The Arithmetic of Binomial Coefficients

D. B. Fuchs and M. B. Fuchs

Every student knows the formulas

$$(1+x)^2 = 1+2x+x^2,$$
$$(1+x)^3 = 1+3x+3x^2+x^3.$$

The numbers (1, 2, 1), (1, 3, 3, 1), as well as numbers obtained in an analogous way by raising $(1+x)$ to the fourth power, the fifth power, and so on, are called *binomial coefficients*. This article deals with various properties of binomial coefficients. In the first section we lay out the "general theory": Most of the theorems we prove here used to be part of the school curriculum. In the second section we will show a very easy way to find the remainder when a binomial coefficient is divided by a prime number. The third, and concluding, section deals with certain remarkable properties of binomial coefficients. The main assertions in this section are formulated as hypotheses. Perhaps the readers of *Kvant*[1] will try to prove them.

1. Definition and Simplest Properties of Binomial Coefficients.

If the binomial $1+x$ is raised to some power n, where n is a natural number, then the result will obviously be a polynomial of degree n (i.e., the greatest power to which x will appear in this polynomial will be equal to n). For example:

$$(1+x)^0 = 1,$$
$$(1+x)^1 = 1+x,$$
$$(1+x)^2 = 1+2x+x^2,$$
$$(1+x)^3 = 1+3x+3x^2+x^2,$$
$$(1+x)^4 = 1+4x+6x^2+4x^3+x^4,$$
$$(1+x)^5 = 1+5x+10x^2+10x^3+5x^4+x^5.$$

The coefficients of these polynomials are called binomial coefficients. There is a special notation for them: The coefficient of x^m in $(1+x)^n$ is denoted by $\binom{n}{m}$. For example, $\binom{2}{1} = 2$, $\binom{4}{2} = 6$, $\binom{5}{3} = 10$. Old algebra textbooks call the number $\binom{n}{m}$ "the number of combinations of n things taken m at a time." There are reasons for

The Russian original is published in *Kvant* 1970, no. 6, pp. 17–25.

[1] *Translation editor's note*: And the readers of this book!

this, but we won't go into them here: For our purposes, they are not important. Thus,

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n. \tag{1}$$

From this, it is easy to obtain that

$$(a+x)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}x + \binom{n}{2}a^{n-2}x^2 + \cdots + \binom{n}{n}x^n$$

holds as well (all you have to do is apply formula (1) to $(1+\frac{x}{a})^n$ and then multiply both sides of the resulting equation by a^n). This last formula is called *Newton's binomial.* This is where the term "binomial coefficient" comes from.

It is clear that the numbers $\binom{n}{m}$ are nonnegative integers and that $\binom{n}{m} = 0$ for $m > n$ (the polynomial $(1+x)^n$ has degree n, and x^m with $m > n$ doesn't appear in it). It is easy to convince yourself, furthermore, that $\binom{n}{0} = \binom{n}{n} = 1$. The other binomial coefficients $\binom{n}{m}$, where $0 < m < n$, can be found by raising $1+x$ to various powers. Their values for $n \leq 10$ are shown in Table 1.

TABLE 1. Binomial coefficients.

n \ m	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0
9	1	9	36	84	126	126	84	36	9	1	0
10	1	10	45	120	210	252	210	120	45	10	1

We see that binomial coefficients increase rather rapidly. The observant reader will notice certain patterns in the arrangement of these numbers. As a rule, such patterns are easily deduced from the definition of binomial coefficients. We will prove only the most important ones here. Let us begin with the most important one of all, *Pascal's identity.*

THEOREM 1 (Pascal's identity).

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1} \tag{2}$$

for all natural numbers n, m.

PROOF. By definition, $\binom{n}{m}$ is the coefficient of x^m in the polynomial $(1+x)^n$. In order to find this coefficient, it is necessary, in principle, to multiply the polynomial

$1+x$ by itself n times. Multiplying $1+x$ by itself $n-1$ times, we obtain the polynomial

$$1+\binom{n-1}{1}x+\binom{n-1}{2}x^2+\cdots+x^{n-1}.$$

Performing the final multiplication, we obtain

$$\begin{aligned}(1+x)&\left[1+\binom{n-1}{1}x+\binom{n-1}{2}x^2+\cdots+x^{n-1}\right]\\&=\left[1+\binom{n-1}{1}x+\binom{n-1}{2}x^2+\cdots+x^{n-1}\right]\\&\quad+\left[x+\binom{n-1}{1}x^2+\binom{n-1}{2}x^3+\cdots+x^n\right]\\&=1+\left[\binom{n-1}{1}+1\right]x+\left[\binom{n-1}{2}+\binom{n-1}{1}\right]x^2+\cdots+x^n.\end{aligned}$$

