MATH. SCAND. 39 (1976), 271–281

ON THE NUMBER OF PRIME DIVISORS OF A BINOMIAL COEFFICIENT

ERNST S. SELMER

1.

It must have been observed independently by many people that a binomial coefficient $\binom{n}{k}$ can never be a prime power except in the trivial cases with $k=1$ or $k=n-1$. Strangely enough, the first proof of this fact was apparently not published until 1968 by Hering [4]. Simpler proofs, all using the implication

$$p^a \Big| \binom{n}{k} \Rightarrow p^a \leqq n\,, \tag{1}$$

have later been given by Stahl [8], Scheid [6] and Mignotte [5].

For given $k>1$ and *sufficiently large* n, the binomial coefficient $\binom{n}{k}$ will always contain *at least k different prime divisors.* In what follows, the number of such divisors will be denoted by $V(n,k)$.

Bounds for n and k were discussed by Erdös [2], who also pointed out that if $V(n,k)<k$, then (1) implies that

$$\binom{n}{k} \leqq n^{k-1}\,. \tag{2}$$

Since the left hand side is a polynomial in n of degree k, we get a contradiction for sufficiently large n.

This particular argument was improved by Mignotte [5], who (without reference to Erdös) showed that $V(n,k)\geqq k$ if

$$n \geqq k!+k\,. \tag{3}$$

Since this condition may be written as

$$\binom{n}{k} > n(n-1)\ldots(n-k+2)\,,$$

we get an improvement over (2). The improvement is not significant in terms of the bounds involved, but (3) is of course much simpler to use.

Received August 6, 1975; in revised form June 16, 1976.

2.

We shall improve Mignotte's bound (3), and first give a simplified version of his argument: He showed that if

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_j^{\alpha_j}, \tag{4}$$

then each prime power $p_i^{\alpha_i}$ must divide one of the factors of the numerator (this is trivial only if $p_i > k$). If $j < k$, there is consequently one factor of the numerator which is a divisor of $k!$. In the "worst" case, we may have $n-k+1 = k!$, which immediately gives the bound (3).

If $n-i = k!$, $i < k-1$, one would get a slightly better bound (but of the same order of magnitude). We will, however, not try to establish any such insignificant improvement. It is the dominant term $k!$ of (3) which we shall reduce considerably.

Before doing so, we note the following fact (which was not pointed out by Mignotte): To obtain all cases (4) with $j < k$, it is not necessary to examine all $n < k!+k$, but *only those n where one of the factors*

$$n, n-1, \dots, n-k+1 \tag{5}$$

is a divisor of $k!$. This observation means a great reduction of the numerical work involved. As an example, consider $k = 5$, $k! = 120$. Starting from the top, it then suffices to consider the factorization of

$$\binom{n}{5}, \quad n = 120-124, 60-64, 40-44, 30-34, \dots .$$

It turns out that $n = 32$ is the largest n with $V(n, 5) < 5$.

The improvement of (3) is based on the following obvious observation: The factor, say K, in (5) which divides $k!$ contains only prime divisors $p \leqq k$. If p is small compared to k, then several of the numbers (5) will contain p as a divisor, possibly to varying powers. Removing such divisors from $k!$, we get a smaller bound for K.

This simple approach, combined with a certain amount of sophistication, leads to a proof of the following

THEOREM 1. *Let*

$$P(k) = \prod_{p^m \leqq k} p,$$

the product being taken over all primes p and all positive integers m. If the binomial coefficient $\binom{n}{k}$ *contains less than k different prime divisors, then one of the numbers*

$$n, n-1, \ldots, n-k+1$$

must be a divisor of $P(k)$. *In particular,* $\binom{n}{k}$ *will contain at least* k *different prime divisors if*

$$n \geqq P(k)+k\,. \tag{6}$$

We have thus replaced $k!$ of (3) by $P(k)$, which is of smaller order of magnitude. In fact,

$$\log P(k) = \sum_{p^m \leq k} \log p = \psi(k)\,,$$

the well known function from prime number theory. Since $\psi(k) \sim k$ by the prime number theorem, we have

$$P(k) = e^{k(1+o(1))}\,.$$

Let $n(k)$ denote the largest value of n such that $V(n,k)<k$. Erdös, Gupta and Khare [3] showed that for given $\varepsilon>0$, $n(k)<(e+\varepsilon)^k$ for sufficiently large k. Asymptotically, this yields the same result as our Theorem 1 (which is of course much more useful in numerical applications).

