ON THE SCARCITY OF POWERFUL BINOMIAL COEFFICIENTS

Andrew Granville

Dedicated to the memory of Paul Erdős

Abstract. Assuming the *abc*-conjecture we show that there are only finitely many powerful binomial coefficients $\binom{n}{k}$ with $3 \le k \le n/2$; in fact, that if q^2 divides $\binom{n}{k}$ that $q \ll n^2 \binom{n}{k}^{o(1)}$. Unconditionally we show that there are $N^{1/2+o(1)}$ powerful binomial coefficients in the top N rows of Pascal's Triangle.

Introduction.

Binomial coefficients $\binom{n}{k}$ may be written out as the product of many small integers, divided by the product of many other small integers. Usually there will be a lot of cancellation and we will be left with an integer that is the product of many primes, often to quite high powers. Paul Erdős has asked many intriguing questions about the prime power divisors of binomial coefficients. For example, posing questions about how often they are squarefree (see [8] for some answers), how often they are squarefull (an integer m is said to be *squarefull* or *powerful* if p^2 divides m whenever prime p divides m), or studying the number of different prime divisors a typical binomial coefficient has.

It was Goldbach [7] who first noted that the product of two consecutive integers could not be a square (and thus $\binom{n}{2}$ cannot be twice a square); and Mlle A.D. [1], in 1857, who showed that the product of three consecutive integers could not be a perfect power. In the same year, Liouville considered whether the product of arbitrarily many consecutive integers could possibly be a perfect power (he had previously proved that $(p-1)!+1$ is an exact power of p, only for $p = 2, 3$ and 5). In 1951 Erdős [4] showed that the binomial coefficient $\binom{n}{k}$ could not be a perfect power once $k \ge 4$. In 1975 Erdős and Selfridge [6] proved the very difficult result[1]:

The Erdős–Selfridge Theorem. *The product of two or more consecutive positive integers can never be a perfect power.*

Ramaré and I have shown that there are few squarefree binomial coefficients: Corollary 1 of [8] states that there exists some constant c ($\approx 12\frac{2}{3}$) such that the top N rows of Pascal's triangle contain $\sim cN$ squarefree entries. Recently Ognian Trifonov asked[2] about the frequency of powerful binomial coefficients. Since

A Presidential Faculty Fellow. Also supported, in part, by the National Science Foundation.

[1] In 1940 Erdős and Siegel had proved, in unpublished joint work, the slightly weaker result that the product of κ or more consecutive positive integers can never be a perfect power, for some sufficiently large κ

[2] At the South East Regional Meeting on Numbers at the College of Charleston on 11/3/95.

$\binom{n}{n-k} = \binom{n}{k}$ we will restrict our attention to those $k \le n/2$. We observe that there are infinitely many powerful binomial coefficients of the form $\binom{n}{0} = 1$ and $\binom{n}{1} = n$ trivially; and also infinitely many powerful binomial coefficients of the form $\binom{n}{2}$, which follows from noting that if $x_k + \sqrt{8}y_k = (3+\sqrt{8})^k$ then $\binom{x_k^2}{2} = (2x_k y_k)^2$ for all positive integers k. What of the rest of Pascal's triangle? Does it contain many other powerful numbers? We believe not:

Conjecture 1. *The only powerful binomial coefficient $\binom{n}{k}$ with $2 < k < n-2$ is $\binom{50}{3} = \binom{50}{47} = 140^2$.*

Erdős and Selfridge [6] made a conjecture[3] that would unify these slightly different problems, implying (most of) their Theorem as well as Conjecture 1:

The Erdős–Selfridge Conjecture. *If $3 \le k \le n/2$ then $\binom{n}{k}$ must be divisible by some prime $p \ge k$, but not by p^2; except in the example $\binom{50}{3} = 140^2$.*

This easily implies Conjecture 1. We showed that the Erdős–Selfridge Conjecture is true whenever $n \le 10^6$ (in a computation that we describe in section 8).

Erdős and Selfridge write that their "*conjecture, if true, seems very deep*". As well as our computations, we justify it by showing that it follows (up to finitely many counterexamples) from

The *abc*-conjecture. *(Oesterlé, Masser, Szpiro). Fix $\varepsilon > 0$. If a, b, c are pairwise coprime positive integers satisfying $a + b = c$ then $c^{1-\varepsilon} \ll_\varepsilon \prod_{p|abc} p$.*

Theorem 1. *The abc-conjecture implies the Erdős–Selfridge Conjecture, and thus Conjecture 1, with at most finitely many counterexamples. That is, if the abc-conjecture is true then there are only finitely many pairs of integers (k, n) with $3 \le k \le n/2$ such that whenever prime $p \ge k$ divides $\binom{n}{k}$ then so does p^2.*

To prove Theorem 1 for "small" k we use the *abc*-conjecture. For larger k we have a very different argument: Liouville (1857) noted that if one has a prime p in the range $k \le n-k < p \le n$ then the only term that p divides in the expansion $\binom{n}{k} = \frac{n(n-1)\dots(n-(k-1))}{k!}$ is the p in the numerator, and so $\binom{n}{k}$ is divisible by p but not p^2. Such a prime p certainly exists for $k = n/2$ by Bertrand's postulate. To use Liouville's argument in a wide range for k, we need good bounds for the size of gaps between consecutive primes. Unfortunately what is currently known unconditionally only leads to a result for $k < n^{1/2+\delta}$ for some constant $\delta > 0$. This is not good enough for our purposes.