In the resulting equation the coefficient of x^m is equal to $\binom{n-1}{m}+\binom{n-1}{m-1}$. Therefore,

$$\binom{n}{m}=\binom{n-1}{m}+\binom{n-1}{m-1},$$

which is just what we needed to prove. □

Pascal's identity is useful for computing binomial coefficients. For instance, if we want to put another (eleventh) row in our table, all we have to do is add in pairs the adjacent numbers in the previous (tenth) row:

$$\begin{aligned}\binom{11}{0}&=1, & \binom{11}{6}&=\binom{10}{6}+\binom{10}{5}=462,\\ \binom{11}{1}&=\binom{10}{1}+\binom{10}{0}=11, & \binom{11}{7}&=\binom{10}{7}+\binom{10}{6}=330,\\ \binom{11}{2}&=\binom{10}{2}+\binom{10}{1}=55, & \binom{11}{8}&=\binom{10}{8}+\binom{10}{7}=165,\\ \binom{11}{3}&=\binom{10}{3}+\binom{10}{2}=165, & \binom{11}{9}&=\binom{10}{9}+\binom{10}{8}=55,\\ \binom{11}{4}&=\binom{10}{4}+\binom{10}{3}=330, & \binom{11}{10}&=\binom{10}{10}+\binom{10}{9}=11,\\ \binom{11}{5}&=\binom{10}{5}+\binom{10}{4}=462, & \binom{11}{11}&=\binom{10}{11}+\binom{10}{10}=1.\end{aligned}$$

From this we can see that it is convenient to write down binomial coefficients in the form of a triangular table (see Figure 1), called *Pascal's triangle.*

Each number in Pascal's triangle is equal to the sum of the two numbers above it.

By using Pascal's identity we can also obtain the general formula that expresses $\binom{n}{m}$ as a function of n and m.