It was also stated in [3] that Erdös and Szemerédi (unpublished) have proved a slightly stronger result: There is an $\alpha<e$ such that $n(k)<\alpha^k$ for sufficiently large k.

A lower bound for $n(k)$ was also given in [4], in the form

$$\liminf_{k\to\infty} \frac{\log n(k)}{\log k} \geqq e\,.$$

This led the authors to assume that $n(k)$ might actually be of the order of magnitude k^e. In Section 4, we shall find further evidence supporting this assumption. Thus our new bound (6), which means a great improvement over (3), is probably still far too large.

3.

We now turn to a proof of Theorem 1. Let p denote an arbitrary prime $\leqq k$, and determine the exponent $\varkappa(p,k)$ by

$$p^{\varkappa(p,k)} \leqq k < p^{\varkappa(p,k)+1}$$

Then $P(k)$ can be written as

$$P(k) = \prod_{p\leq k} p^{\varkappa(p,k)}\,.$$

We assume that we have a factorization (4) with $j<k$. By Mignotte's argument, each prime power $p_i^{a_i}$ must divide at least *one* of the factors (5). For each p_i, we select a factor which is divisible by the *highest* power of p_i. There is then at least one "spare" factor in (5), which we denote by K, and which must divide $k!$. Note that some of the p_i may well divide K, but that there is always another factor in (5) which is divisible by p_i to at least the same power as is K.

To abbreviate, put $\varkappa(p,k)=\varkappa$. For any prime p such that

$$p^{\varkappa+1} \mid K\,, \tag{7}$$

p cannot divide any other factor in (5) to the same power (since (5) contains k consecutive integers, and $p^{\varkappa+1}>k$). Hence p cannot be any of the prime divisors p_i of $\binom{n}{k}$. On the other hand, we shall see that (7) implies

$$p \left| \binom{n}{k}\right., \tag{8}$$

a contradiction. Consequently $p^{\varkappa}$ is the highest power of p which can divide K, and we conclude that $K \mid P(k)$. The theorem will then be proved when we have established the contradiction (8).

Let $p^{\mu} \parallel k!$ ("exactly divide"), where

$$\mu = \left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\ldots+\left[\frac{k}{p^{\varkappa}}\right].$$

Let further $p^{\nu} \parallel n(n-1)\ldots(n-k+1)$. Since this product consists of k consecutive integers, it contains at least $[k/p]$ factors divisible by p, $[k/p^2]$ factors divisible by $p^2,\ldots$, until at least $[k/p^{\varkappa}]$ factors divisble by $p^{\varkappa}$, and finally one factor (namely K) divisible by at least $p^{\varkappa+1}$. Hence

$$\nu \geqq \left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\ldots+\left[\frac{k}{p^{\varkappa}}\right]+1 = \mu+1\,,$$

which implies (8).

4.

We shall consider a numerical application of Theorem 1. The reduction of calculations described in connection with (5) of course also applies when we use the smaller bound (6).

We have already introduced the notation $n(k)$ for the largest value of n such that $V(n,k)<k$. Let further K (defined as above) refer to this particular $V(n(k),k)$. Some preliminary numerical results for $k\leqq 15$ are given in Table 1. For larger values of k, there may be several of the numbers (5) dividing $P(k)$. For $k\leqq 15$, however, there is only one such number K for $n=n(k)$.