We thus modify Liouville's idea by looking for a prime $p > k$ which divides $n(n-1)\dots(n-(k-1))$, whereas p^2 does not (that some prime $p > k$ divides $n(n-1)\dots(n-(k-1))$, is precisely the Sylvester-Schur Theorem). Note that any prime $p > k$ cannot divide $k!$, nor can it divide more than one of the integers $n, n-1, \dots, n-(k-1)$. Therefore we only need check that p, but not p^2, divides $n-i$ for some $i, 0 \le i < k$. This is certainly the case if $k \ge \sqrt{n}$ (since then $p^2 > k^2 \ge n \ge n-i$), and should usually be the case, which we will show by using Sander's estimates for exponential sums [11]. In the next section we prove unconditionally:

[3] Actually they made a slightly weaker conjecture, which is equivalent to ours for $k \ge 4$.

Theorem 2. *There exists a constant $c_1 > 0$ such that if n is sufficiently large and $\exp\left(c_1(\log n)^{2/3}(\log\log n)^{1/3}\right) < k \le n/2$ then there exists a prime $p \ge k$ which divides $\binom{n}{k}$ to exactly the first power.*

Combining this with Theorem 2 in [8] we get

Corollary 1. *If $\binom{n}{k}$ is either powerful or squarefree, then either k or $n-k$ is $\ll \exp\left(c_1(\log n)^{2/3}(\log\log n)^{1/3}\right)$.*

Unconditionally we can prove the following estimate for the number of powerful binomial coefficients in the top N rows of Pascal's Triangle:

Corollary 2. *There are $N^{1/2+o(1)}$ powerful binomial coefficients $\binom{n}{k}$ with $1 \le k < n \le N$.*

We complete the proof of this in section 6. Thus we can prove, unconditionally, that powerful binomial coefficients are far scarcer than squarefree binomial coefficients. It seems plausible that one could unconditionally prove that there are $N^{o(1)}$ pairs of powerful numbers $x, y < N$ for which $x - y = N^{o(1)}$. If so then one can deduce, by a method described at the end of section 6, that there are $N^{o(1)}$ powerful binomial coefficients[4] with $2 \le k \le n-2$ and $n \le N$.

Recently Langevin [10, Théorème 2] proved a result about prime factors of consecutive integers which immediately implies:

Lemma 1. *Fix $\varepsilon > 0$ and integer $r \ge 1$. The abc-conjecture implies that if n is sufficiently large then*

$$\prod_{p \mid \binom{n}{r}} p \ge \binom{n}{r}^{1-1/r-\varepsilon}.$$

Modifying our arguments above, and using Lemma 1, we will obtain:

Proposition 1. *Fix $\varepsilon > 0$. The abc-conjecture implies, whenever $1 \le k \le n/2$, that*

$$\prod_{p \mid \binom{n}{k}} p \gg_\varepsilon \binom{n}{k}^{1-1/k-\varepsilon}.$$

Notice that Proposition 1 is somewhat stronger than Lemma 1 since it is uniform in k.

Henceforth the notation $p||m$ means that p divides m, but p^2 does not divide m. Then $\binom{n}{k}\prod_{p||\binom{n}{k}} p \ge \prod_{p\mid\binom{n}{k}} p^2 \gg_\varepsilon \binom{n}{k}^{2-2/k-2\varepsilon}$ by Proposition 1. Therefore (changing the value of $\varepsilon > 0$) we have the following strengthening of Theorem 1:

Theorem 1'. *Fix $\varepsilon > 0$. The abc-conjecture implies that the product of the primes which divide $\binom{n}{k}$ to the first power (where $3 \le k \le n/2$) is $\gg_\varepsilon \binom{n}{k}^{1-2/k-\varepsilon}$.*

In particular we get the following strengthening of the Erdős-Selfridge Theorem:

[4]Gang Yu has recently shown that there are $\le N^{2/5+o(1)}$ pairs of powerful numbers $x, y < N$, from which one deduces that there are no more than $N^{2/5+o(1)}$ such powerful binomial coefficients.

Corollary 3. *Fix $\varepsilon > 0$. The abc-conjecture implies that if $\binom{n}{k} = ay^\ell$ with $3 \le k \le n/2$ and $\ell \ge 2$, then $a \gg_\varepsilon \binom{n}{k}^{1-2/k-\varepsilon}$. In particular, selecting $\varepsilon < 1/12$, we see that there are only finitely many integer solutions to $\binom{n}{k} = ay^\ell$, with $3 \le k \le n-3$, $\ell \ge 2$ and $a \le \binom{n}{k}^{1/4}$.*

We will prove in section 9:

Proposition 2. *If $n = 9x^2$ where $3x+2\sqrt{2}y = (3+2\sqrt{2})^q$ and q is a prime $\ge k+2$, then $(xy)^2$ divides $\binom{n}{k}$ whenever $2 \le k \le n-2$.*

For the examples given by Proposition 2, we have $(xy)^2 = \frac{n(n-1)}{72} \ge \frac{1}{36}\binom{n}{k}^{2/k}$, so that

$$\prod_{p|\binom{n}{k}} p \le \binom{n}{k} \Big/ (xy) \le 6\binom{n}{k}^{1-1/k}, \quad \text{and} \quad \prod_{p||\binom{n}{k}} p \le \binom{n}{k} \Big/ (xy)^2 \le 36\binom{n}{k}^{1-2/k}.$$

Thus we see that Propositions 1 and Theorem 1' are essentially "best possible".

We can prove a weak, but unconditional result, along the lines of Proposition 1:

Theorem 3. *We have*

$$\prod_{p|\binom{n}{k}} p \ge \begin{cases} k^{\{1/2+o(1)\}k} & \text{if } \ n \ge k^2 \\ (n/k)^{\{1+o(1)\}k} & \text{if } \ n \le k^2 \end{cases}$$

Using the methods of Erdős and Selfridge [6], we will prove a weaker but unconditional result like Corollary 3:

Theorem 4. *Suppose that $\binom{n}{k} = a\alpha y^\ell$, where $a\alpha$ is not divisible by the ℓth power of any prime, a is free of prime factors $< k$ and α is free of prime factors $\ge k$. If $n \ge k^\ell$ then $\prod_{p|a} p \ge (\log k)^{k+o(k)}$ if $\ell \ge 3$; and $\prod_{p|a} p \gg (17/9)^k$ if $\ell = 2$. On the other hand, if $n < k^\ell$ then $a \ge \binom{n}{k}/n^{\pi(k-1)}$. Thus $a \ge (\log k)^{k+o(k)}$ for $n \gtrsim k \log k$ with $\ell \ge 3$; and $a \gg (17/9)^k$ for $n \ge 2k$.*

In fact Erdős and Selfridge [6, Theorem 2] proved that if n is at least as large as the smallest prime $\ge k$, with $k \ge 2$ then $a \ge k$ (with the notation as in our Theorem 4).

