THE TEACHING OF MATHEMATICS
2000, Vol. III, 1, pp. 15–40

SELECTED CHAPTERS FROM ALGEBRA

I. R. Shafarevich

Abstract. This paper is the continuation of the third part of the publication "Selected chapters of algebra", the first two being published in previous issues of the Teaching of Mathematics, Vol. I (1998), 1–22, and Vol. II, 1 (1999), 1–30, and the beginning of this part in Vol. II, 2 (1999), 65–80.

AMS Subject Classification: 00 A 35

Key words and phrases: Algebra of sets, probability theory, Bernoulli's scheme, Chebyshev inequalities.

CHAPTER III. SET (continued)

3. Algebra of sets

If the intersection of two subsets $M_1 \subset M$ and $M_2 \subset M$ is empty (i.e. $M_1 \cap M_2 = \varnothing$), then the union $M_1 \cup M_2$ consists of elements which belong either to M_1 or to M_2, and any element of $M_1 \cup M_2$ can belong only to one of the sets M_1 or M_2. Hence, $M_1 \cup M_2 = M_1 + M_2$, and so $n(M_1 \cup M_2) = n(M_1) + n(M_2)$.

The case when $M_1 \cap M_2$ is not empty can be reduced to the previous one. Denote by M_1' the complement of $M_1 \cap M_2$ with respect to M_1, that is to say the set of those elements of M_1 which do not belong to $M_1 \cap M_2$. Then $M_1 = (M_1 \cap M_2) + M_1'$ and

$$n(M_1) = n(M_1 \cap M_2) + n(M_1'). \tag{17}$$

Analogously,

$$n(M_2) = n(M_1 \cap M_2) + n(M_2'), \tag{18}$$

where M_2' is the complement of $M_1 \cap M_2$ with respect to M_2. Adding up (17) and (18) we obtain

$$n(M_1) + n(M_2) = 2n(M_1 \cap M_2) + n(M_1') + n(M_2'). \tag{19}$$

But the sets $M_1 \cap M_2$, M_1' and M_2' do not have common elements and their union is $M_1 \cup M_2$. Therefore $M_1 \cup M_2 = M_1 \cap M_2 + M_1' + M_2'$ and so $n(M_1 \cup M_2) =$

This paper is an English translation of the second part of: И. Р. Шафаревич, *Избраные главы алгебры*, Математическое образование, 3, окт.--дек. 1997, Москва, стр. 2--45. In the opinion of the editors, the paper merits wider circulation and we are thankful to the author for his kind permission to let us make this version.

$n(M_1 \cap M_2) + n(M_1') + n(M_2')$. Using this, we can rewrite the equality (19) as: $n(M_1) + n(M_2) = n(M_1 \cap M_2) + n(M_1 \cup M_2)$, that is to say

$$n(M_1 \cup M_2) = n(M_1) + n(M_2) - n(M_1 \cap M_2). \tag{20}$$

This is the relation we wanted. Our further aim is to generalize it and to obtain the expression for the number of elements of the union of an arbitrary number of sets $n(M_1 \cup \cdots \cup M_r)$, and not only the union of two sets. We shall have to establish some more or less evident properties of intersections and unions of several sets.

First of all notice that the union $M_1 \cup M_2 \cup \cdots \cup M_r$ of several subsets M_1, M_2, ... , M_r can be defined by means of unions of only two subsets. For instance,

$$M_1 \cup M_2 \cup M_3 = (M_1 \cup M_2) \cup M_3,$$

and also for arbitrary k

$$M_1 \cup M_2 \cup \cdots \cup M_k = (M_1 \cup M_2 \cup \cdots \cup M_{k-1}) \cup M_k.$$

The second formula we need has the form

$$(M_1 \cup M_2 \cup \cdots \cup M_k) \cap N = (M_1 \cap N) \cup (M_2 \cap N) \cup \cdots \cup (M_k \cap N).$$