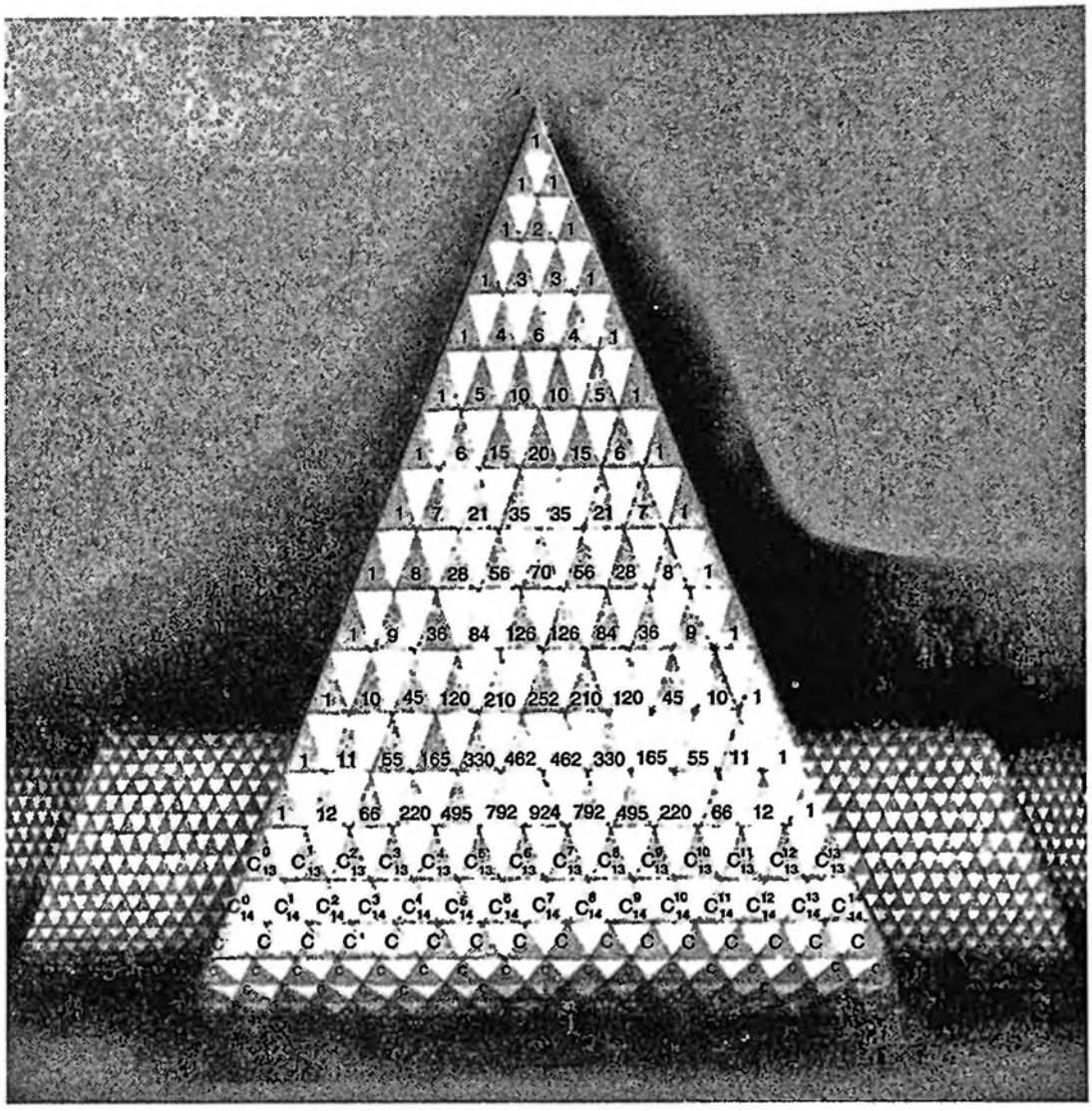

FIGURE 1. Pascal's triangle.

THEOREM 2 (Formula for binomial coefficients).

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{1\cdot 2\cdots m} \tag{3}$$

for all natural numbers n and m.

PROOF. We will use the method of mathematical induction. If $n = 1$, then formula (3) is true:

$$\binom{1}{1} = 1 = \frac{1}{1};$$

$$\binom{1}{m} = 0 = \frac{1\cdot 0\cdots(1-m+1)}{1\cdot 2\cdots m}, \quad m > 1.$$

Let us assume that

$$\binom{n-1}{m} = \frac{(n-1)(n-2)\cdots(n-m)}{1\cdot 2\cdots m}, \quad m = 1, 2, 3, \ldots$$

for some n. Then, if $m > 1$,

$$\begin{aligned}\binom{n}{m} &= \binom{n-1}{m} + \binom{n-1}{m-1} \\ &= \frac{(n-1)(n-2)\cdots(n-m+1)(n-m)}{1\cdot 2\cdots(m-1)m} + \frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)} \\ &= \left[\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}\right]\cdot\left[\frac{n-m}{m}+1\right] \\ &= \left[\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}\right]\cdot\frac{n}{m} \\ &= \frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots m}.\end{aligned}$$

If $m = 1$, on the other hand, then

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1} = \binom{n-1}{1} + \binom{n-1}{0} = \frac{n-1}{1} + 1 = \frac{n}{1}.$$

Thus (3) holds for $n = 1$, and if it holds for $n-1$, it also holds for n. This proves formula (3) for all n. □

We recommend that the readers who encounter formula (3) for the first time derive from it the equalities that are already familiar to us: $\binom{n}{0} = \binom{n}{n} = 1$ and $\binom{n}{m} = 0$ for $m > n$.

Formula (3) is already interesting by the very fact that the fraction that appears on its right-hand side is equal to an integer, i.e., that all the numbers in the denominator will be canceled by numbers in the numerator.

We shall use the following theorem later on.

THEOREM 3. *If the numbers n and m are relatively prime (i.e., if the greatest common factor of n and m is equal to 1), then $\binom{n}{m}$ is divisible by n.*

PROOF.

$$\begin{aligned}\binom{n}{m} &= \frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots m} \\ &= \frac{n}{m}\cdot\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)} \\ &= \frac{n}{m}\cdot\binom{n-1}{m-1}.\end{aligned}$$

Thus

$$m\binom{n}{m} = n\binom{n-1}{m-1}.$$

That is, the number $m\binom{n}{m}$ is divisible by n. But since m and n are relatively prime, i.e., m is not divisible by any prime factor of the number n, it follows that $\binom{n}{m}$ is divisible by n. □

For example, $\binom{9}{4} = 126$ is divisible by 9; $\binom{10}{3} = 120$ is divisible by 10. Let us have a look at several other properties of binomial coefficients:

1. $\binom{n}{m} = \binom{n}{n-m}$.
2. $\binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{m+k}{m} = \binom{m+k+1}{m}$.
3. $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.
4. $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$.

We leave the proofs of these properties to the reader.