We deduce, from results above, a quite complete (conditional) answer to the Erdős-Selfridge Conjecture:

Corollary 4. *If the abc-conjecture is true then*

$$i) \qquad \min_{n \ge 2k} \prod_{p||\binom{n}{k}} p = 4^{k+o(k)} \qquad \text{(Erdos)},$$

$$ii) \qquad \min_{n \ge 2k} \prod_{p||\binom{n}{k},\ p \ge k} p = \mathrm{e}^{k+o(k)}.$$

Proof. i) We may assume $k \to \infty$. By Theorem 1', our product is $\gg \binom{n}{k}^{1+o(1)} \ge \binom{2k}{k}^{1+o(1)} = 4^{k+o(k)}$. However this minimum is attained by $\binom{2k}{k}$.

ii) If $n > 4k$ then $\binom{n}{k} > \binom{4k}{k} > \mathrm{e}^{(2+\delta)k+o(k)}$, for some fixed $\delta > 0$. By Theorem 1' and the prime number theorem we then have

$$\prod_{p||\binom{n}{k},\ p\ge k} p \gg_\varepsilon \binom{n}{k}^{1-2/k-\varepsilon} \Big/ \mathrm{e}^{k+o(k)} > \mathrm{e}^{(1+\delta)k+o(k)}.$$

If $4k \ge n \ge 2k$ then $p|\binom{n}{k}$ with $p > k$ exactly for those primes in the intervals $(n-k, n]$, $(\max\{k, (n-k)/2\}, n/2]$ and $(k, \max\{k, n/3\}]$. The product of these primes is $\mathrm{e}^{n/2+o(n)}$ (for $3k \ge n \ge 2k$) $\mathrm{e}^{n/3+k/2+o(n)}$ (for $4k \ge n \ge 3k$) by the prime number theorem. The result follows and the minimum is attained when $n = 2k + o(k)$.

Acknowledgements:. I would like to thank Ognian Trifonov for his inspiring question, and Paul Erdős and Carl Pomerance for making several pertinent remarks.

2. Proof of Theorem 2.

Large k: $(n^{1/2} \le k \le n/2)$.

The theorem of Sylvester and Schur states that if $n \ge 2k$ then $\binom{n}{k}$ has a prime factor $p > k$ (note that Bertrand's postulate is just the case with $n = 2k$). But then p does not divide the denominator $k!$, and divides at most one term in the numerator, say $n - i$. However $p^2 > k^2 \ge n \ge n - i$ and so p^2 cannot divide $n - i$, and thus it cannot divide $\binom{n}{k}$.

Medium k: $(n^{1/2-\delta} < k \le n^{1/2})$.

We will show that there is a prime $p > n^{1/2}$ which divides $\binom{n}{k}$. Then $p > k$ and $p^2 > n$, so arguing as in the previous case, we have found our prime p.

A recent paper of Sander [11] gives us a useful lemma with which to study the distribution of multiples of powers of primes:

Lemma 2. *Fix $\varepsilon > 0$ and integer $J \ge 1$. There exists a constant $c_2 > 0$ such that for any $y \le n^{1/J}$, there are*

$$\sigma_1\sigma_2\dots\sigma_J\pi(y) + O\left(\left(y^{1-c_2(\log y/\log n)^2} + y^{J/2+1+\varepsilon}n^{-1/2}\right)(\log n)^{4J}\right)$$

primes $p \le y$ for which $\{n/p^j\} < \sigma_j$ for $j = 1, 2, \dots, J$ (where $0 \le \sigma_j \le 1$ for each j).

We take $J = 1$ and $\sigma_1 = k/y$ in Lemma 2. By the prime number theorem, we deduce that there are

$$\{1 + o(1)\}\frac{k}{2\log y} + O\left(\left(y^{1-c_2(\log y/\log n)^2} + y^{3/2+\varepsilon}n^{-1/2}\right)\log^4 n\right) \tag{1}$$

primes p, $y/2 < p \le y$ for which $\{n/p\} < k/y$, whenever $y \le n$. Note that for each such prime p we have $p\{n/p\} < pk/y \le k$, so that p divides $n-i$ for some $0 \le i < k$. If we select $y = 2n^{1/2}$ then each such prime $p > n^{1/2}$, and such primes exist since the expression in (1) is non-zero in the range stated, for some (sufficiently small) value of $\delta > 0$.

Small k: $(\exp\left(c_1(\log n)^{2/3}(\log\log n)^{1/3}\right) < k \le n^{1/2-\delta})$.

In this case we will show that there are many primes between k and $2k$ which divide $\binom{n}{k}$, but whose square does not:

We take $J = 2,\ y = 2k,\ \sigma_1 = 1/2, \sigma_2 = 1/k$ in Lemma 2, and subtract the result from (1) to get that there are

$$\{1+o(1)\}\frac{k}{2\log k} + O\left(\left(k^{1-c_3(\log k/\log n)^2} + k^{2+\varepsilon}n^{-1/2}\right)\log^8 n\right) \tag{2}$$

primes $p,\ k < p \le 2k$ for which $\{n/p\} < 1/2$ and $\{n/p^2\} > 1/k$, whenever $2k \le n^{1/2}$ as $k \to \infty$. The expression in (2) is non-zero in the range stated, provided $\varepsilon > 0$ is chosen sufficiently small, so there does exist such a prime p. Now $p\{n/p\} < p/2 \le k$ so that p divides $n-i$ for some $i,\ 0 \le i < k$. On the other hand $p^2\{n/p^2\} > p^2/k > k$ so that p^2 does not divide $n-i$. Therefore p divides $\binom{n}{k}$ but not p^2.

