ON THE PRIME FACTORS OF $\binom{n}{k}$

P. ERDÖS
Hungarian Academy of Sciences, Budapest, Hungary
and
R. L. GRAHAM
Bell Laboratories, Murray Hill, New Jersey

A well known theorem of Sylvester and Schur (see [5]) states that for $n \geqslant 2k$, the binomial coefficient $\binom{n}{k}$ always has a prime factor exceeding k. This can be considered as a generalization of the theorem of Chebyshev: There is always a prime between m and $2m$. Set

$$\binom{n}{k} = u_n(k)v_n(k)$$

with

$$u_n(k) = \prod_{\substack{p^\alpha \| \binom{n}{k} \\ p<k}} p^\alpha, \qquad v_n(k) = \prod_{\substack{p^\alpha \| \binom{n}{k} \\ p \geq k}} p^\alpha .$$

In [4] it is proved that $v_n(k) > u_n(k)$ for all but a finite number of cases (which are tabulated there).

In this note, we continue the investigation of $u_n(k)$ and $v_n(k)$. We first consider $v_n(k)$, the product of the large prime divisors of $\binom{n}{k}$.

Theorem.

$$\max_{1 \leqslant k \leqslant n} v_n(k) = e^{\frac{n}{2}(1+o(1))}.$$

Proof. For $k < \epsilon n$ the result is immediate since in this case $\binom{n}{k}$ itself is less than $e^{n/2}$. Also, it is clear that the maximum of $v_n(k)$ is not achieved for $k > n/2$. Hence, we may assume $\epsilon n \leqslant k \leqslant n/2$. Now, for any prime

$$p \in \left(\frac{n-k}{r}, \frac{n}{r} \right]$$

with $p \geqslant k$ and $r \geqslant 1$, we have $p \mid v_n(k)$. Also, if $k^2 > n$ then $p^2 \nmid v_n(k)$ so that in this case the contribution to $v_n(k)$ of the primes

$$p \in \left(\frac{n-k}{r}, \frac{n}{r} \right]$$

is (by the Prime Number Theorem (PNT)) just $e^{\frac{k}{r}(1+o(1))}$. Thus, letting $\frac{n}{t+1} < k \leqslant \frac{n}{t}$, we obtain

$$v_n(k) = \exp\left[\left(\sum_{r=1}^{t-1} \frac{k}{r} + \left(\frac{n}{t} - k\right)\right)\right](1+o(1)) = \exp\left[\left(\frac{n}{t}\sum_{r=1}^{t-1} \frac{1}{r}\right)(1+o(1))\right]$$

$$\leqslant e^{\frac{n}{2}(1+o(1))}$$

and the theorem is proved.

It is interesting to note that since

$$\frac{n}{t}\sum_{r=1}^{t-1} \frac{1}{r} = \frac{1}{2}$$

for both $t = 2$ and $t = 3$ then

$$\lim_n v_n(k)^{1/n} = e^{1/2}$$

for any $k \in \left(\frac{n}{3}, \frac{n}{2}\right)$.

In Table 1, we tabulate the least value $k^*(n)$ of k for which $v_n(k)$ achieves its maximum value for selected values of $n \le 200$. It seems likely that infinitely often $k^*(n) = \frac{n}{2}$ but we are at present far from being able to prove this.

Table 1

n	$k^*(n)$	n	$k^*(n)$	n	$k^*(n)$
2	1	10	2	18	8
3	1	11	3	19	9
4	2	12	6	20	10
5	2	13	4	50	22
6	2	14	4	100	42
7	3	15	5	200	100
8	4	16	6		
9	2	17	7		

Note that

$$v_7(0) < v_7(1) < v_7(2) < v_7(3).$$

It is easy to see that for $n > 7$, the $v_n(k)$ cannot increase monotonically for $0 \le k \le \frac{n}{2}$.

Next, we mention several results concerning $u_n(k)$. To begin with, note that while $u_7(k) = 1$ for $0 \le k \le \frac{n}{2} = \frac{7}{2}$, this behavior is no longer possible for $n > 7$. In fact, we have the following more precise statement.

Theorem. For some $k \le (2 + o(1)) \log n$, we have $u_n(k) > 1$.

Proof. Suppose $u_n(k) = 1$ for all $k \le (2 + \epsilon) \log n$. Choose a prime $p < (1 + \epsilon) \log n$ which does not divide $n + 1$. Such a prime clearly exists (for large n) by the PNT. Since $p \nmid n + 1$ then for some k with $p < k < 2p$,

$$p^2 \mid n(n-1) \cdots (n-k+1), \quad p^2 \nmid k!$$

Thus, $p \mid u_n(k)$ and since

$$k < 2p < (2 + 2\epsilon) \log n,$$

the theorem is proved.

In the other direction we have the following result.

