From (4), we have

$$P(X_m^n = k) \to \frac{1}{k!}\left(\frac{1}{\alpha}\right)^k e^{-1/\alpha}.$$

Thus we obtain our main result.

THEOREM. *Let X_m^n be the number of matches. When $m = [\alpha n]$ and α is any real number greater than or equal to 1, the limiting distribution of X_m^n is the Poisson distribution with parameter $1/\alpha$.*

It turns out that this approximation is remarkably good for moderate values of n. Table 1 gives the comparison between the Poisson approximation and the exact probability of random variable X_m^n when $\alpha = 2, 3, 5$, with $m = \alpha n$.

REFERENCES

1. W. Feller, An Introduction to Probability and Its Applications, Vol. 1, 3rd ed., Wiley, New York, 1968.
2. N. L. Johnson and S. Kotz, Urn Models and Their Application, Wiley, New York, 1977.
3. S. M. Ross, Introduction to Probability Models, 2nd ed., Academic Press, 1980.

Computing Binomial Coefficients

P. GOETGHELUCK
Université de Paris-sud, Department de Mathématiques, Bat 425, 91405 Orsay cedex, France.

The purpose of this paper is to show how results of the last century about binomial coefficients have been rediscovered with a micro-computer and the way that they can be used to compute $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ for large values of n.

1. Introduction. The usual means for computing binomial coefficients is based on the formula

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

and tables such as [5] have been constructed using this relation. Unfortunately, to get for instance the value of $\binom{1000}{353}$ you have to compute $353 \times (1000 - 353) = 228391$ terms of Pascal's triangle.

Our aim is to give a fast process to get the factorization of $\binom{n}{k}$ into primes. The exact value of $\binom{n}{k}$ is easy to obtain from the factorization.

NOTATION. Let I and J be two positive integers and a_i's and b_i's defined by

$$I = a_r 2^r + a_{r-1}2^{r-1} + \cdots + a_1 2 + a_0,$$

$$J = b_r 2^r + b_{r-1}2^{r-1} + \cdots + b_1 2 + b_0, \quad 0 \leqslant a_i, b_i \leqslant 1 \quad (i = 0, \ldots, r).$$

Using Boolean notation we set

$$(I \text{ and } J) = c_r 2^r + \cdots + c_1 2 + c_0, \quad c_i = \operatorname{Min}(a_i, b_i) \quad (i = 0, \dots, r),$$
$$(I \text{ or } J) = d_r 2^r + \cdots + d_1 2 + d_0, \quad d_i = \operatorname{Max}(a_i, b_i) \quad (i = 0, \dots, r).$$

EXAMPLE:

$43 \rightleftarrows 101011$, $25 \rightleftarrows 011001$, $(43 \text{ and } 25) \rightleftarrows 001001$,

$(43 \text{ or } 25) \rightleftarrows 111011$ then $(43 \text{ and } 25) = 9$, $(43 \text{ or } 25) = 59$.

2. Factorization of binomial coefficients into primes. We start with the following remark. The pattern of Fig. 1 was obtained with a computer by two different ways:

(1) for every $(n, k) \in \mathbb{N}^2$ (n, k) is plotted if and only if $\binom{n}{k}$ is odd (an analogous pattern can be seen in [**8**]);

(2) for every $(I, J) \in \mathbb{N}^2$ $((I \text{ or } J), (I \text{ and } J))$ is plotted.

This observation suggests that

(R1) $\binom{n}{k}$ is divisible by 2 if and only if $\binom{n}{k}$ cannot be written as $((I \text{ or } J), (I \text{ and } J))$.

This is the same as:

(R2) Let n and k be two positive integers ($k \leqslant n$), $n = a_r \dots a_0$ and $k = b_r \dots b_0$ their binary representation. $\binom{n}{k}$ is divisible by 2 if and only if there exists i such that $b_i > a_i$.