3. Small k, and the *abc*-conjecture

In the previous section we dealt with the "large" values of k. For the smaller values of k we attack the problem quite differently:

Proposition 3. *Assume that the abc-conjecture is true and fix λ in the range $1/3 > \lambda > 0$. If n is sufficiently large and $3 \le k < n^\lambda$ then there exists some prime $p \ge k$ such that p divides $\binom{n}{k}$ but p^2 does not.*

Note that Proposition 3, combined with Theorem 2, yields Theorem 1. Before proving Proposition 3 we make the following observations:

Suppose that if prime $p \ge k$ divides $\binom{n}{k}$ then so does p^2. For each $0 \le i < k$ we write $n - i = \tau_i\eta_i$ where τ_i is squarefree, η_i is powerful and $(\tau_i, \eta_i) = 1$. By assumption we see that all of the prime factors of τ_i must be $\le k$. Therefore

$$\prod_{0\le i<k}\prod_{p|\tau_i} p = \prod_{p\le k} p^{\#\{0\le i<k:\ p||n-i\}} \le \prod_{p\le k} p^{1+k/p} = k^k e^{O(k)} \tag{3}$$

using the prime number theorem.

Proof of Proposition 3. Note that, since η_i is powerful, and since τ_i is squarefree, we get

$$\prod_{p|n-i} p = \prod_{p|\tau_i} p \prod_{q|\eta_i} q \le \left(\tau_i \prod_{p|\tau_i} p\right)^{1/2} \eta_i^{1/2} \le \left(n\prod_{p|\tau_i} p\right)^{1/2}.$$

By (3) we deduce that $\prod_{p|\tau_{i-1}\tau_i\tau_{i+1}} p \ll k^3$ for some integer $i,\ 1 \le i \le k-2$. Therefore, applying the *abc*-conjecture to $(n-i-1)(n-i+1)+1 = (n-i)^2$, with $\varepsilon = (1-3\lambda)/8$, we obtain

$$\begin{aligned} n^{2(1-\varepsilon)} &\ll_\varepsilon \prod_{p|(n-i-1)(n-i)(n-i+1)} p \le \left(n^3 \prod_{p|\tau_{i-1}\tau_i\tau_{i+1}} p\right)^{1/2} \\ &\ll k^{3/2}n^{3/2} \ll n^{3(1+\lambda)/2}, \end{aligned}$$

which gives a contradiction for sufficiently large n.

4. Proof of Proposition 1

Large k: $(n^{1/2} \le k \le n/2)$.

Kummer's Theorem (1852) states that the exact power of p that divides $\binom{n}{k}$ is given by the number of "carries" when we add k and $n-k$ in base p. Therefore, if p^{a_p} divides $\binom{n}{k}$ then we must have $p^{a_p} \le n$. In particular, if $a_p \ge 2$ then $p \le \sqrt{n}$ so that

$$\prod_{p^2 \mid \binom{n}{k}} p^{a_p} \le n^{\pi(\sqrt{n})} \le \mathrm{e}^{\{2+o(1)\}\sqrt{n}}$$

by the prime number theorem. This is evidently $\ll \binom{n}{k}^{\varepsilon}$ since $k \ge \sqrt{n}$. Therefore

$$\prod_{p \mid \binom{n}{k}} p \ge \binom{n}{k} \Big/ \prod_{p^2 \mid \binom{n}{k}} p^{a_p} \gg \binom{n}{k}^{1-\varepsilon}. \tag{4}$$

Medium k: $(n^{1/3} \le k < n^{1/2})$.

Let $z = k(\log n)^{1/3}$. Suppose that $p > z \ge k$ is a prime for which p^2 divides $\binom{n}{k}$. Then p^2 divides some integer $n-i$, where $0 \le i < k$. Write $n - i = ap^2$ so that $a \le n/p^2 < n/z^2$. Now, for any integer $a \ge 1$, there is at most one square in the range $(n/a - k/a, n/a]$, since $k/a < (n/a)^{1/2}$ (and so at most one integer of the form $am^2 \in (n-k, n]$). Therefore there are $\le n/z^2$ primes $p > z$ for which p^2 divides some integer in the range $(n-k, n]$ (that is, at most one for each value of a).

Thus, in total, we have $\le \pi(z) + n/z^2 \le 5k/(\log n)^{2/3}$ primes p for which p^2 divides $\binom{n}{k}$ (by the prime number theorem, and since $k \ge n^{1/3}$). Proceeding as above we find that

$$\prod_{p^2 \mid \binom{n}{k}} p^{a_p} \le n^{5k/(\log n)^{2/3}} \ll \binom{n}{k}^{\varepsilon}$$

since $\binom{n}{k} \ge n^{k/3}$ in this range. The result then follows as in (4).

Small k: $(2 \le k \le n^{1/3})$.

Select r to be a fixed integer $> 12/\varepsilon$. If $k \le r^2$ then the result follows directly from Lemma 1 (with $r = k$), by suitably adjusting the implicit constant (since k is in amongst a finite set of integers).