Both formulas are obvious; it is enough to ask oneself: what does it mean that an element $a \in M$ belongs to the left or to the right-hand side? For example, in the last formula $a \in (M_1 \cup M_2 \cup \cdots \cup M_k) \cap N$ means that $a \in M_1 \cup M_2 \cup \cdots \cup M_k$ and $a \in N$. The second statement is merely that $a \in N$ and the first that $a \in M_i$ for some $i = 1, \dots, k$. But then $a \in M_i \cap N$ for the same i, and this means that $a \in (M_1 \cap N) \cup (M_2 \cap N) \cup \cdots \cup (M_k \cap N)$. Notice that this property resembles the distributivity of numbers. Indeed, if we replace the sets M_1, M_2, ... , M_k and N by the numbers a_1, a_2, ... , a_k and b, if we replace the sign $\cup$ by $+$ and $\cap$ by $\cdot$, we obtain the equality $(a_1 + \cdots + a_k)b = a_1 b + \cdots + a_k b$, i.e. the distributivity law for numbers. There are other properties which show an analogy between the operations union and intersection of subsets on one side, and addition and multiplication of numbers on the other (see Problem 1). Investigation of system of subsets of a given set M with respect to the operations $\cup$ and $\cap$ is called the *algebra of sets*.

We now derive the formula for $n(M_1 \cup M_2 \cup M_3)$. Since $M_1 \cup M_2 \cup M_3 = (M_1 \cup M_2) \cup M_3$, we can apply formula (20) to obtain

$$n(M_1 \cup M_2 \cup M_3) = n((M_1 \cup M_2) \cup M_3) = n(M_1 \cup M_2) + n(M_3) - n((M_1 \cup M_2) \cap M_3).$$

We can apply formula (20) to the term $n(M_1 \cup M_2)$ and since $(M_1 \cup M_2) \cap M_3 = (M_1 \cap M_3) \cup (M_2 \cap M_3)$, we can also apply formula (20) to the last term above. We get

$$\begin{aligned} n(M_1 \cup M_2 \cup M_3) = n(M_1) + n(M_2) + n(M_3) & \\ - n(M_1 \cap M_2) - n(M_1 \cap M_3) - n(M_2 \cap M_3) & \\ + n((M_1 \cap M_3) \cap (M_2 \cap M_3)). & \end{aligned}$$

Clearly, $(M_1 \cap M_3) \cap (M_2 \cap M_3) = M_1 \cap M_2 \cap M_3$ and so the last term can be written as $n(M_1 \cap M_2 \cap M_3)$. We obtain the formula

$$\begin{aligned} n(M_1 \cup M_2 \cup M_3) = n(M_1) &+ n(M_2) + n(M_3) \\ &- n(M_1 \cap M_2) - n(M_1 \cap M_3) - n(M_2 \cap M_3) \\ &+ n(M_1 \cap M_2 \cap M_3). \end{aligned}$$

Now we can guess what should be the form of the formula for $n(M_1 \cup \cdots \cup M_r)$. It must contain the terms $n(M_{i_1} \cap \cdots \cap M_{i_k})$ where $M_{i_1}, \ldots, M_{i_k}$ are any k sets taken among the sets $M_1, \ldots, M_r$ for all $k = 1, 2, \ldots, r$ and if k is even we take the sign $-$, while if k is odd we take $+$. In other words, the sign of the term $n(M_{i_1} \cap \cdots \cap M_{i_k})$ is $(-1)^{k-1}$.

We shall now prove this formula by induction on r in the same way as we proved it for $r = 3$. The induction basis will be formula (20). Write $M_1 \cup M_2 \cup \cdots \cup M_r$ in the form $(M_1 \cup M_2 \cup \cdots \cup M_{r-1}) \cup M_r$, and use formula (20):

$$\begin{aligned} n(M_1 \cup M_2 \cup \cdots \cup M_r) &= n(M_1 \cup M_2 \cup \cdots \cup M_{r-1}) + n(M_r) \\ &\quad - n((M_1 \cup M_2 \cup \cdots \cup M_{r-1}) \cap M_r). \end{aligned}$$