2. Remainders in Dividing Binomial Coefficients by Prime Numbers.

In this (as well as the next) section we will often have to use the sentence "integers a and b have equal remainders after division by p." Usually, this sentence is abbreviated by the expression $a \equiv b \pmod{p}$. In other words, the formula $a \equiv b \pmod{p}$ means that $a - b$ is divisible by p. For instance, $4 \equiv 1 \pmod{3}$, $999999 \equiv 222222 \pmod{7}$. The formula $a \equiv b \pmod{p}$ is sometimes read as follows: "The number a is congruent to the number b, modulo p." (However, we are not going to use this expression.)

Here are two obvious properties of the symbol "$\equiv$":

1. If $a \equiv b \pmod{p}$ and k is an integer, then $ka \equiv kb \pmod{p}$. For if $a - b$ is divisible by p, then $ka - kb = k(a - b)$ is also divisible by p.
2. If $a \equiv b \pmod{p}$ and $b \equiv c \pmod{p}$, then $a \equiv c \pmod{p}$.

Indeed, if $a-b$ is divisible by p and $b-c$ is divisible by p, then $a-c = (a-b)+(b-c)$ is also divisible by p.

Let us recall that any natural number a can be divided by a natural number p "with a remainder"; i.e., the number a can be written down in a unique way in the form $a = bp + c$, where b and c are integers with $0 \le c < p$.

The main purpose of this section is to prove the following assertion.

THEOREM 4. *Let p be a prime number and let m, n be natural numbers. Furthermore, let k and l be the quotients after division of m and n, respectively, by p, and let s and t be the respective remainders (i.e., $m = kp + s$, $n = lp + t$, where k, l, s, t are integers and $0 \le s < p$, $0 \le t < p$). Then*

$$\binom{n}{m} \equiv \binom{l}{k} \cdot \binom{t}{s} \pmod{p}.$$

As we will see below, this theorem allows us to find remainders in the division of binomial coefficients by prime numbers with almost no calculation.

The proof of Theorem 4 is preceded by three lemmas.

LEMMA 1. *The following equality holds:*[2]

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}).$$

PROOF. The proof is obvious: By carrying out the multiplication on the right-hand side of the equation and simplifying what can be simplified, we obtain the expression on the left-hand side. □

LEMMA 2. *If p is a prime number and $0 < r < p$, then $\binom{p}{r}$ is divisible by p (i.e., without remainder).*

[2]This proposition, of course, has no relation to binomial coefficients. We have isolated it into a separate lemma in order to simplify the proof of Theorem 4.

PROOF. This follows from Theorem 3: Since p is a prime and $r < p$, the numbers r and p are relatively prime. □

(We note that the primality of the number p is not used anywhere else in the proof of Theorem 4; nevertheless, for a nonprime p, the assertion of the theorem does not hold.)

LEMMA 3. *The polynomial* $(1+x)^p - (1+x^p)$ *is divisible by* p *(i.e., each coefficient of this polynomial is divisible by* p*).*

PROOF. Indeed,

$$(1+x)^p - (1+x^p) = 1 + \binom{p}{1}x + \cdots + \binom{p}{p-1}x^{p-1} + x^p - 1 - x^p$$
$$= \binom{p}{1}x + \cdots + \binom{p}{p-1}x^{p-1}.$$

The last expression is divisible by p by virtue of Lemma 2. □

And now we move on to proving Theorem 4.

PROOF OF THEOREM 4. Let us look at the polynomial

$$P(x) = (1+x)^{lp+t} - (1+x)^t(1+x^p)^l.$$

This polynomial is divisible by p. Indeed, by Lemma 1,

$$P(x) = (1+x)^t\left[(1+x)^{pl} - (1+x^p)^l\right]$$
$$= (1+x)^t\left[(1+x)^p - (1+x^p)\right]\left[(1+x)^{p(l-1)} + \cdots + (1+x^p)^{l-1}\right]$$

According to Lemma 3, the second factor is divisible by p; therefore, the entire product is also divisible by p.

Let us determine the coefficient of x^{kp+s} in $P(x)$. As we know, x^{kp+s} appears in $(1+x)^{lp+t}$ with the coefficient $\binom{lp+t}{kp+s}$. As for the product $(1+x)^t(1+x^p)^l$, it is equal to

$$\left[1 + \binom{t}{1}x + \binom{t}{2}x^2 + \cdots + x^t\right]\left[1 + \binom{l}{1}x^p + \binom{l}{2}x^{2p} + \cdots + x^{lp}\right]$$
$$= 1 + \binom{t}{1}x + \binom{t}{2}x^2 + \cdots + x^t + \binom{l}{1}x^p + \binom{l}{1}\binom{t}{1}x^{p+1}$$
$$+ \binom{l}{1}\binom{t}{2}x^{p+2} + \cdots + \binom{l}{1}x^{p+t} + \binom{l}{2}x^{2p} + \binom{l}{2}\binom{t}{1}x^{2p+1}$$
$$+ \binom{l}{2}\binom{t}{2}x^{2p+2} + \cdots + \binom{l}{2}x^{2p+t} + \cdots$$
$$+ x^{lp} + \binom{t}{1}x^{lp+1} + \binom{t}{2}x^{lp+2} + \cdots + x^{lp+t}.$$

