Reprinted from the AMERICAN MATHEMATICAL MONTHLY
Vol. 97, No. 6, June–July 1990

Representing Binomial Coefficients as Sums of Squares

ANDREW GRANVILLE AND YILIANG ZHU, *University of Toronto*

ANDREW GRANVILLE: Having completed my B.A. and CASM at Cambridge University, I crossed the Atlantic in order to get my Ph.D. on Fermat's Last Theorem under the supervision of Paulo Ribenboim at Queen's University. Presently I am in my second year as a postdoctoral fellow at the University of Toronto. My current research interests include elementary number theory, solving Diophantine equations, studying the distributions of primes and of other special integers, and the theory of 3-designs.

YILIANG ZHU: Having completed my B.Sc. at Shanghai University of Science and Technology, I crossed the Pacific in order to pursue further studies. Life was very enjoyable during my M.Sc. Program at Queen's University. I now look forward to obtaining my Ph.D. in statistics at the University of Toronto, under the supervision of Nancy Reid.

1. Introduction. In the late eighteenth century, Lagrange proved that every positive integer can be represented as a sum of at most four squares of integers. This cannot be improved to three squares as there are infinitely many integers (e.g., 7) which cannot be represented as a sum of three squares of integers:

LEMMA 1 (Legendre, 1798). *A positive integer n cannot be expressed as the sum of three squares of integers if and only if n is of the form* $n = 2^{2k}(8m + 7)$ *where m and k are non-negative integers.*

In this article we shall prove two recent conjectures about whether various binomial coefficients can be written as the sum of less than four squares, using methods from the elementary theories of numbers, stochastic matrices and of graphs. First we will prove a conjecture stated by Alvan Beall, Blair Kelly, and Bob Morris at the Western Number Theory Conference in December, 1987:

THEOREM 1. *For every positive integer n, except* 1, 2, 3, 4, 5, 9, 14, 17, 18, 20, 21, 35 *and* 41, *there exists an integer* $m, 0 \le m \le n$, *divisible by* 4, *for which* $\binom{n}{m}$ *cannot be represented as a sum of three squares.*

We will also prove a conjecture of Neville Robbins [3]:

THEOREM 2. *The set of integers n, for which* $\binom{2n}{n}$ *cannot be represented as a sum of three squares, has asymptotic density* 1/8 *in the set of all natural numbers.*

Our proof of Theorem 1 will rely on the following result, which we shall prove in Section 2:

PROPOSITION 1. *Suppose that m and n are positive integers with m divisible by* 4. *If* $\binom{n}{m}$ *cannot be written as the sum of three squares then neither can* $\binom{2n}{2m}$ *nor* $\binom{2n+1}{2m}$.

We define E_1 to be the set of exceptional n in the hypothesis of Theorem 1. We define S to be the set of positive integers that cannot be written as the sum of three squares of integers. We can now give the

Proof of Theorem 1. Let E_2 and E_3 be the sets of values of n that are given in Tables I and II respectively. We see there that for each such n there exists a value of m for which $\binom{n}{m} \in S$; moreover if $n \in E_3$, then m is divisible by 4.

TABLE I. The least m with $\binom{n}{m} \in S$, for each $n \in E_2$.

m	n	m	n	m	n
1	7, 28, 71, 284	9	164	17	142
2	8, 11, 43, 57, 136	10	40	18	37
3	82	11	56	19	73
5	10, 34, 83	14	36		
6	19, 165	15	68		

TABLE II. The least m, divisible by 4, with $\binom{n}{m} \in S$, for each $n \in E_3$.

n	Binary Expansion	m	n	Binary Expansion	m
16	10000	4	81	1010001	4
272	100010000	4	328	101001000	100
273	100010001	20	329	101001001	28
137	10001001	52	330	101001010	36
69	1000101	20	331	101001011	12
70	1000110	4	166	10100110	4
568	1000111000	100	167	10100111	28
569	1000111001	84	42	101010	20
285	100011101	4	86	1010110	68
143	10001111	12	87	1010111	4
72	1001000	28	22	10110	20
146	10010010	36	23	10111	4
147	10010011	44	6	110	4
74	1001010	12	112	1110000	44
75	1001011	36	113	1110001	36
38	100110	4	114	1110010	60
39	100111	12	115	1110011	4
80	1010000	20	29	11101	4
			15	1111	12

One can also see, from Table II, that for any positive integer n, not in $E_1 \cup E_2$, there exists an integer $e \in E_3$ such that the first few digits in binary notation of n are precisely those of e: in other words, there exist integers k and r such that $0 \le r \le 2^k - 1$ where

$$n = e \cdot 2^k + r.$$

(As an example, suppose that $n = 13 = (1101)_2$ in binary notation. Now $6 = (110)_2 \in E_3$ and so $13 = 6.2 + 1$. Try also $575 = (1000111111)_2$; we have $143 = (10001111)_2 \in E_3$ and so $575 = 143.2^2 + 3$.)

