s}} F_{kr+m}$


GREGORY WULCZYN

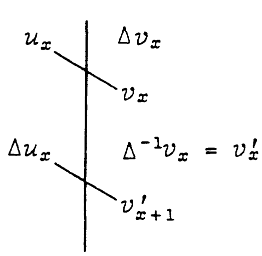
*Bucknell University, Lewisburg, PA 17837*


### PRELIMINARIES

$r^{\bar{s}} = r(r + 1) \cdots (r + s - 1)$. The various identities will be formed by using, if necessary, an iterated integration by parts formula for finite differences. $r^{\bar{s}}$ is convenient since $\Delta r^{\bar{s}} = s(r + 1)^{\overline{s-1}}$, $\Delta^2 r^{\bar{s}} = s(s - 1)(r + 2)^{\overline{s-2}}$, $\cdots$, $\Delta r^{\bar{s}} = s!$

$$\Delta^{-1}[u_x \Delta v_x] = u_x v_x - \Delta^{-1}[(\Delta u_x)(v_{x+1})].$$

This formula can be iterated:




*(continued)*