By the induction hypothesis, the formula is true for $n(M_1 \cup \cdots \cup M_{r-1})$ and gives those terms of $n(M_1 \cup \cdots \cup M_r)$ which do not contain M_r. Now we have

$$(M_1 \cup M_2 \cup \cdots \cup M_{r-1}) \cap M_r = (M_1 \cap M_r) \cup (M_2 \cap M_r) \cup \cdots \cup (M_{r-1} \cap M_r)$$

and by the induction hypothesis we can also apply the formula to the expression $n((M_1 \cap M_r) \cup \cdots \cup (M_{r-1} \cap M_r))$. The intersection

$$(M_{i_1} \cap M_r) \cap \cdots \cap (M_{i_k} \cap M_r)$$

is obviously $M_{i_1} \cap \cdots \cap M_{i_k} \cap M_r$ and so we obtain all the terms of the formula which contain M_r. Moreover, if the term of the formula for $n((M_1 \cap M_r) \cup \cdots \cup (M_{r-1} \cap M_r))$ had the sign $(-1)^{r-1}$, it has the sign $(-1)^r$ in the formula for $n(M_1 \cup \cdots \cup M_r)$ and it will depend on $k+1$ sets $M_{i_1} \cap \cdots \cap M_{i_k} \cap M_r$.

The formula for $n(M_1 \cup \cdots \cup M_r)$ can be written down more conveniently if we consider the number of elements of the complement $\overline{M_1 \cup \cdots \cup M_r}$ of the set $M_1 \cup \cdots \cup M_r$, i.e. the number of elements of the set M which do not belong to any of the subsets M_i. Since for any subset $N \subset M$ we always have $M = N + \overline{N}$, then $n(\overline{N}) = n(M) - n(N)$. In our case $n(\overline{M_1 \cup \cdots \cup M_r})$ will be the sum of the terms $(-1)^k n(M_{i_1} \cap \cdots \cap M_{i_k})$, where $M_{i_1}, \ldots, M_{i_k}$ are any k subsets taken from $M_1, \ldots, M_r$. For $k = 0$ we take the term $n(M)$. In other words,

$$\begin{aligned} n(\overline{M_1 \cup \cdots \cup M_r}) = n &- n(M_1) - \cdots - n(M_r) \\ &+ n(M_1 \cap M_2) + \cdots \\ &+ (-1)^r n(M_1 \cap \cdots \cap M_r), \end{aligned} \tag{21}$$

where $n = n(M)$.

This formula consists of expressions $n(M_{i_1} \cap \cdots \cap M_{i_k})$ where $i_1, \ldots, i_k$ are any k elements of the set $\{1, 2, \ldots, n\}$. We have met such expressions in connection with Viète's formula (formula (12)). It is worthwhile to compare these two formulas. Formula (21) follows from (12) if we put $x = 1$, $a_i = -x_i$ in (12) and then replace everywhere $x_{i_1}, \ldots, x_{i_k}$ by $n(M_{i_1} \cap \cdots \cap M_{i_k})$. Indeed, it is sometimes written in this "symbolic" way

$$n(\overline{M_1 \cup \cdots \cup M_r}) = n(1 - M_1) \cdots (1 - M_r), \tag{22}$$

where we suppose that the product on the right-hand side is expanded by Viète's formula as if M_i were variables, and then the expression $n \cdot M_{i_1} \cdots M_{i_k}$ (which is meaningless) is replaced by the expression $n(M_{i_1} \cap \cdots \cap M_{i_k})$, and $n \cdot 1$ is replaced by $n = n(M)$.

Formula (22) can serve as a means for remembering formula (21), but in algebra, whenever two relations, concerned with different questions, have the same form, it is *always* possible to devise such a definition so that one formula coincides with the other. We shall show this on the example of formulas (21), (22) and Viète's formula (12).

In order to do this we shall have to consider functions on a set M. Undoubtedly, you must have already met with the concept of a function—in one way or another. By a function we shall mean any way of corresponding to each element $a \in M$ a certain number. The actual process of corresponding will be denoted by f, and the number corresponded to the element a by this process will be denoted by $f(a)$. It is also called the value of the function f at the element a. Although the concept of a function is defined for arbitrary sets, we shall at the moment be interested only in the case when the set M is finite. Then a function can be represented by writing with each element a its corresponding number $f(a)$. For example, here are two functions f and g, defined on the set of three elements $M = \{a, b, c\}$ (Fig. 5).