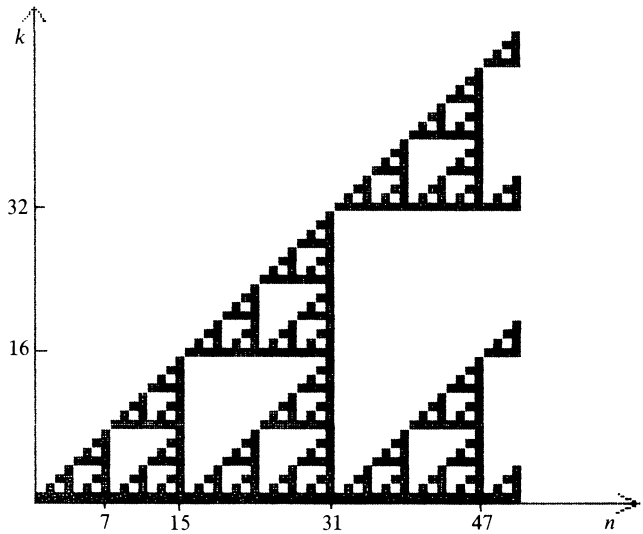

FIG. 1. Odd binomial coefficients.

The last result, discovered here by studying diagrams, is not only true but is an easy corollary of a theorem known as Lucas' Lemma ([**1**] and [**4**, p. 417]).

THEOREM. *Let n and k be two positive integers and p be a prime. Let $a_r \dots a_0$ and $b_r \dots b_0$ be the p-ary representation of n and k, respectively. Then*

$$\binom{n}{k} \equiv \binom{a_r}{b_r}\binom{a_{r-1}}{b_{r-1}} \cdots \binom{a_0}{b_0} \pmod p$$

(*with conventional value* $\binom{a}{b} = 0$ *if* $a < b$).

A natural question arises: What is the power of 2 in the factorization of $\binom{n}{k}$ into primes? The pattern of Fig. 2 shows binomial coefficients divisible by 2 but not by 4 and on Fig. 3 binomial coefficients divisible by 4 but not by 8. These drawings suggest there is an underlying mathematical reason for their regularity. The list of n and k such that (n, k) is plotted either in Fig. 2 or 3 is easily provided by the computer. A careful examination of the list shows that

(R3) The power of 2 in the factorization of $\binom{n}{k}$ into primes is equal to the number of borrow(s) in the subtraction $n - k$ in base 2.
Furthermore, computational experiments show that (R3) remains valid when replacing 2 by any prime:
(R4) Let p be a prime. The power of p in the factorization of $\binom{n}{k}$ into primes is equal to the number of borrow(s) in the subtraction $n - k$ in base p.

This result (re)discovered by the author on a micro-computer was already known though never formulated as (R4). The first version of (R4) by Kummer ([**3**] pp. 115–116), rephrased by Singmaster [**7**], says:
(R5) The power of p in the factorization of $\binom{n}{k}$ into primes is equal to the number of carry(ies) when summing $(n - k)$ and k.
A second version of (R4) is due to Kazantzidis [**2**].

Now we give a sketch for an elementary proof of (R4) providing an algorithm for computing the power of p in the factorization into primes (for extensive proofs see [**2**], [**3**], [**7**]).

(1) The power of p in the factorization of $n!$ into primes is $\Sigma_{i>0}[n/p^i]$. ($[x]$ denotes the greatest integer lower than or equal to x.)
(2) The power of p in the factorization of $\binom{n}{k}$ into primes is:

$$E(n, k) = \sum_{i>0} \left([n/p^i] - [k/p^i] - [(n-k)/p^i]\right). \tag{1}$$

(3) Writing $n = a_n p^2 + b_n p + c_n$, $k = a_k p^2 + b_k p + c_k$, with $0 \leqslant b_i,\ c_i < p$ $(i = k, n)$ we have:

(a) $E(n, 0) = 0$.
(b) If $c_n \geqslant c_k$, then $E(n, k) = E([n/p], [k/p])$.