Table 1. *Comparison of* $k!$, $P(k)$ *and* $n(k)$ *for some small values of* k.

k	$P(k)$	$k!/P(k)$	$n(k)$	K	$P(k)/K$
2	2	1	3	2	1
3	$6 = 2\cdot 3$	1	8	6	1
4	$12 = 2^2\cdot 3$	2	14	12	1
5	$60 = 2^2\cdot 3\cdot 5$	2	32	30	2
6		12	62	60	1
7	$420 = 2^2\cdot 3\cdot 5\cdot 7$	12	87	84	5
8	$840 = 2^3\cdot 3\cdot 5\cdot 7$	48	169	168	5
9	$2\,520 = 2^3\cdot 3^2\cdot 5\cdot 7$	144	132	126	20
10		1 440	367	360	7
11	$27\,720 = 2^3\cdot 3^2\cdot 5\cdot 7\cdot 11$	1 440	389	385	72
12		17 280	510	504	55
13		17 280	394	390	924
14	$360\,360 = 2^3\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 13$	241 920	512	504	715
15		3 628 800	512	504	715

The quotient $k!/P(k)$ in Table 1 shows the improvement by (6) over (3), and the quotient $P(k)/K$ indicates how much the new bound (6) differs from the "best possible" result. The growth of $P(k)/K$ seems to confirm the belief, stated earlier, that the bound (6) is still too large.

Since Theorem 1 is such a strong tool in numerical applications, it was decided to extend Table 1. The necessary calculations were performed on the UNIVAC 1110 at the University of Bergen. I am greatly indebted to Svein Mossige for accurate and efficient programming of the problems.

The resulting Tables 2 and 3 represent many hours of computing time, on one of the world's fastest computers. To indicate its speed, we may mention that Mossige wrote a FORTRAN program which produced the complete factorization of all natural numbers $\leqq 10^5$ (the range of the British Association factor table) in 40 seconds!

The word length of UNIVAC 1110 allows for representation of integers $\lessapprox 3.4\cdot 10^{10}$. Since $P(27)$ exceeds this bound, a complete calculation based on Theorem 1 was performed only for $k \leqq 26$. The computation for each k started "from the top", determining the integral quotients $K = P(k)/i$, $i = 1, 2, 3, \ldots$, then forming the binomial coefficients $\binom{n}{k}$ with $K + k - 1 \geqq n \geqq K$, and stopping when a $V(n,k) < k$ was first obtained.

Since multiple precision calculations would require excessive computing times, we decided to "cheat" for $k \geqq 27$. The computation was then started "from the bottom", counting whether $V(n,k)$ was $< k$ or $\geqq k$, and stopping when a certain multiple of the last $n = n_0$ with $V(n_0, k) < k$ was reached. The bounds $10n_0$ and $5n_0$ were used for $27 \leqq k \leqq 50$ and $51 \leqq k \leqq 100$, respectively.

Table 2. *The largest $n=n(k)$ such that $\binom{n}{k}$ contains less than k distinct prime divisors (not completely guaranteed for $n \geqq 27$, cf. the text).*

k	$n(k)$	k	$n(k)$	k	$n(k)$	k	$n(k)$	k	$n(k)$
		21	1 885	41	10 667	61	25 002	81	67 248
2	3	22	2 102	42	10 667	62	26 263	82	61 682
3	8	23	3 470	43	10 668	63	24 714	83	55 859
4	14	24	3 470	44	11 710	64	34 520	84	61 685
5	32	25	4 805	45	11 711	65	33 365	85	61 685
6	62	26	4 806	46	12 799	66	33 366	86	65 600
7	87	27	4 806	47	12 800	67	33 367	87	74 771
8	169	28	3 475	48	12 799	68	33 780	88	74 771
9	132	29	4 806	49	15 673	69	36 497	89	74 772
10	367	30	4 938	50	20 365	70	36 498	90	74 776
11	389	31	4 939	51	20 366	71	40 047	91	65 606
12	510	32	5 108	52	20 367	72	36 497	92	75 997
13	394	33	5 119	53	20 369	73	38 345	93	113 196
14	512	34	6 271	54	20 369	74	40 050	94	113 198
15	512	35	5 122	55	20 187	75	41 215	95	113 198
16	1 880	36	5 869	56	20 187	76	44 235	96	113 200
17	1 880	37	10 663	57	26 959	77	44 285	97	113 201
18	1 882	38	10 663	58	26 959	78	40 047	98	113 201
19	2 099	39	10 663	59	26 960	79	44 285	99	102 485
20	1 879	40	7 421	60	23 814	80	46 459	100	111 863

We feel it is a safe bet to assume that the n_0 thus obtained is really $n(k)$, but we stress that this is not guaranteed by Theorem 1.