Since $t < p$, it follows that in the last sum, each power of the variable x never appears more than once. As can be seen, the coefficient of x^{kp+s} is equal to $\binom{l}{k}\binom{t}{s}$ (in particular, if $s > t$, then this coefficient is equal to zero).

Thus, the coefficient of x^{kp+s} in $P(x)$ is equal to $\binom{lp+t}{kp+s} - \binom{l}{k}\binom{t}{s}$. Since $P(x)$ is divisible by p, $\binom{lp+t}{kp+s} - \binom{l}{k}\binom{t}{s}$ is divisible by p as well, which is just what we needed to prove. □

Let us now show how the theorem we have just proved can be used to find the remainders in dividing binomial coefficients by prime numbers. Let us figure out, for example, the remainder when the number $\binom{119}{33}$ is divided by 5. (Of course, this can also be done by figuring out $\binom{119}{33}$ according to formula (2), but that would require a lot of work. After all, $\binom{119}{33}$ is a 24-digit number!)

Dividing the numbers 119 and 33 by 5, we obtain $119 = 23 \cdot 5 + 4$ and $33 = 6 \cdot 5 + 3$. By the theorem, $\binom{119}{33} \equiv \binom{23}{6}\binom{4}{3} \pmod 5$. In an analogous way we may investigate the number $\binom{23}{6}$. We have $23 = 4 \cdot 5 + 3$, $6 = 1 \cdot 5 + 1$, and therefore $\binom{23}{6} \equiv \binom{4}{1}\binom{3}{1} \pmod 5$. According to the first property of the symbol $\equiv$ (cf. the beginning of this section), $\binom{23}{6}\binom{4}{3} \equiv \left[\binom{4}{1}\binom{3}{1}\right]\binom{4}{3} \pmod 5$. According to the second property of the symbol $\equiv$, we have that $\binom{119}{33} \equiv \binom{4}{1}\binom{3}{1}\binom{4}{3} \pmod 5$. Thus $\binom{119}{33}$ has the same remainder when divided by 5 as does $\binom{4}{1}\binom{3}{1}\binom{4}{3} = 4 \cdot 3 \cdot 4 = 48$, i.e., the number 3.

In an analogous way we can find the remainders when the number $\binom{119}{33}$ is divided by other prime numbers. For example:

$$119 = 59 \cdot 2 + 1,\ 33 = 16 \cdot 2 + 1 \Rightarrow \binom{119}{33} \equiv \binom{59}{16}\binom{1}{1} = \binom{59}{16} \pmod 2;$$

$$59 = 29 \cdot 2 + 1,\ 16 = 8 \cdot 2 + 0 \Rightarrow \binom{59}{16} \equiv \binom{29}{8}\binom{1}{0} = \binom{29}{8} \pmod 2;$$

$$29 = 14 \cdot 2 + 1,\ 8 = 4 \cdot 2 + 0 \Rightarrow \binom{29}{8} \equiv \binom{14}{4}\binom{1}{0} = \binom{14}{4} \pmod 2;$$

$$14 = 7 \cdot 2 + 0,\ 4 = 2 \cdot 2 + 0 \Rightarrow \binom{14}{4} \equiv \binom{7}{2}\binom{0}{0} = \binom{7}{2} \pmod 2;$$

$$7 = 3 \cdot 2 + 1,\ 2 = 1 \cdot 2 + 0 \Rightarrow \binom{7}{2} \equiv \binom{3}{1}\binom{1}{0} = \binom{3}{1} = 3 \pmod 2;$$

Thus, $\binom{119}{33}$ has the same remainder after being divided by 2 as 3 does, namely, a remainder of 1; that is, $\binom{119}{33}$ is an odd number.