Fact. There exist infinitely many n so that for all $k \le (1/2 + o(1)) \log n$, $u_n(k) = 1$.

Proof. Choose $n + 1 = [\ell.\text{c.m.} \{1, 2, \cdots, t\}]^2$. By the PNT, $n = e^{(2+o(1))t}$. Clearly, if $m \le t$ then $m \nmid \binom{n}{t}$. Thus,

$$u_n(k) = 1 \quad \text{for} \quad k \le \left(\frac{1}{2} + o(1)\right) \log n$$

as claimed.

In Table 2 we list the least value $n^*(k)$ of n such that $u_n(i) = 1$ for $1 \le i \le k$

Table 2

k	$n^*(k)$
1	1
2	2
3	3
4	7
5	23
6	71

Of course, for $k \leqslant 2$, $u_n(k) = 1$ is automatic. By a theorem of Mahler [11], it follows that

$$u_n(k) < n^{1+\epsilon}$$

for $k \geqslant 3$ and large n. It is well known that if $p^\alpha \mid \binom{n}{k}$ then $p^\alpha \leqslant n$. Consequently,

$$u_n(k) \leqslant n^{\pi(k)},$$

where $\pi(k)$ denotes the number of primes not exceeding k. It seems likely that the following stronger estimate holds:

$$(*) \qquad u_n(k) < n^{(1+o(1))(1-\gamma)\pi(k)}, \quad k \geqslant 5,$$

where γ denotes Euler's constant. It is easy to prove (*) for certain ranges of k. For example, suppose k is relatively large compared to n, say, $k = n/t$ for a large fixed t. Of course, any prime $p \in (n - n/t, n)$ divides $v_n(k)$ and by the PNT

$$\prod_{n(1-1/t)<p<n} p = e^{(1+o(1))n/t}.$$

More generally, if $rp \in (n - n/t, n)$ with $r < t$ then $p \geqslant k$ and $p \mid v_n(k)$ so that again by the PNT

$$\prod_{\frac{n}{r}\left(1-\frac{1}{t}\right)<p<\frac{n}{r}} p = e^{(1+o(1))n/rt}.$$

Thus

$$v_n(k) \geqslant \prod_{1 \leqslant r<t} \prod_{\frac{n}{t}\left(1-\frac{1}{t}\right)<p<\frac{n}{r}} p = \exp\left((1+o(1)) \sum_{1\leqslant r<t} \frac{1}{r}\right)\frac{n}{t}$$

$$= \exp\left((1+o(1))(\log t + \gamma)\right)\frac{n}{t}.$$

But by Stirling's formula we have

$$\binom{n}{n/t} = e^{\frac{n}{t}\log t + \frac{n}{t} + o\left(\frac{n}{t}\right)}.$$

Thus,

$$u_n(k) = \binom{n}{k} / v_n(k) \leqslant e^{\frac{n}{t}\log t + \frac{n}{t} + o\left(\frac{n}{t}\right) - (1+o(1))(\log t + \gamma)\frac{n}{t}}$$

$$= e^{(1+o(1))(1-\gamma)\frac{n}{t}} = n^{(1+o(1))(1-\gamma)\pi(k)}$$

which is just (*).

In contrast to the situation for $v_n(k)$, the maximum value of $u_n(k)$ clearly occurs for $k \geqslant \frac{n}{2}$. Specifically, we have the following result.

Theorem. The value $\hat{k}(n)$ of k for which $u_n(k)$ assumes its maximum value satisfies

$$\hat{k}(n) = (1+o(1))\left(\frac{e}{e+1}\right) n.$$

Proof. Let $k = (1-c)n$. For $c \leqslant \tfrac{1}{2}$,

$$v_n(k) = \prod_{n-k<p\leqslant n} p = e^{(1+o(1))cn}.$$

Since

$$\binom{n}{k} = \binom{n}{cn} = e^{-(c\log c + (1-c)\log(1-c))(1+o(1))n}$$

then

$$u_n(k) = \binom{n}{k} / v_n(k) = e^{-(1+o(1))(c+\log c^c(1-c)^{1-c})n}.$$

A simple calculation shows that the exponent is maximized by taking $c = \frac{1}{e+1} = 0.2689\cdots$.