We shall prove that for any positive integer $n \notin E_1 \cup E_2$ there exists a value of m, divisible by 4, for which $\binom{n}{m} \in S$, by induction on k.

For $k = 0$, this is trivial as $n = e \in E_3$, and the value of m is given in Table II. So suppose the result holds for $k - 1$:

For $n = e2^k + r$ let $s = r/2$ (r even), $(r - 1)/2$ (r odd) and $p = e2^{k-1} + s$. As $0 \le s \le 2^{k-1} - 1$, we have a value of t, divisible by 4, for which $\binom{p}{t} \in S$, by the induction hypothesis. Therefore, $\binom{n}{2t} \in S$ by Proposition 1.

Remark. We see, from the proof, that if $n = e2^k + r$ where $e \in E_3$ and $\binom{e}{m}$ cannot be written as the sum of three squares, then neither can $\binom{n}{2^k m}$.

We will prove a stronger result than Theorem 2 in Section 3:

THEOREM 3. *For $a = 0, 1, 2$ and 3,*

$$\#\{n \le x : n \equiv a \pmod 4, n! \in S\} = x/32 + o(x).$$

We see that Theorem 2 follows easily from Theorem 3 by the following result, which we'll prove in Section 2:

PROPOSITION 2. *For any positive integers m and n,*

$$n \in S \quad \text{if and only} \quad m^2 n \in S.$$

Proof of Theorem 2.

$$\begin{aligned}\#\left\{n \le x : \binom{2n}{n} \in S\right\} &= \#\{n \le x : (2n)! \in S\} \quad \text{by Proposition 2} \\ &= \#\{m \le 2x : m \equiv 0 \pmod 2 \quad \text{and} \quad m! \in S\} \\ &= x/8 + o(x) \quad \text{by Theorem 3.}\end{aligned}$$

Theorem 2 is perhaps surprising, as the positive integers $n \le x$, for which $n \in S$, actually have density $1/6$. By Lemma 1,

$$\begin{aligned}\#\{n \le x : n \in S\} &= \sum_{k \ge 0} \#\{n \le x : n = 2^{2k}(8m + 7) \quad \text{for some} \quad m \ge 0\} \\ &= \sum_{k=0}^{\log x} \{x/2^{2k+3} + 0(1)\} \\ &= x/6 + 0(\log x).\end{aligned}$$

However, the reason that we get $1/8$ in Theorem 2 (instead of $1/6$) can most easily be explained by realizing that the parity of the power of 2 dividing $n!$ is equally distributed between even and odd, whereas this is not the case for ordinary integers.

2. Sequences of 0's and 1's (Proofs of Propositions 1 and 2). Any positive integer n can be written in the form $2^a b$ where a and b are nonnegative integers, and b is odd. Let $v(n)$ be the residue class of $a \pmod 2$ and $f(n)$ be the residue class of $b \pmod 8$. Lemma 1 may be expressed as

$$n \in S \quad \text{iff} \quad v(n) = 0 \quad \text{and} \quad f(n) = 7. \tag{1}$$

We also note that

$$v(mn) = v(m) + v(n) \quad \text{and} \quad f(mn) = f(m)f(n). \tag{2}$$

for any integers m and n. We can immediately give the

Proof of Proposition 2. By (2) we see that

$$v(m^2n) = 2v(m) + v(n) = v(n) \quad \text{and} \quad f(m^2n) = f(m)^2 f(n) = f(n).$$

Thus, by (1), $n \in S$ iff $v(n) = 0$, and $f(n) = 7$

$$\text{iff} \quad v(m^2n) = 0, \quad \text{and} \quad f(m^2n) = 7$$

$$\text{iff} \quad m^2n \in S.$$

Define $w(n) = v(n!)$ and $g(n) = f(n!)$. Also, for any fixed sequence $\alpha\beta \cdots \chi$ of 0's and 1's, define $\sigma_{\alpha\beta \ldots \chi}(n)$ to be the number of occurrences of this sequence in the binary expansion of n. We prove

LEMMA 2. *For any given positive integer n,*
(a) $w(n) \equiv n - \sigma_1(n) \pmod 2$, *and*
(b) $g(n) \equiv 3^{\sigma_{011}(n)+\sigma_{100}(n)} 7^{\sigma_{101}(n)+\sigma_{110}(n)} \pmod 8$.