If $k > r^2$ then we let $m = [k/r]$. We will use the identity

$$\binom{k}{mr} \frac{(mr)!}{r!^m} \binom{n}{k} = \left(\binom{n}{r} \binom{n-r}{r} \binom{n-2r}{r} \cdots \binom{n-(m-1)r}{r} \right) \binom{n-mr}{k-mr}. \tag{5}$$

Note that $\binom{k}{mr} \frac{(mr)!}{r!^m}$ is an integer, whose prime factors are all $\le k$; and that $\binom{k}{mr} \frac{(mr)!}{r!^m} = k^k \mathrm{e}^{O(k)}$. Also note that prime p can divide no more than $1 + k/p$ integers in $(n-k, n]$, so if it divides two such integers then we must have $p \le k$.

Therefore, using Lemma 1 with n sufficiently large, we obtain from (5) and the prime number theorem, that

$$\begin{aligned}\prod_{p|\binom{n}{k}} p \ge \prod_{p|\binom{n}{k},\ p>k} p &\ge \left(\prod_{p|\binom{n}{r}} p \prod_{p|\binom{n-r}{r}} p \cdots \prod_{p|\binom{n-(m-1)r}{r}} p\right) \prod_{p|\binom{n-mr}{k-mr}} p \Big/ \prod_{p\le k} p^{1+k/p} \\ &\ge \left(\binom{n}{r}\binom{n-r}{r}\binom{n-2r}{r}\cdots\binom{n-(m-1)r}{r}\right)^{1-1/r-\varepsilon/3} \Big/ k^k \mathrm{e}^{O(k)} \\ &\ge \left(\binom{n}{k} k^k \mathrm{e}^{O(k)} \Big/ \binom{n-mr}{k-mr}\right)^{1-1/r-\varepsilon/3} \Big/ k^k \mathrm{e}^{O(k)} \\ &\gg \binom{n}{k}^{1-2/r-2\varepsilon/3-2r/k} > \binom{n}{k}^{1-\varepsilon}\end{aligned}$$

where the penultimate step is justified by noting that, in our range, $k^k \mathrm{e}^{O(k)} \ll \binom{n}{k}$ and $\binom{n-mr}{k-mr} \le n^r \le \binom{n}{k}^{2r/k}$.

5. Proof of Theorems 3 and 4

As above, the exact power of prime p dividing dividing $\binom{n}{k}$ is $\le n$. Since $\frac{n-i}{k-i} \ge \frac{n}{k}$ for each $i \ge 0$, we have $\binom{n}{k} \ge \left(\frac{n}{k}\right)^k$. Therefore if $n \ge k^2$ there are at least $k/2$ distinct primes dividing $\binom{n}{k}$; and their product is at least as large as the product of the smallest $k/2$ primes, which is $\ge k^{(1/2+o(1))k}$. This proves Theorem 3 for $n \ge k^2$.

Now, in Theorem 4, suppose that prime p divides y and is $\ge k$. Since $p \ge k$ it divides at most one $n-i$ with $0 \le i < k$. Then p^ℓ divides $n-i$ and so $k^\ell \le p^\ell \le n-i \le n$. Therefore if $n < k^\ell$ then all of the prime factors of y are $< k$. As above, if p^{a_p} is the exact power of p dividing $\binom{n}{k}$ then $p^{a_p} \le n$, and so

$$\alpha y^\ell = \prod_{p<k} p^{a_p} \le \prod_{p<k} n = n^{\pi(k-1)},$$

which gives the second part of Theorem 4.

We may take this same argument (when $\ell = 2$) to note that if $n \le k^2$, then the product of the primes dividing $\binom{n}{k}$ is at least $\binom{n}{k} \prod_{p<k} \frac{p}{n}$. However $\prod_{p<k} \frac{n}{p} = \binom{n}{k}^{O(1/\log k)}$ and so Theorem 3 follows in this range since $\binom{n}{k} \ge \left(\frac{n}{k}\right)^k$.

We now complete the proof of Theorem 4: Assume that $n \ge k^\ell$ and write each $n-i = a_i \alpha_i y_i^\ell$ where all of the prime factors of a_i and α_i are $\ge k$ and $< k$, respectively, and neither are divisible by the ℓth power of a prime . By Lemma 1 of [6] we know that the numbers $a_i\alpha_i$ must all be distinct, and also that the products of pairs $(a_i\alpha_i)(a_j\alpha_j)$ must be distinct if $\ell > 2$. Therefore, by (10) of [6], the number of $a_i\alpha_i \le t$ must be $< t/\log t + O(t/\log^2 t)$ (for any $t > 1$). If I is a subset of $\{0, 1, \dots, k-1\}$ then we deduce that

$$(6)\quad \int_2^x \left(\sum_{i\in I,\ a_i\alpha_i \le t} 1\right) \frac{dt}{t} < \int_2^x \left(\frac{t}{\log t} + O\left(\frac{t}{\log^2 t}\right)\right) \frac{dt}{t} < \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Select i_p so that the power of p dividing $n-i$ is maximal amongst i in the range $0 \le i < k$. By Lemma 2 of [6] we know that the product of the α_i, with $0 \le i < k$, and $i \ne i_p$ for any prime $p < k$, divides $(k-1)!$. In particular, letting I be that subset of $\{0, 1, \dots, k-1\}$, where $i \in I$ if $a_i = 1$ and $i \ne i_p$ for any prime $p < k$, we have

$$\sum_{i \in I} \log \alpha_i \le \log(k-1)! \le k(\log k - 1) + O(1). \tag{7}$$

Now, by partial summation, we get

$$\begin{aligned}\sum_{i \in I,\ \alpha_i \le x} \log \alpha_i &= \int_2^x \log t \ d\left(\sum_{i \in I,\ \alpha_i \le t} 1\right) \\ &= \left(\sum_{i \in I,\ \alpha_i \le x} 1\right) \log x - \int_2^x \left(\sum_{i \in I,\ a_i\alpha_i \le t} 1\right) \frac{dt}{t} \\ &> \left(\sum_{i \in I,\ \alpha_i \le x} 1\right) \log x - \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)\end{aligned}$$

using (6). Adding to both sides each $\alpha_i > x$ we find that

$$\sum_{i \in I} \log \alpha_i \ge |I| \log x - \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Taking $x = k \log k$ and comparing this to (7) gives

$$|I| \le k\left(1 - \frac{\log\log k}{\log k} + O\left(\left(\frac{\log\log k}{\log k}\right)^2\right)\right).$$