The resulting values of $n(k)$ for $k \leqq 100$ are listed in Table 2. In most cases, it turned out that $V(n(k), k) = k-1$, but $V(n(k), k) = k-2$ for $k = 88, 95$.

Erdös, Gupta and Khare [3] introduced the *smallest* number $n = n_k$ such that $V(n, k) \geqq k$, and tabulated n_k for $k \leqq 25$. They showed that for given $\varepsilon > 0$, $n_k > (1-\varepsilon)k^2 \log k$ for sufficiently large k, and that

$$\limsup_{k \to \infty} \frac{\log n_k}{\log k} \leqq e .$$

Since the necessary programs had already been developed by Mossige, we decided to put also the determination of n_k on the computer. The results for $k \leqq 200$ are given in Table 3 (no "cheating" was necessary here).

As in [3], denote by m_k the smallest number $n = m_k$ such that $V(n, k)$ *exactly* equals k. (The existence of m_k for all k has in fact not been proved.) Usually, of course, one would expect $m_k = n_k$. In the range of Table 3, we have the

Table 3. *The smallest* $n=n_k$ *such that* $\binom{n}{k}$ *contains at least* k *different prime divisors.*

k	n_k	k	n_k	k	n_k	k	n_k	k	n_k
1	2	41	1 834	81	11 585	121	35 697	161	72 851
2	4	42	2 147	82	11 586	122	35 719	162	72 854
3	9	43	2 263	83	12 327	123	39 353	163	72 855
4	10	44	2 519	84	12 939	124	41 410	164	81 548
5	22	45	2 519	85	13 642	125	43 362	165	72 855
6	26	46	3 021	86	14 171	126	35 723	166	92 596
7	40	47	3 306	87	14 174	127	41 410	167	92 597
8	50	48	3 306	88	15 622	128	41 410	168	93 685
9	54	49	3 427	89	16 827	129	41 410	169	90 161
10	55	50	3 441	90	16 827	130	43 365	170	93 686
11	78	51	3 445	91	16 836	131	43 365	171	93 692
12	115	52	3 820	92	16 837	132	44 448	172	95 794
13	123	53	4 075	93	18 551	133	43 371	173	101 106
14	154	54	3 445	94	19 367	134	44 429	174	99 333
15	155	55	4 350	95	20 257	135	44 429	175	102 379
16	209	56	4 560	96	20 257	136	44 454	176	96 730
17	288	57	4 346	97	20 305	137	44 455	177	96 730
18	220	58	4 347	98	20 304	138	51 832	178	102 383
19	221	59	4 348	99	20 304	139	44 457	179	105 205
20	292	60	5 071	100	18 410	140	44 457	180	106 168
21	301	61	5 568	101	20 305	141	51 837	181	106 169
22	378	62	6 006	102	20 304	142	55 282	182	108 490
23	494	63	6 767	103	20 305	143	55 283	183	108 491
24	494	64	5 786	104	20 305	144	57 541	184	108 491
25	551	65	5 786	105	20 305	145	58 008	185	112 056
26	715	66	6 772	106	23 506	146	60 010	186	112 056
27	670	67	7 316	107	26 611	147	58 014	187	112 057
28	786	68	7 833	108	26 572	148	62 891	188	112 058
29	805	69	7 429	109	27 069	149	62 937	189	112 065
30	803	70	8 385	110	26 574	150	58 017	190	112 066
31	1 079	71	8 387	111	27 265	151	62 894	191	128 757
32	966	72	8 388	112	27 267	152	62 894	192	128 781
33	1 190	73	8 654	113	28 274	153	69 746	193	112 066
34	1 222	74	9 744	114	31 919	154	66 316	194	128 783
35	1 274	75	10 064	115	32 338	155	66 309	195	112 066
36	1 274	76	11 259	116	32 339	156	66 309	196	128 782
37	1 276	77	10 557	117	32 337	157	66 310	197	128 783
38	1 771	78	11 573	118	33 467	158	72 850	198	144 989
39	1 836	79	11 583	119	35 697	159	72 851	199	144 991
40	1 807	80	11 583	120	35 696	160	72 850	200	128 785

following exceptions with $m_k > n_k$:

k	51	57	79	149	181	185
m_k	3 446	4 865	12 368	62 938	106 171	112 065

In all these cases, $V(n_k, k) = k+1$.