Proof. Suppose that the binary expansion of n is $\sum_{i=0}^{d} a_i 2^i$ where each $a_i = 0$ or 1. Then the power of 2 dividing $n!$ is

$$\sum_{j \geq 1} \left[\frac{n}{2^j} \right] = \sum_{j \geq 1} \sum_{i=j}^{d} a_i 2^{i-j} = \sum_{i=1}^{d} a_i \sum_{j=1}^{i} 2^{i-j}$$

$$= \sum_{i=1}^{d} a_i (2^i - 1) = n - \sigma_1(n).$$

Now, as

$$\prod_{\substack{j=1 \\ j \text{ odd}}}^{m} j \equiv \begin{cases} 1 & \\ 3 & \text{if} \\ 7 & \end{cases} \begin{matrix} m \equiv 0,1,2,7 \\ m \equiv 3,4 \\ m \equiv 5,6 \end{matrix} \pmod 8,$$

we can see that

$$g(n) = \prod_{k \geq 0} \prod_{\substack{i=1 \\ 2^k \| i}}^{n} \frac{i}{2^k} = \prod_{k \geq 0} \prod_{\substack{j=1 \\ j \text{ odd}}}^{[n/2^k]} j \pmod 8$$

$$= 3^{\#\{k \geq 0 : \tau_k = 3 \text{ or } 4\}} 7^{\#\{k \geq 0 : \tau_k = 5 \text{ or } 6\}} \pmod 8$$

where $\tau_k = 4a_{k+2} + 2a_{k+1} + a_k$, which establishes the result.

By noting that $3^a 7^b \equiv 7 \pmod 8$ if and only if a is even and b is odd, we can deduce, from Lemma 2 and (1), the following result.

COROLLARY 1. *For a given positive integer n, $n!$ is an element of S if and only if* (i) $\sigma_1(n) \equiv n \pmod 2$, (ii) $\sigma_{011}(n) \equiv \sigma_{100}(n) \pmod 2$ *and* (iii) $\sigma_{101}(n) \equiv \sigma_{110}(n) + 1 \pmod 2$.

In practice, Corollary 1 provides an efficient algorithm for determining whether $n!$ is an element of S: Simply write n in its binary notation, count the frequency of occurrences of the various digit patterns 1, 011, 100, 101 and 110, and then check whether (i), (ii), and (iii) are satisfied.

We can also deduce from Lemma 2:

COROLLARY 2. *For any positive integer* n, $w(2n+1) = w(2n) \equiv w(n) + n \pmod 2$ *and* $g(2n+1)/g(n)$ *and* $g(2n)/g(n)$ *are congruent to* 1 *and* 1, 3 *and* 1, 7 *and* 3, *and* 1 *and* 7 $\pmod 8$ *as* $n \equiv 0, 1, 2, 3 \pmod 4$, *respectively*.

Proof. $w(2n+1) - w(2n) = v(2n+1) = 0$, by definition, and $w(2n) - w(n) \equiv (2n - \sigma_1(2n)) - (n - \sigma_1(n)) \equiv n \pmod 2$ by Lemma 2(a). Also $g(2n+1)/g(2n) \equiv 2n + 1 \pmod 8$ and $g(2n)/g(n) \equiv 1, 1, 3$ and $7 \pmod 8$ as $n \equiv 0, 1, 2, 3 \pmod 4$ by Lemma 2(b).

From this, we can immediately deduce

COROLLARY 3. *Suppose that* m *is divisible by* 4 *with* $0 \le m \le n$. *Then*

$$v\left(\binom{2n+1}{2m}\right) = v\left(\binom{2n}{2m}\right) = v\left(\binom{n}{m}\right)$$

and

$$f\left(\binom{2n+1}{2m}\right) = f\left(\binom{2n}{2m}\right) = f\left(\binom{n}{m}\right).$$

Proposition 1 follows immediately from (1) and Corollary 3.