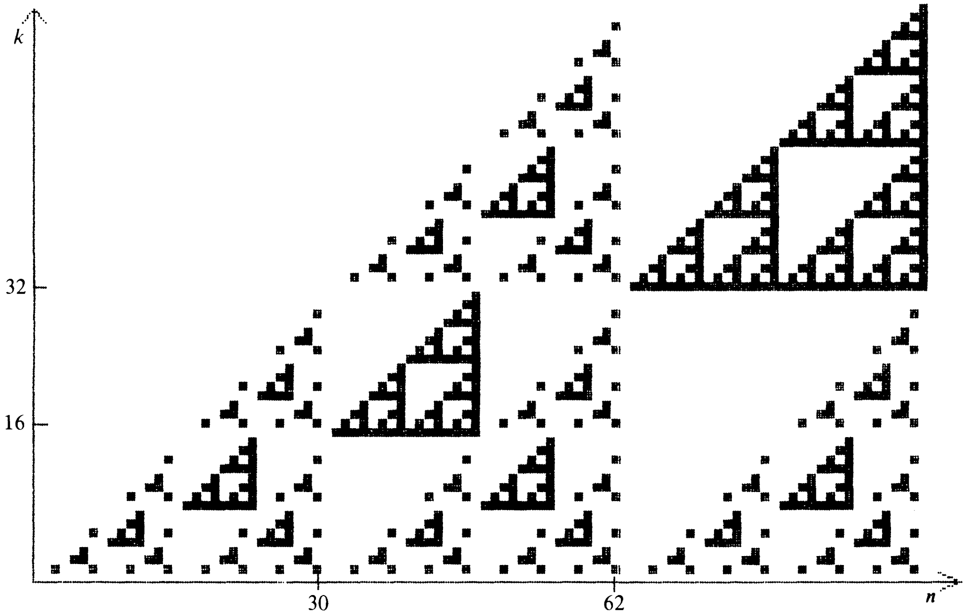

FIG. 2. Binomial coefficients divisible by 2 but not by 4.

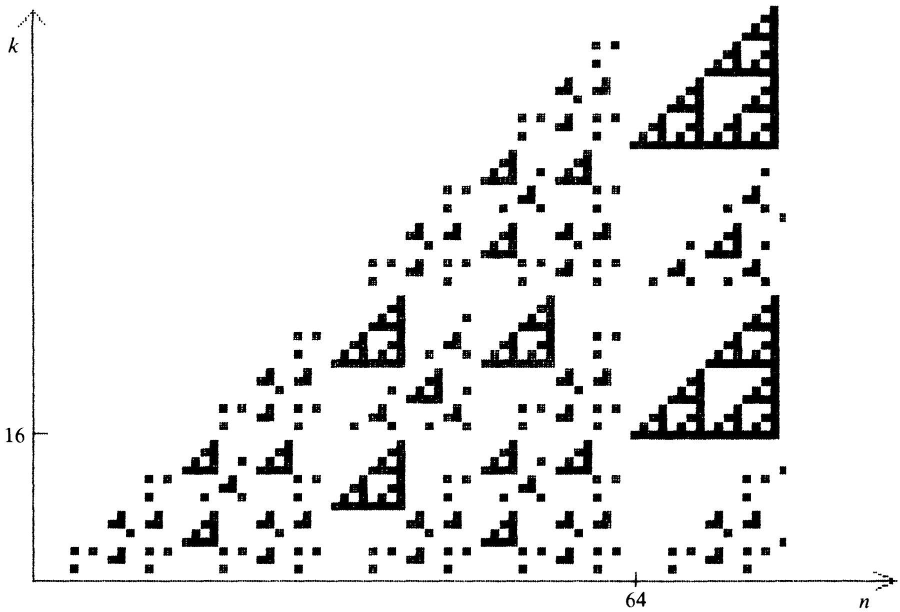

FIG. 3. Binomial coefficients divisible by 4 but not by 8.

(c) If $c_n < c_k$ and $b_n \neq b_k$, then $E(n, k) = E([n/p], [k/p]) + 1$.
(d) If $c_n < c_k$, $b_n = b_k$ and $b_n \neq 0$, then $E(n, k) = E([n/p] - 1, [k/p]) + 1$.
(e) If $c_n < c_k$ and $b_n = b_k = 0$, then $E(n, k) = E([n/p], [k/p] + 1) + 1$.

(Proofs of (b), (c), (d) and (e) are made using (1) and $[[n/p]/p^i] = [n/p^{i+1}]$).

(4) Denoting by $B(n, k)$ the number of borrow(s) in the subtraction $n - k$ in base p, we easily see that $B(n, k)$ satisfies the same induction relations as $E(n, k)$ and then is equal to $E(n, k)$.

3. Algorithm for computing the power of primes in the factorization. Let us note that formula (1) gives

$$E = 1, \quad \text{if } n - k < p \leqslant n,$$
$$E = 0, \quad \text{if } n/2 < p \leqslant n - k.$$

Furthermore if $p > n^{1/2}$, n and k have at most two digits in base p, and there is at most one borrow (on the least significant digits of n and k) in the subtraction $n - k$ in base p.

We denote by INT(x) the greatest integer lower than or equal to x, and by $\leftarrow$ the assignment operation.