Concluding remarks. We mention here several related problems which were not able to settle or did not have time to investigate. One of the authors [8] previously conjectured that $\binom{2n}{n}$ is never squarefree for $n > 4$ (at present this is still open). Of course, more generally, we expect that for all α, $\binom{2n}{n}$ is always divisible by an α^{th} power of a prime $> k$ if $n > n_0(\alpha,k)$. We can show the much weaker result that $n = 23$ is the largest value of n for which *all* $\binom{n}{k}$ are squarefree for $0 \leqslant k \leqslant n$. This follows from the observation that if p is prime and $p^{\alpha} \nmid \binom{n}{k}$ for any k then $p^{\beta} | n+1$, where

$$p^{\beta} \geqslant \frac{n+1}{p^{\alpha}-1}\ .$$

Thus, $2^2 \nmid \binom{n}{k}$ for any k implies $2^{\beta} | n+1$ where $2^{\beta} \geqslant \frac{n+1}{3}$. Also, $3^2 \nmid \binom{n}{k}$ for any k implies $3^{\gamma} | n+1$ where $3^{\gamma} \geqslant \frac{n+1}{8}$. Together these imply that $d = 2^{\beta}3^{\gamma} | n+1$ where $d \geqslant (n+1)^2/24$. Since d cannot exceed $n+1$ then $n+1 \leqslant 24$ is forced, and the desired result follows.

For given n let $f(n)$ denote the largest integer such that for *some k*, $\binom{n}{k}$ is divisible by the $f(n)^{th}$ power of a prime. We can prove that $f(n) \to \infty$ as $n \to \infty$ (this is not hard) and very likely $f(n) > c \log n$ but we are very far from being able to prove this. Similarly, if $F(n)$ denotes the largest integer so that for *all k*, $1 \leqslant k < n$, $\binom{n}{k}$ is divisible by the $F(n)^{th}$ power of some prime, then it is quite likely that $\overline{\lim}\ F(n) = \infty$, but we have not proved this.

Let $P(x)$ and $p(x)$ denote the greatest and least prime factors of x, respectively. Probably

$$P\left(\binom{n}{k}\right) > \max\,(n-k,\ k^{1+\epsilon})$$

but this seems very deep (for related results see the papers of Ramachandra and others [11], [12]).

J. L. Selfridge and P. Erdös conjectured and Ecklund [1] proved that $p\left(\binom{n}{k}\right) < \frac{n}{2}$ for $k > 1$, with the unique exception of $p\left(\binom{7}{3}\right) = 5$. Selfridge and Erdös [9] proved that

$$p\left(\binom{n}{k}\right) < \frac{c_1 n}{k^{c_2}}$$

and they conjecture

$$p\left(\binom{n}{k}\right) < \frac{n}{k} \quad \text{for} \quad n > k^2\ .$$

Finally, let $d\left(\binom{n}{k}\right)$ denote the greatest divisor of $\binom{n}{k}$ not exceeding n. Erdös originally conjectured that $d\left(\binom{n}{k}\right) > n-k$ but this was disproved by Schinzel and Erdös [13]. Perhaps it is true however, that $d_n > cn$ for a suitable constant c.

For problems and results of a similar nature the reader may consult [2], [3], [6], [7] or [10].

REFERENCES

1. E. Ecklund, Jr., "On Prime Divisors of the Binomial Coefficients," *Pac. J. of Math.,* 29 (1969), pp. 267–270.
2. E. Ecklund, Jr., and R. Eggleton, "Prime Factors of Consecutive Integers," *Amer. Math. Monthly,* 79 (1972) pp. 1082–1089.
3. E. Ecklund, Jr., P. Erdös and J. L. Selfridge, "A New Function Associated with the Prime Factors of $\binom{n}{k}$, *Math. Comp.,* 28 (1974), pp. 647–649.
4. E. Ecklund, Jr., R. Eggleton, P. Erdös and J. L. Selfridge, "On the Prime Factorization of Binomial Coefficients," to appear.
5. P. Erdös, "On a Theorem of Sylvester and Schur," *J. London Math. Soc.,* 9 (1934), pp. 282–288.
6. P. Erdös, "Some Problems in Number Theory," *Computers in Number Theory, Proc. Atlas Symp.,* Oxford, 1969, Acad. Press (1971), pp. 405–414.

7. P. Erdös, "Über die Anzahl der Primzahlen-von $\binom{n}{k}$," *Archiv der Math.,* 24 (1973).
8. P. Erdös, "Problems and Results on Number Theoretic Properties of Consecutive Integers and Related Questions," *Proc. Fifth Manitoba Conf. on Numerical Mathematics* (1975), pp. 25–44.
9. P. Erdös and J. L. Selfridge, "Some Problems on the Prime Factors of Consecutive Integers," *Pullman Conf. on Number Theory,* (1971).
10. P. Erdös, R. L. Graham, I. Z. Ruzsa and E. G. Straus, "On the Prime Factors of $\binom{2n}{n}$," *Math Comp.,* 29 (1975), pp. 83–92.
11. K. Ramachandra, "A Note on Numbers with a Large Prime Factor II," *J. Indian Math. Soc.,* 34 (1970), pp. 39–48.
12. K. Ramachandra, "A Note on Numbers with a Large Prime Factor III," *Acta Arith.,* 19 (1971), pp. 49–62.
13. A. Schinzel, "Sur un Probleme de P. Erdös," *Coll. Math.,* 5 (1952), pp. 198–204.

****