3. Proof of Theorem 3. Define $g(0) = 1, w(0) = 0$ and let

$$T(x, a; g, w) = \#\{0 \le n < x : n \equiv a \pmod 4, \quad g(n) = g \quad \text{and } w(n) = w\}$$

for

$$a = 0, 1, 2, \text{or } 3, \quad g = 1, 3, 5 \text{ or } 7 \quad \text{and} \quad w = 0 \text{ or } 1 \ldots . \tag{3}$$

Let $p(x, a; g, w) = T(x, a; g, w)/x$, which can be thought of as the "probability" that an integer $n < x$ has the properties that $n \equiv a \pmod 4$, $g(n) = g$ and $w(n) = w$. By (1), Theorem 3 is evidently implied by

THEOREM 4. *For each* a, g *and* w *in the range* (3), *we have*

$$p(x, a; g, w) \sim 1/32 \quad \text{as} \quad x \to \infty.$$

We shall prove, in Section 4,

PROPOSITION 3. *Fix* $\varepsilon > 0$. *If* n *is sufficiently large* ($> n_\varepsilon$ *say*), *then*

$$\left| p(2^{43n}x, a; g, w) - \frac{1}{32} \right| < \varepsilon$$

for any a, g *and* w *in the range* (3) *and integer* $x \ge 1$.

From this, we can immediately give the

Proof of Theorem 4. Fix $\varepsilon > 0$ and choose $n > n_{\varepsilon/2}$ (where n_ε is as in Proposition 3). For any $z > 2^{43n}(1 + 2/\varepsilon)$ choose x to be that integer for which $2^{43n}(x-1) < z \le 2^{43n}x$. Then

$$\left| T(z, a; g, w) - \frac{z}{32} \right| \le \left| T(2^{43n}x, a; g, w) - \frac{2^{43n}x}{32} \right| + 2^{43n}$$

$$\le 2^{43n}\left(\frac{\varepsilon x}{2} + 1\right) < \varepsilon z.$$

4. Stochastic matrices. Let $p(x)$ be the 32 by 1 vector with entries $p(x, a, g, w)$. Let Q be the 32 by 32 matrix indexed in both directions by (a, g, w); where the entry in the (a', g', w')th row and (a, g, w)th column is

$$1/2 \quad \text{if} \quad a' = \begin{cases} 0 \\ 0 \\ 1 \\ 1 \\ 2 \\ 2 \\ 3 \\ 3 \end{cases} \qquad a = \begin{cases} 0 \\ 2 \\ 0 \\ 2 \\ 1 \\ 3 \\ 1 \\ 3 \end{cases} \qquad g'/g \equiv \begin{cases} 1 \\ 3 \\ 1 \\ 7 \\ 1 \\ 7 \\ 3 \\ 1 \end{cases} \pmod 8 \qquad w' - w \equiv \begin{cases} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{cases} \pmod 2$$

0 otherwise.

Note that Q is a doubly stochastic matrix all of whose entries are non-negative. (A matrix M is said to be stochastic if the sum of the entries in each of its columns is 1, doubly stochastic if the same is true for each of its rows). In Section 5 we shall prove

PROPOSITION 4. *$A = Q^{43}$ is a doubly stochastic matrix all of whose entries are positive.*

Now Corollary 2 implies that $p(2x) = Qp(x)$ for any positive integer x; by iterating this n times we get

LEMMA 3. *For any positive integers n and x, $p(2^n x) = Q^n p(x)$.*

For a given matrix M and vector x we say that $\lim_{n\to\infty} M^n x$ exists and equals y if the ith component of $M^n x$ tends to the ith component of y as n tends to ∞, for each i. An important result on stochastic matrices has been given by Perron (see [1, p. 216] for a nice proof).

LEMMA 4. *Suppose that M is a stochastic matrix all of whose entries are positive. There exists a vector a $(= a(M))$ such that, for* any *stochastic vector v with components all nonnegative, we have $\lim_{n\to\infty} M^n v = a$.*

We can now give a proof of Proposition 3 by using the three results directly above:

Proof of Proposition 3. $M = Q^{43}$ is a doubly stochastic matrix, all of whose entries are positive, by Proposition 4. Let v be the 32×1 vector with each entry equal to $1/32$. As each row sum of M is 1 we see that $Mv = v$, and so the value of a in Lemma 4 is given by

$$a = \operatorname*{Lim}_{n\to\infty} M^n v = \operatorname*{Lim}_{n\to\infty} v = v.$$

Therefore,

$$\operatorname*{Lim}_{n\to\infty} p(2^{43n}x) = \operatorname*{Lim}_{n\to\infty} M^n p(x) \qquad \text{by Lemma 3,}$$

$$= v \qquad \text{by Lemma 4,}$$

and the result follows immediately, by definitions.