The following algorithm gives the power E of the prime p in the factorization of $\binom{n}{k}$ into primes:

(1) Input n, k and p.
(2) $E \leftarrow 0$, $r \leftarrow 0$.
(3) If $p > n - k$ then $E \leftarrow 1$; end.
If $p > n/2$ then $E \leftarrow 0$; end.
If $p * p > n$ then if $n \bmod p < k \bmod p$ then $E \leftarrow 1$; end.
Repeat
(a) $a \leftarrow n \bmod p$, $n \leftarrow \text{INT}(n/p)$,
$b \leftarrow (k \bmod p) + r$, $k \leftarrow \text{INT}(k/p)$.
(b) If $a < b$ then $E \leftarrow E + 1$, $r \leftarrow 1$
else $r \leftarrow 0$.
until $n = 0$.
end.

4. Computation of $\binom{n}{k}$. From (R4), if a prime p satisfies $p > n$, n is not divisible by p. Then to factorize $\binom{n}{k}$ it is sufficient to compute the power of primes p such that $p \leqslant n$ which can be done quickly using the preceding algorithm. Knowing the factorization we can reconstruct the binomial coefficient by a classical multiprecision computation (large integers are stored as one-dimensional arrays of small integers, and the multiplication of two large integers is performed on the components of arrays taking care of the carries between successive components. For more details see [**6**, p. 332]) and we get easily $\binom{n}{k}$'s which are not available in tables for $n > 200$.

Example. The following computation, performed on a micro-computer with a 5 mhz 8086 CPU running CP/M, spends less than half a second to get the factorization and about 8 seconds for the exact value. (Program written in PASCAL)

Factorization of $\binom{1000}{353}$ into primes :

$2^3 \times 3^6 \times 5^3 \times 11 \times 19 \times 29 \times 31^2 \times 37 \times 41 \times 47 \times 59 \times 61 \times 71 \times$
$73 \times 83 \times 89 \times 97 \times 109 \times 131 \times 137 \times 139 \times 163 \times 179 \times 181 \times 191 \times 193 \times$
$197 \times 199 \times 223 \times 227 \times 229 \times 233 \times 239 \times 241 \times 331 \times 359 \times 367 \times 373 \times 379 \times$
$383 \times 389 \times 397 \times 401 \times 409 \times 419 \times 421 \times 431 \times 433 \times 439 \times 443 \times 449 \times 457 \times$
$461 \times 463 \times 467 \times 479 \times 487 \times 491 \times 499 \times 653 \times 659 \times 661 \times 673 \times 677 \times 683 \times$
$691 \times 701 \times 709 \times 719 \times 727 \times 733 \times 739 \times 743 \times 751 \times 757 \times 761 \times 769 \times 773 \times$
$787 \times 797 \times 809 \times 811 \times 821 \times 823 \times 827 \times 829 \times 839 \times 853 \times 857 \times 859 \times 863 \times$
$877 \times 881 \times 883 \times 887 \times 907 \times 911 \times 919 \times 929 \times 937 \times 941 \times 947 \times 953 \times 967 \times$
$971 \times 977 \times 983 \times 991 \times 997$.

Exact value of $\binom{1000}{353}$:

2 5229445633 0659742351 4408025205 5773735613 0435153119
5689363559 4388544559 6891848033 3018014952 8141512945 3596585561
6639939234 6118918439 7715091949 2045952055 6252295683 8053320988
8250237463 6769258037 6666922328 1259276867 8750591171 8832270161
1589146743 0491067982 6394724366 5313803538 2214107000 .

Truncated value : 2.52×10^{280} .

REFERENCES

1. N. J. Fine, Binomial coefficients modulo a prime, this MONTHLY, 54 (1947) 589.
2. G. S. Kazantzidis, On a congruence and a practical method for finding the highest power of a prime p which divides the binomial coefficient $\binom{A}{B}$, Bull. Soc. Math. Grèce n.s. 6 II (1965) Fasc. 2, 358–360. MR 34# 7440.
3. E. E. Kummer, Uber die Erganzumgssatze zu den allgemeinen Reciprocitatsgesetzen, J. Reine Angew. Math., 44 (1852) 93–146.
4. E. Lucas, Théorie des Nombres, Blanchard, Paris, 1961.
5. J. C. P. Miller, Table of Binomial Coefficients, University Press, Cambridge, 1964.
6. H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhauser, Boston, 1985.
7. D. Singmaster, Notes on binomial coefficients I. A generalization of Lucas' congruence, J. London Math. Soc., (2) 8 (1974) 545–548.
8. S. Wolfram, Geometry of binomial coefficients, this MONTHLY, 91 (1984) 566.