As already mentioned in Section 2, there are reasons to suspect that $n(k)$ might be of the order of manitude k^e, and similarly for n_k. To verify this, we have calculated $n(k)/k^e$ and n_k/k^e for the values of Tables 2 and 3. The results

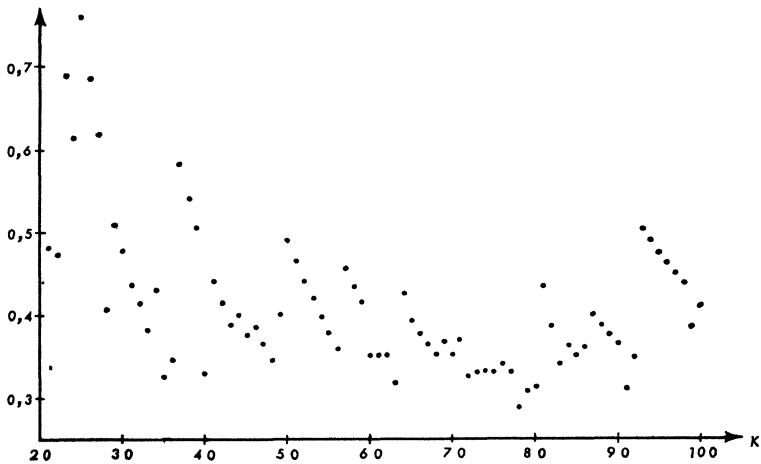

Diagram 1.
Values of $n(k)/k^e$ for $20 < k \leqq 100$.

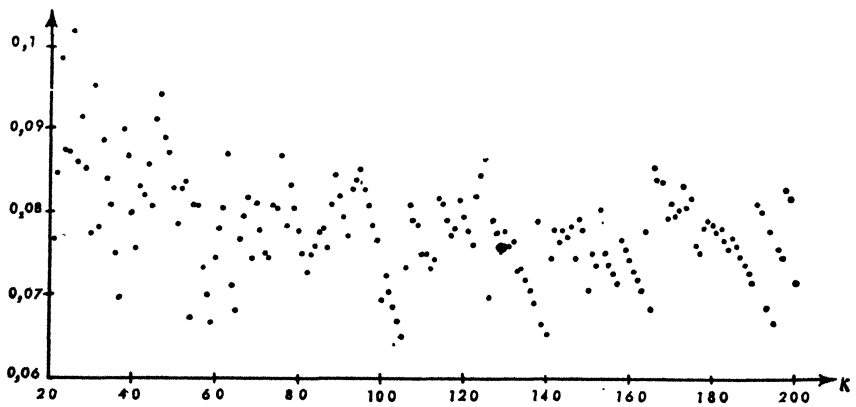

Diagram 2.
Values of n_k/k^e for $20 < k \leqq 200$.

are plotted in Diagrams 1 and 2, which seem to confirm the suspicion. As a matter of fact, the diagrams may justify the following

CONJECTURE. *Weaker form*: *There are constants* b, B, c, C, *with*

$$0.3 < b < B < 0.5, \quad 0.065 < c < C < 0.085,$$

such that

$$b < \frac{n(k)}{k^e} < B, \quad c < \frac{n_k}{k^e} < C$$

for sufficiently large k.

Stronger form: *There are constants* β, γ *such that*

$$n(k) \sim \beta k^e, \quad n_k \sim \gamma k^e .$$

Even the weaker form is stronger than the conjecture

$$\lim_{k\to\infty} \frac{\log n(k)}{\log k} = \lim_{k\to\infty} \frac{\log n_k}{\log k} = e$$

made in [3].

The stronger form of the conjecture is probably too strong. One reason to believe this is given by the strings of dots sloping down to the right in both diagrams. These strings correspond to values of $n(k)$ or n_k which are (nearly) equal for several values of k. This phenomenon is not unexpected: If $V(n,k)$ is particularly small or particularly large, the same is likely to happen for $V(n_1,k_1)$ with $n_1 \approx n$, $k_1 \approx k$.