Another example:

$$119 = 39 \cdot 3 + 2,\ 33 = 11 \cdot 3 + 0 \Rightarrow \binom{119}{33} \equiv \binom{39}{11}\binom{2}{0} = \binom{39}{11} \pmod 3;$$

$$39 = 13 \cdot 3 + 0,\ 11 = 3 \cdot 3 + 2 \Rightarrow \binom{39}{11} \equiv \binom{13}{3}\binom{0}{2} = 0 \pmod 3.$$

Here we have made use of the fact that $\binom{0}{2} = 0$, since $2 > 0$. It turns out, then, that $\binom{119}{33} \equiv 0 \pmod 3$, i.e., $\binom{119}{33}$ is divisible by 3.

Let us note that if we apply Theorem 4 to $\binom{n}{m}$, where $n \geq m$, then, writing $m = kp + s$, $n = lp + t$, we will of course get $l \geq k$; however, it is impossible to predict which of the numbers s, t will turn out to be larger. If $s > t$, then according to our theorem, $\binom{n}{m} \equiv \binom{l}{k}\binom{t}{s} = 0 \pmod p$. That is, $\binom{n}{m}$ is divisible by p. As we have seen, in order to determine the remainder when the number $\binom{n}{m}$ is divided by

p, Theorem 4 generally has to be used several times; and each time, a phenomenon similar to the one described above can occur, and moreover, no matter when this happens, it means that the *initial* number, $\binom{n}{m}$, is divisible by p. That was how we determined that $\binom{119}{33}$ is divisible by 3.

We see that the greater n is, the more likely it is that the number $\binom{n}{m}$ is divisible by p. It is easy to prove the following, more precise, assertion: In all, there are $\frac{p^r(p^r+1)}{2}$ numbers $\binom{n}{m}$, with $0 \le n \le p^r$, $0 \le m \le n$, of which exactly $\frac{p^r(p+1)^r}{2^r}$ are not divisible by p (here p is a prime, r a natural number; the proof uses only Theorem 3—we leave it to the reader). We should emphasize that for large numbers r, the number $\frac{p^r(p+1)^r}{2^r}$ is many times smaller than the number $\frac{p^r(p^r+1)}{2}$. Thus, for example, of the numbers $\binom{n}{m}$ with $0 \le n \le 3^5$, $0 \le m \le n$, approximately 26.2% are not divisible by 3. For $0 \le n \le 3^{10}$, the number is approximately 3.6%, and for $0 \le n \le 3^{15}$, it is approximately 0.45%.

In conclusion, let us say several words about the graphic interpretation of Theorem 4 that can be obtained by examining "Pascal's triangle modulo p." This is the table that can be obtained from Pascal's triangle by replacing every number in it by its remainder after division by p. We won't prove any theorems about this triangle, but instead we offer the reader Figure 2, Pascal's triangle modulo 3. Think about what the parts of these triangles that don't appear in the picture look like. Try to formulate Theorem 4 in such a way as to make it a theorem about Pascal's triangle modulo p.

3. A Brief Digression into the Remainders in Divisions of Binomial Coefficients by Powers of Prime Numbers.

We won't go into great generality about properties of remainders after division of binomial coefficients by composite numbers. (However, readers can think about this on their own. What, for example, is the remainder after division of the number $\binom{119}{33}$ by 4? Is it 1 or 3?) We will limit ourselves to talking about one remarkable and still not fully explained phenomenon.

Let us begin with some computations. Using formula (1) for binomial coefficients, we get

$$\binom{2}{1} = 2; \qquad \binom{4}{2} = 6; \qquad \binom{8}{4} = 70;$$

$$\binom{16}{8} = 12\,870; \qquad \binom{32}{16} = 601\,080\,390.$$

(The reader will, of course, have noticed that $1, 2, 4, 8, 16, 32, \ldots$ are successive powers of 2.) The actual numbers we obtain are not in any way remarkable. Their successive differences, however, exhibit amazing properties. Let us look at them:

$$6 - 2 = 4 = 2^2;$$
$$70 - 6 = 64 = 2^6;$$
$$12\,870 - 70 = 12\,800 = 2^9 \cdot 25;$$
$$601\,080\,390 - 12\,870 = 601\,067\,520 = 2^{12} \cdot 146\,745.$$