But $|I| \ge k - \pi(k-1) - \#\{a_i > 1\}$ and so

$$\#\{a_i > 1\} \ge k\left(\frac{\log\log k - 1}{\log k} + O\left(\left(\frac{\log\log k}{\log k}\right)^2\right)\right).$$

But the a_i are all free of prime factors $< k$, and thus coprime. Moreover those that are > 1 are divisible by a distinct prime $\ge k$ and so

$$\prod_{p \mid a} p \ge \prod_{k \le p < \{1+o(1)\}k \log\log k} p = (\log k)^{k+o(k)}.$$

This completes the proof when $\ell > 2$.

Since the $a_i\alpha_i$ are distinct and squarefree for $\ell = 2$, so $\prod_i a_i\alpha_i \ge (\pi^2 k/6e)^{k+o(k)}$, by Stirling's formula. The power of prime $p \le k$ dividing $\prod_i \alpha_i$, which we denote by e_p, is given by the number of integers $n-i,\ 0 \le i < k$ which are exactly divisible

by an odd power of p. Trivially $e_p \le [k/p]+1 \le 1+g_p$, where g_p is the power of p dividing $k!$. We can write e_p by the exact formula

$$e_p := \left(\left[\frac{n}{p}\right] - \left[\frac{n-k}{p}\right]\right) - \left(\left[\frac{n}{p^2}\right] - \left[\frac{n-k}{p^2}\right]\right) + \left(\left[\frac{n}{p^3}\right] - \left[\frac{n-k}{p^3}\right]\right) - \dots$$

Let p^γ be the smallest power of p which is $\ge k$; and let N be that integer in the interval $(n-k, n]$ which is divisible by the highest power of p. If $j \ge \gamma$ then there cannot be any integer in $(n-k,n]$, other than N, which is divisible by p^j. Therefore $e_p = k/(p+1) + O(\log k/\log p)$. By a similar argument one shows that $g_p = k/(p-1) + O(\log k/\log p)$, and so $e_p \le g_p - 2k/(p^2-1) + O(\log k/\log p)$. Therefore

$$\begin{aligned}\prod_i \alpha_i &\le k! \prod_{p\le k} p \ \exp\left(-\sum_{p\le\sqrt{k}} \left\{2k\frac{\log p}{p^2-1} + O(\log k)\right\}\right)\\ &\le k^k \exp\left(-2k\sum_p \frac{\log p}{p^2-1} + O\left(\frac{k}{\log k}\right)\right)\end{aligned}$$

by the prime number theorem and Stirling's formula. Therefore $\prod_i a_i \ge e^{\{c+o(1)\}k}$ where $c := 2\sum_p \frac{\log p}{p^2-1} + \log(\pi^2/6) - 1 \approx .6376\dots$.

6. Unconditionally bounding the number of powerful binomial coefficients

Proof of Corollary 2. If $\binom{n}{k}$ is powerful then $\tau_i \ll k$ for some i, by (3); that is there exists $i,\ 0 \le i < k$ for which $n-i$ is τ_i times a powerful number. Therefore, for a given k, $m_k(N)$, the number of powerful $\binom{n}{k}$ with $N < n \le 2N$, is at most k times the number of integers $\tau\eta \le x$ where $\tau \ll k$ and η is powerful. As is well-known (see section 7), there are $\ll \sqrt{x}$ powerful numbers $\le x$, and so $m_k(N) \ll k\sum_{\tau\ll k}\sqrt{N/\tau} \ll k^{3/2}N^{1/2}$. Therefore $\sum_{k\le K} m_k(N) \ll K^{5/2}N^{1/2}$. Taking $K = \exp\left(c_1(\log N)^{2/3}(\log\log N)^{1/3}\right)$ and combining this with Theorem 2, gives the result.

We can hope to improve upon this argument by improving on (3). Let e_p be the number of integers $i,\ 0 \le i < k$ with $p||n-i$. Evidently

$$e_p := \left(\left[\frac{n}{p}\right] - \left[\frac{n-k}{p}\right]\right) - \left(\left[\frac{n}{p^2}\right] - \left[\frac{n-k}{p^2}\right]\right) \le \left[\frac{k}{p}\right] - \left[\frac{k}{p^2}\right] + 1$$

Proceeding as in the argument from the end of the previous section we deduce that $\prod_i \tau_i \le k^k/e^{\{c+o(1)\}k}$ where $c := \sum_p (2p-1)\log p/p^2(p-1) \approx 1.2484\dots$. Since the τ_i are squarefree, this implies that $\tau_i = \tau_j$ for many pairs i,j. In fact if $\tau_i = \tau_j$ then $|\eta_j - \eta_i| < k/\tau_i$. If we could show that there is such a pair with $\tau_i \ge k/2$ then we would show the existence of a pair of consecutive powerful numbers arises as a consequence. Even if we could show that there is such a pair with $\tau_i \gg k$ then we would have a pair of powerful numbers a bounded distance apart.

In fact, from (3) we easily deduce that there exists $i \neq j$ with $\tau_i, \tau_j \ll k$. Thus $x = (\tau_i\tau_j)^2(n-i)$ and $y = (\tau_i\tau_j)^2(n-j)$ are both powerful numbers, with $x-y = (\tau_i\tau_j)^2(j-i) \ll k^5$. On the other hand, given any pair of powerful numbers x, y with $x - y \ll k^5$ there are no more than k choices for each of τ_i, τ_j, i and then the values of j and n follow. Thus the number of powerful binomial coefficients $\binom{n}{k}$ with $N < n \leq 2N$, is $\leq k^3$ times the number of pairs of powerful numbers $x, y \leq N$, with $x - y \ll k^5$. This implies the remark that follows Corollary 2.