In Table 2, some of the "stable" values of $n(k)$ have large clusters of primes just below $n(k)$, for instance

$$k = 16, 17, 18, 20, 21:$$

primes 1867, 1871, 1873, 1877, 1879;

$$k = 25, 26, 27, 29:$$

primes 4783, 4787, 4789, 4793, 4799, 4801 .

5.

It is clear from the above that the (extended) argument of Mignotte is useful both in theoretical and numerical applications. Some further such applications are described by the author in [7]. We mention the following

THEOREM 2. *The binomial coefficient* $\binom{2t}{t}$ *contains at least* k *different prime divisors if the product of the first* $t-k+1$ *composite numbers larger than* t *exceeds* $t!$.

A similar result holds for arbitrary $\binom{n}{k}$. In [7], this is used to obtain a substantial reduction of a calculation by Ecklund and Eggleton [1]. Their purpose was to show that $\binom{n}{t}$ always contains a prime divisor $>t$ for $n \geqq 2t$. The following by-product of these calculations in [7] may be worth while mentioning:

Erdös [2] showed that for given $\varepsilon > 0$ and $t > t_0(\varepsilon)$, $n \geqq 2t$, we have

$$V(n,t) > (1-\varepsilon)\frac{t \log 4}{\log t}.$$

This of course implies that for $n \geqq 2t$,

$$V(n,t) \geqq \pi(t)$$

for sufficiently large t. It turns out, however, that this inequality holds for *all* t. In other words, *the binomial coefficient* $\binom{n}{t}$, $n \geqq 2t$, *contains at least as many different prime divisors as its denominator* $t!$.

We conclude with another result, also prompted by a remark of Erdös [2]. It is clear that on the average, $V(n,k)$ will be an *increasing function* of both n and k. Erdös noted that, for given k, there exist values of n such that

$$V(n,k) > V(n,k+1), \tag{9}$$

and gave $k=5$, $n=78$ as an example. (There are simpler cases, the smallest one being $k=4$, $n=10$.) He also conjectured that for sufficiently large $n > n_0$, there is always a k satisfying (9).

It turns out that much more can be said about the analogous inequality

$$V(n,k) > V(n+1,k).$$

Let $\omega(m)$ denote the number of different prime divisors of m. We then have the following result, the proof of which is found in [7]:

THEOREM 3. *For given positive integers* k *and* d, *there are infinitely many* n *satisfying*

$$V(n,k) - V(n+1,k) \geqq d..$$

For given k, *there is only a finite number of* n *satisfying*

$$V(n,k) - V(n,k+1) = \omega(k+1).$$

For given k, there are infinitely many n satisfying

$$V(n,k)-V(n,k+1) = \omega(k+1)-1 .$$

REFERENCES

1. E. F. Ecklund and R. B. Eggleton, *Prime factors of consecutive integers*, Amer. Math. Monthly 79 (1972), 1082–1089.
2. P. Erdös, *Über die Anzahl der Primfaktoren von* $\binom{n}{k}$, Arch. Math. (Basel) 24 (1973), 53–56.
3. P. Erdös, H. Gupta and S. P. Khare, *On the numbers of distinct prime divisors of* $\binom{n}{k}$, Utilitas Math. 10 (1976), 51–60.
4. F. Hering, *Eine Beziehung zwischen Binomialkoeffizienten und Primzahlpotenzen*, Arch. Math. (Basel) 19 (1968), 411–412.
5. M. Mignotte, *Sur les coefficients du binôme*, Arch. Math. (Basel) 24 (1973), 162–163.
6. H. Scheid, *Die Anzahl der Primfaktoren in* $\binom{n}{k}$, Arch. Math. (Basel) 20 (1969), 581–582.
7. E. S. Selmer, *On the number of prime divisors of a binomial coefficient*, Univ. of Bergen, Dept. of Pure Math., Preprint Series, No. 8, 1976.
8. W. Stahl, *Bemerkung zu einer Arbeit von Hering*, Arch. Math. (Basel) 20 (1969), 580.

UNIVERSITY OF BERGEN
NORWAY