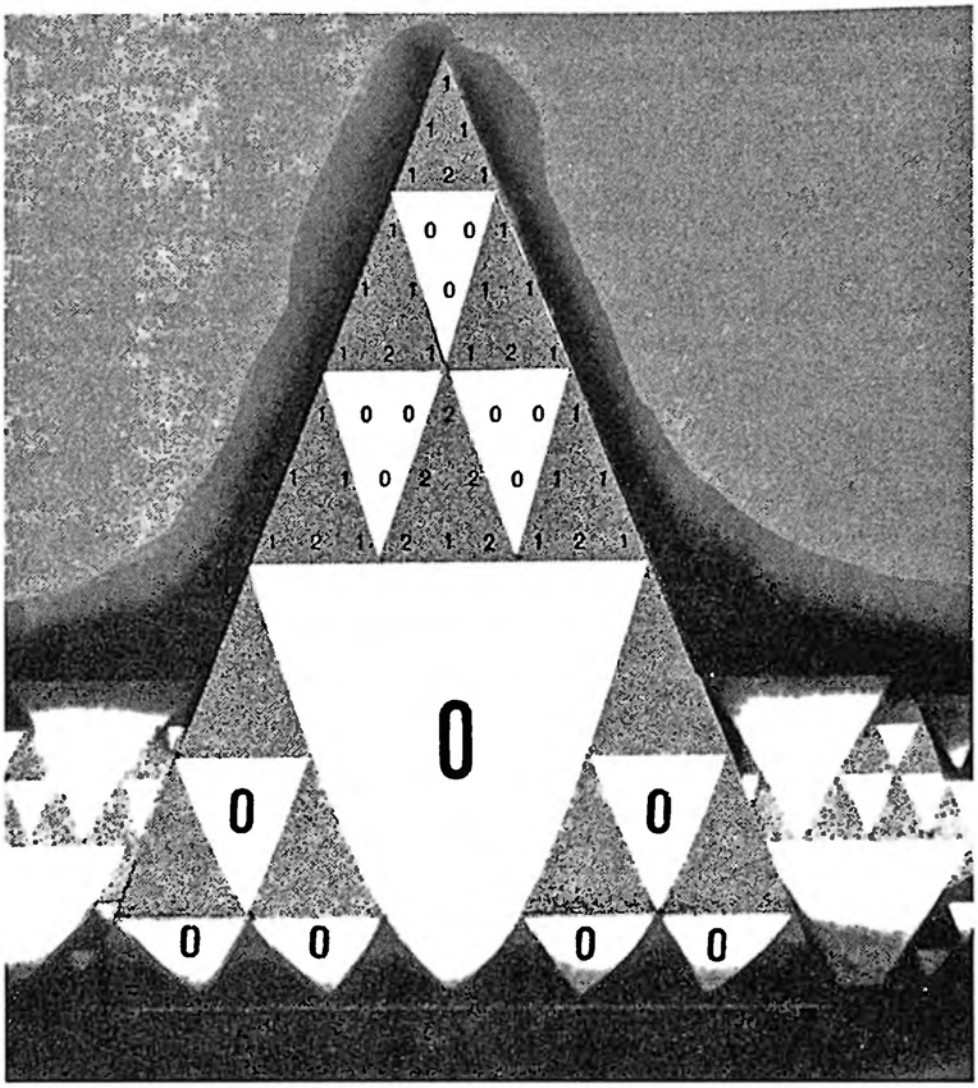

FIGURE 2. Pascal's triangle modulo 3.

We see that these differences are divisible by large powers of 2, and these powers are so high that it is unlikely that this is just an accident. Indeed, we can prove a theorem that at least partly explains this phenomenon.

THEOREM 5. *For $n > 1$, the number*

$$\alpha_n = \binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$$

is divisible by 2^{2n+2}.

REMARKS.

1. The assumption that $n > 1$ is significant, since α_1 is equal to 4 and is not divisible by $2^{2\cdot 1+2} = 2^4 = 16$.
2. It seems plausible that for $n > 1$, α_n is divisible even by 2^{3n}: This is true for $n = 2, 3, 4$, but it is something that none of us has yet been able to prove or disprove in general.

PROOF OF THEOREM 5. Let us begin with the general observation that if the number r is odd, then $\binom{2^n}{r}$ is divisible by 2^n. Indeed, since r is odd and 2^n has no prime factors other than 2, the numbers r and 2^n are relatively prime, and the assertion follows from Theorem 3.

Now let us define

$$P(x) = (1+x)^{2^{n+1}} - (1-x^2)^{2^n}.$$

The polynomial $P(x)$ has the term x^{2^n} with coefficient $\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}} = \alpha_n$. (Here we use the fact that $n > 1$: By raising $(1-x^2) = 1 + (-x^2)$ to the power 2^n, we obtain next to the coefficient $\binom{2^n}{2^{n-1}}$ not x^{2^n}, but $(-x^2)^{2^{n-1}} = (-1)^{2^{n-1}} x^{2^n}$, while the number $(-1)^{2^{n-1}}$ is equal to 1 when $n > 1$ and to -1 when $n = 1$.)