7. Powerful binomial coefficients in the first two columns

Counting the number of powerful $\binom{n}{1} = \binom{n}{n-1} = n \leq N$ is straightforward once we note that every powerful number may be written in a unique way as d^3y^2 with d squarefree. Then we get that the number is

$$\sum_{d\leq N^{1/3}} \mu^2(d)\left[\left(\frac{N}{d^3}\right)^{1/2}\right] = N^{1/2}\sum_{d\leq N^{1/3}}\frac{\mu^2(d)}{d^{3/2}} + O(N^{1/3})$$
$$= N^{1/2}\left(\prod_p\left(1+\frac{1}{p^{3/2}}\right) + O\left(\frac{1}{N^{1/6}}\right)\right) + O(N^{1/3}) = \frac{\zeta(3/2)}{\zeta(3)}N^{1/2} + O(N^{1/3}),$$

where $\zeta(s) := \sum_{n\geq 1} 1/n^s$ is Riemann's zeta function.

For the rest of this section we study when $\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$ is powerful. Since

$$(2n-1)^2 - 8\binom{n}{2} = 1, \tag{8}$$

we see that the solutions to $\binom{n}{2} = d^3y^2$ with d squarefree, are in 1-1 correspondance with the integer solutions to

$$x^2 - 8d(dy)^2 = 1 \quad \text{with } d \text{ squarefree.} \tag{9}$$

(To see the reverse implication, simply note that x must be odd in (9) so taking $n = (x+1)/2$ gives, by (8), that $\binom{n}{2}$ is powerful). Proceeding as one does for the Pell equation, one finds that all solutions to (9) with d fixed are powers of a "fundamental solution"; that is, there exist integers r and s satisfying $r^2 - 8d(ds)^2 = 1$, such that every solution to (9) is of the form $x + dy\sqrt{8d} = (r + ds\sqrt{8d})^m$ for some integer m. We next investigate how to obtain the fundamental solution to (9) from the fundamental solution of the corresponding Pell equation:

If d is odd we let $D = 2d$ so that (9) becomes $x^2 - D(Dy)^2 = 1$.

If d is even we let $D = d/2$ so that (9) becomes $x^2 - D(8Dy)^2 = 1$.

Either way D is squarefree and there exists a fundamental solution to the Pell equation $u^2 - Dv^2 = 1$. We now determine the integer $m = m_d$ for which

$$r + ds\sqrt{8d} = r + D's\sqrt{D} = u_m + v_m\sqrt{D} := (u + v\sqrt{D})^m$$

(where $D' = D, 8D$ as d is odd or even). Evidently m_d is the smallest integer $m \geq 1$ for which D' divides v_m. By the binomial expansion we find that $v_m \equiv mu^{m-1}v$

(mod D). Since $u^2 - Dv^2 = 1$ we see that $(u, D) = 1$, and so $D|v_m$ if and only if D divides mv; that is $D/(v, D)$ divides m.

If d is even (so that D is odd) we need 8 to divide v_m.

• If v is even then $v_m \equiv mu^{m-1}v \pmod 8$; and, since u must be odd, $v_m \equiv 0 \pmod 8$ if and only if 8 divides mv. Thus $8/(8, v)$ must divide m.

• If v is odd then u is even. If m is odd then v_m is odd, so we may suppose that m is even. Then $v_m \equiv m(\sqrt{D}v)^{m-2}uv \pmod 8$ and so $v_m \equiv 0 \pmod 8$ if and only if 8 divides mu. Therefore $8/(8, u)$ divides m. Since m must be even, we conclude, in this case, that $8/(4, u)$ must divide m.

We deduce that $m_d = 2^{\rho_D} D/(v, D)$ with $\rho_D = 0, 1$ or 2. Therefore, the number of $n \le N$ with $\binom{n}{2}$ of the form d^3y^2 is $(v, D) \log N/2^{\rho_D} D \log(u + v\sqrt{D}) + O(1)$.

Thus, for any fixed d, we obtain $\gg \log N$ powerful $\binom{n}{2}$ with $n \le N$. Presumably the total number of powerful $\binom{n}{2}$ with $n \le N$ is $\sim c_4 \log N$ for some constant $c_4 > 0$. It can be shown that this is true, and that

$$c_4 = \sum_d \frac{\mu^2(d)}{\log(r + ds\sqrt{8d})} = \sum_D \frac{\mu^2(D)(v, D)}{2^{\rho_D} D \log(u + v\sqrt{D})},$$

provided that this sum converges.

Cohen and Lenstra's heuristics [2] suggest that, for almost all squarefree D, we have $\log(u+v\sqrt{D}) = D^{1/2+o(1)}$. Moreover, several conjectures[5] suggest that usually $(v, D) = D^{o(1)}$. Therefore we expect that $\log(r + ds\sqrt{8d}) \approx d^{3/2+o(1)}$ for almost all d, and so the above sum indeed converges.

We ran a computer search for small fundamental solutions in (9) with $d \le 10^5$. The first few values of n are, in ascending order (n_d will be the n coming from the fundamental solution for d):

$$n_2 = 2,\ n_3 = 243,\ n_{23} = 12168,\ n_{215} = 1431126,\ n_6 = 1825201,$$
$$n_5 = 19740250,\ n_7 = 5425069448,\ n_{10} = 865363202001,\ n_{3634} = 11968683934832.$$

8. Computer search for non-trivial powerful binomial coefficients

In this section we describe the computations which allow us to assert that the only binomial coefficients $\binom{n}{k}$, with $2 \le k \le n/2$ and $n \le 10^6$, which have the property that whenever p is a prime $\ge k$ dividing $\binom{n}{k}$ then also p^2 divides $\binom{n}{k}$, are $\binom{50}{3}$, and $\binom{n}{2}$ with $n = 2, 9, 50, 289, 1682, 9801, 57122$ or 332929 (which are all derived from n_2), $n = 243$ or 235225 (which are derived from n_3) or $n = n_{23} = 12168$.