5. Graphs of Stochastic matrices. Suppose that M is an $n \times n$ matrix, all of whose entries are non-negative. The directed graph $G(M)$ of such a matrix is obtained by taking n vertices $v_1, \dots, v_n$ and putting a directed edge from v_i to v_j if and only if the (i, j)th entry of M is non-zero. A path of length k from v to w is a sequence of k (not necessarily distinct) directed edges, starting at v and ending at w; e.g.,

$$v = a_0 \text{ to } a_1, a_1 \text{ to } a_2, a_2 \text{ to } a_3, \dots, a_{k-1} \text{ to } a_k = w.$$

From this definition we have

LEMMA 5. *Suppose that M is an $n \times n$ matrix all of whose entries are non-negative and k is a positive integer. Every entry of M^k is positive if and only if there is a directed path of length k, in both directions, between every pair of (not necessarily distinct) vertices in $G(M)$.*

Proof of Proposition 4. It is not difficult to show that the product of any two doubly stochastic matrices is itself doubly stochastic; therefore, as Q is doubly stochastic, so are $Q^2, Q^3, \dots, Q^{43} = A$.

In FIGURE 1 we give a subgraph of $G(Q)$. By visual inspection one can see that there is a directed path of length $a_v (\le 17)$ from v to 071, and one of length $b_v (\le 26)$ back from 071 to v, for each vertex v in $G(Q)$. Therefore, for any pair of (not necessarily distinct) vertices v and w in $G(Q)$ we let P_{vw} be the path given by joining the path of length a_v from v to 071, to $43 - a_v - b_w$ circuits of the edge from 071 to itself, to the path of length b_w from 071 to w. As P_{vw} has length 43 in each case, we know that every entry of $A = Q^{43}$ is positive, by Lemma 5.

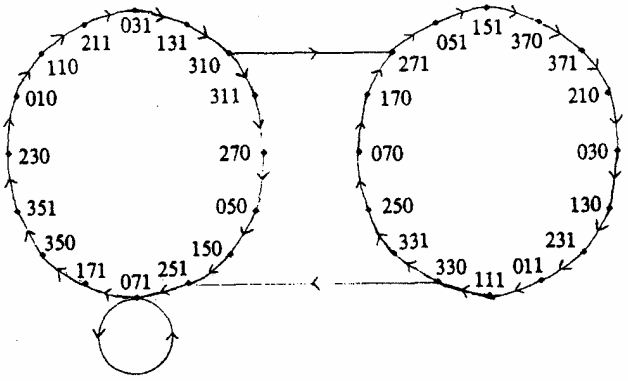

FIG. 1. The vertices are indexed by three numbers which, in order, correspond to a, g and w.

6. Some final comments. A number of related questions can be asked:

1. If we fix k what is the density of integers n for which $\binom{n}{k} \in S$? It seems possible to derive a complicated general formula that gives a variety of different values as we vary over values of k.

2. In the proof of Theorem 1 the values of $m \to \infty$ as $n \to \infty$. Is it true that there exists an integer m_0, such that for all $n \notin E_1$ we have $\binom{n}{m} \in S$ for some $m \le m_0$? The answer to this is yes with $m_0 = 74$; however our proof is extremely

complicated and uses the idea of an *infinite* system of congruences that cover the integers (see [2] for a review).

3. Let $P(n)$ be the number of integers m in row n of Pascal's triangle for which $\binom{n}{m} \in S$. Let $\Pi(N) = P(1) + P(2) + \cdots + P(N)$. Does $\operatorname{Lim}_{N\to\infty} \Pi(N)/(N^2/2)$ exist? If so, what is it?, i.e., is there a density of integers in Pascal's triangle that are not representable as a sum of three squares?

REFERENCES

1. J. M. Ortega, Matrix Theory, A Second Course, Plenum, New York, 1987.
2. S. Porubsky, Results and problems on covering systems of residue classes, *Math. Seminar Giessen*, 150 (1981) 85.
3. N. Robbins, Representing $\binom{2n}{n}$ as a sum of squares, *Fib. Quarterly*, 25 (1987) 29–33.