On the other hand,

$$\begin{aligned} P(x) &= (1+x)^{2^{n+1}} - (1+x)^{2^n}(1-x)^{2^n} \\ &= (1+x)^{2^n}\left[(1+x)^{2^n} - (1-x)^{2^n}\right]. \end{aligned}$$

At the same time

$$\begin{aligned} (1+x)^{2^n} - (1-x)^{2^n} &= (1+x)^{2^n} - (1+(-x))^{2^n} \\ &= 1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \binom{2^n}{3}x^3 + \cdots + x^{2^n} \\ &\quad -1 - \binom{2^n}{1}(-x) - \binom{2^n}{2}(-x)^2 \\ &\quad - \binom{2^n}{3}(-x)^3 - \cdots - (-x)^{2^n} \end{aligned}$$

(since $(-x)^k$ is equal to x^k when k is even and to $-x^k$ when k is odd)

$$\begin{aligned} &= 2\left[\binom{2^n}{1}x + \binom{2^n}{3}x^3 + \binom{2^n}{5}x^5 + \cdots \right. \\ &\quad \left. + \binom{2^n}{2^n-1}x^{2^n-1}\right]. \end{aligned}$$

Note that x appears in the resulting polynomial only to odd powers.

We want to know the coefficient of x^{2^n} in $P(x)$, i.e., in the product

$$\begin{aligned} &(1+x)^{2^n}\left[(1+x)^{2^n} - (1-x)^{2^n}\right] \\ &\quad = 2\left(1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \binom{2^n}{3}x^3 + \cdots + x^{2^n}\right) \\ &\qquad \times \left(\binom{2^n}{1}x + \binom{2^n}{3}x^3 + \binom{2^n}{5}x^5 + \cdots + \binom{2^n}{2^n-1}x^{2^n-1}\right). \end{aligned}$$

Obviously, the term in x^{2^n} can be obtained by multiplying the x^{2^n-1} term from the first factor by the x term from the second, by multiplying the x^{2^n-3} term from the

first factor by the x^3 term from the second, and so on. In this way, the coefficient of x^{2^n} in $P(x)$, which, as we know, is equal to α_n, is also equal to

$$2\left[\binom{2^n}{1}\binom{2^n}{2^n-1}+\binom{2^n}{3}\binom{2^n}{2^n-3}+\cdots+\binom{2^n}{2^n-1}\binom{2^n}{1}\right].$$

As we know, each of the numbers $\binom{2^n}{1}, \binom{2^n}{3}, \ldots, \binom{2^n}{2^n-1}$ is divisible by 2^n. Therefore, each of the terms in the square brackets is divisible by $2^n \cdot 2^n = 2^{2n}$. Moreover, a 2 stands in front of the entire expression, and in addition, each term in the square brackets appears twice. Thus α_n is divisible by 2^{2n+2}, which is what we wanted to show. □

Thus, the strange phenomenon of the divisibility of the numbers α_n by high powers of two has to some extent been explained. But something similar can be observed when the 2 is replaced by 3, 5, or 7. Indeed,

$$\binom{9}{3}-\binom{3}{1}=84-3=3^4;$$

$$\binom{27}{9}-\binom{9}{3}=4\,686\,825-84=4\,686\,741=3^7\cdot 2\,143;$$

$$\binom{81}{27}-\binom{27}{9}=2\,306\,279\,447\,501\,851\,002\,720-4\,686\,825$$

$$=2\,306\,279\,447\,501\,846\,315\,895=3^{10}\cdot 39\,057\,044\,954\,221\,855;$$

$$\binom{25}{5}-\binom{5}{1}=43\,130-5=43,125=5^5\cdot 69;$$

$$\binom{49}{7}-\binom{7}{1}=85\,900\,584-7=85\,900\,577=7^5\cdot 5\,111.$$

In short, it appears to be the case that for prime numbers p the integer

$$\binom{p^{n+1}}{p^n}-\binom{p^n}{p^{n-1}}$$

is divisible by a high power of the number p. But proving this is something that none of us has yet figured out how to do.[3]

By the way, if p is not prime, then nothing whatsoever like this occurs. For example,

$$\binom{16}{4}-\binom{4}{1}=1820-4=1816$$

isn't even divisible by 4^2, and

$$\binom{36}{6}-\binom{6}{1}=1\,947\,792-6=1\,947\,786$$

isn't even divisible by 6^2.

We take it for granted that some reader of *Kvant* will be able to clarify this complicated question of the arithmetic of binomial coefficients.

Translated by ILYA BERNSTEIN

[3]See the article by Shirshov in this volume, pp. 49–55.