To show this we will modify the proofs given in previous sections to be practical for computations. Our computations were all done in Maple V on a SPARCstation 5. Initially we explicitly computed all $\binom{n}{k}$ with $n \le 30$, so henceforth we will assume that whenever prime $p \ge k$ divides $\binom{n}{k}$ then so does p^2, with $30 < n \le 10^6$ and $2 \le k \le n/2$:

[5] For example, the Ankeny-Artin-Chowla conjecture states that $(p, v) = 1$ for the fundamental unit $(u + v\sqrt{p})/2$ for primes $p \equiv 1 \pmod 4$.

• Computations showed that the largest gap between primes $\le 10^6$ is 114 (following 492113). Thus by Liouville's argument (see just below the statement of Theorem 1) we deduce that $k < 114$.

• Computations showed that there exists an integer $jp \in (n-28, n]$, for each such $n \le 10^6$, with $j \le 28$ and p prime[6]. If $n > 3220$ then $p > (n-28)/28 \ge 114 > k$. If $k \ge 28$ then p cannot divide j, nor any other $n-i$ with $0 \le i < k$, and so p contradicts our assumption. Therefore if $28 \le k < 114$ then $n \le 3220$.

• The only gap, which is larger than 28, between primes < 3500, is the gap from 1327 to 1361. However $1341 = 9 \times 149$, so using the ideas in the two steps above, we deduce that if $28 \le k < 114$ then $n \ge 3500$.

We can thus assert that $k \le 27$. Note that $n-i$ must have property $(P)_{27}$ for $0 \le i < k$. (An integer m is said to have *property* $(P)_q$ if it may be written in the form $m = \tau\eta$, where η is powerful, τ is squarefree and has all of its prime divisors $\le q$ and $(\tau, \eta) = 1$.) To prove this, let τ be the product of all primes that divide m to the first power. By assumption τ only has prime divisors $< k \le 27$. The properties of η follow.

• We made a list of all $m \le 10^6$ having property $(P)_{27}$ $=(P)_{23}$ (by running through all possible divisors τ of $\prod_{p \le 23} p$, and multiplying τ by all $\eta = \delta^2\gamma^3$ where $(\tau, \delta\gamma) = 1$). This list does not contain six consecutive integers > 30. Therefore $k \le 5$, and integer n must have property $(P)_5$.

• We made a list of all $m \le 10^6$ having property $(P)_5$. The only three consecutive integers > 30 on the list were $48, 49, 50$ leading to the powerful $\binom{50}{3}$. There were 29 pairs of consecutive integers > 30 on the list. We computed $\binom{n}{2}$ in each of those cases to compile our list above.

9. Best possible examples

We now prove Proposition 2: Since q is a prime ≥ 5, we can deduce that x and y are both integers, not divisible by 3 and 2 respectively (by expanding $(3+2\sqrt{2})^q$ mod 9 and 8 respectively). We will show that if prime p divides xy then $p > k$. This implies that $(xy, k!) = 1$; but $(xy)^2 = n(n-1)/72$ divides $n(n-1)\dots(n-k+1)$, and so the theorem follows.

For any prime p in the range $k \ge p > 3$, consider the p-divisibility of the integers v_n given by $(3+2\sqrt{2})^n = u_n + v_n\sqrt{2}$. Evidently v_m divides v_n whenever $m|n$; and so there exists some integer $m = m_p$ such that $p|v_n$ if and only if $m|n$. Now $(3+2\sqrt{2})^p \equiv 3 \pm 2\sqrt{2} \pmod p$ and so $m_p|(p \mp 1)$. Thus $m_p \le p+1$. On the other hand, if $p|xy$ then $p|v_{2q}$ and so $m_p|2q$. However $q > k+1 \ge p+1 \ge m_p$ so $m_p = 1$ or 2, which is impossible since $v_1 = 2$ and $v_2 = 12$.

References

[1] Mlle. A.D., Nouv. Ann. Math. **16** (1857), 288-290.

[2] H. Cohen and H.W. Lenstra Jr., *Heuristics on class groups of number fields*, Lecture Notes in Math. **1068** (1984), 33–62.

[3] H. Davenport, *Multiplicative Number Theory*, vol. 2nd ed, Springer-Verlag, New York, 1980.

[4] P. Erdős, *On a Diophantine Equation*, J. London Math. Soc. **26** (1951), 176–178.

[6] We actually showed that the gaps, up to 10^6, between consecutive integers of the form jp, are all ≤ 28, which implies what is needed.

[5] P. Erdős and R.L. Graham, *Old and new problems and results in combinatorial number theory*, L'Enseign. Math., Geneva, 1980.
[6] P. Erdős and J.L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.
[7] C. Goldbach, *letter to D. Bernoulli* (July 23rd, 1724).
[8] A. Granville and O. Ramaré, *Explicit bounds on exponential sums and the scarcity of square-free binomial coefficients*, Mathematika **43** (1996), 73–107.
[9] R.K. Guy, *Unsolved Problems in Number Theory*, vol. 2nd ed, Springer-Verlag, New York, 1994.
[10] M. Langevin, *Cas d'égalité pour le Théorème de Mason et applications de la conjecture (abc)*, C.R. Acad. Sci. Paris **317** (1993), 441–444.
[11] J.W. Sander, *Prime power divisors of binomial coefficients*, J. reine angew Math **430** (1992), 1–20.
[12] P. Shiu, *On the number of squarefull integers between successive squares*, Mathematika **27** (1980), 171–178.

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA
E-mail address: andrew@math.uga.edu