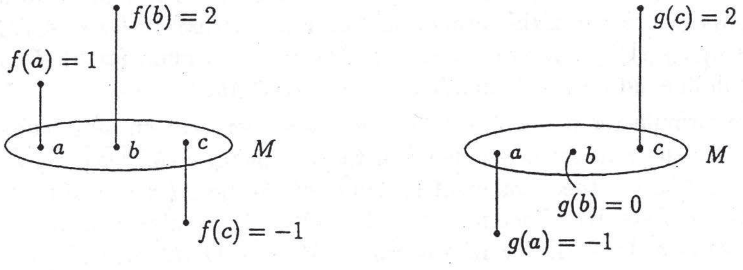


Fig. 5

Therefore, if $M = \{a_1, \ldots, a_n\}$, then a function on M is the sequence $(f(a_1), \ldots, f(a_n))$. Functions can be added up and multiplied, these operations being defined by the values of the functions. In other words, the functions $f + g$

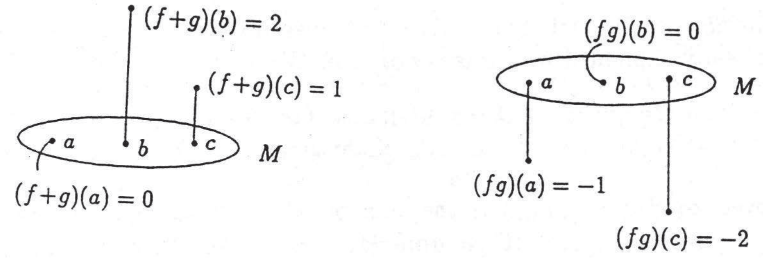


Fig. 6

and fg are defined by $(f+g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$ for arbitrary a. For example, if f and g are represented by Fig. 5, then $f+g$ and fg are represented by Fig. 6.

Since the operations with functions are defined by their values, they have the same properties as the operations with numbers: commutativity, associativity, distributivity, etc. We can apply any identity, proved for numbers, if we replace numbers by functions on a given set M. The function $f_M(a)$ which to any element $a \in M$ corresponds the number 1 is denoted by $\mathbf{1}$. Clearly, $\mathbf{1} \cdot f = f$ for any function f.

We now connect the notion of a function with the notion of a subset. For any subset $N \subset M$ there exists the function defined as follows: the values of elements which belong to N are 1, and the values of those which do not belong to N are 0. This function is called the *characteristic function* of the subset N and is denoted by f_N. Thus, $f_N(a) = 1$ if $a \in N$ and $f_N(a) = 0$ if $a \in \overline{N}$. Conversely, it is clear that the function $f_N(a)$ defines the set N—it consists of all elements $a \in M$ such that $f_N(a) = 1$. (In this way we obtain a one-to-one correspondence between the subsets $N \subset M$ and those functions which take only two values 0, 1. This is the same relation which enables us to deduce Theorem 1 from Theorem 2. See Problem 1 from Section 2, where p and q should be replaced by 0 and 1.)

Some properties of subsets are simply expressed in terms of their characteristic functions. For example, the characteristic function of the whole set M has all values equal to 1, and hence $f_M = \mathbf{1}$. If $\overline{N}$ is the complement of N, then $f_{\overline{N}} = \mathbf{1} - f_N$: indeed, if $a \in N$, i.e. $f_N(a) = 1$, then $(\mathbf{1} - f_N)(a) = 0$, as it should be. Analogously for $a \in \overline{N}$. If N_1 and N_2 are arbitrary subsets then $f_{N_1 \cap N_2} = f_{N_1} \cdot f_{N_2}$, since if $a \in N_1$ and $a \in N_2$ then $f_{N_1} f_{N_2}(a) = 1 \cdot 1 = 1$. If a does not belong to one of the sets N_1 or N_2, then one of the factors f_{N_1} or f_{N_2} is 0 and so $f_{N_1} f_{N_2}(a) = 0$, and also $f_{N_1 \cap N_2}(a) = 0$. Clearly, this is also true for several subsets:

$$\text{(23)} \qquad \text{if} \quad N' = N_1 \cap \cdots \cap N_r, \quad \text{then} \quad f_{N'} = f_{N_1} \cdots f_{N_r}.$$

We can now rewrite formula (21) in the language of characteristic functions. First of all, notice that the considered set $\overline{M_1 \cup \cdots \cup M_r}$ is equal to $\overline{M_1} \cap \cdots \cap \overline{M_r}$. This is evident: an element a does not belong to the set $M_1 \cup \cdots \cup M_r$ if it does not belong to any of M_i, i.e. if it belongs to all $\overline{M_i}$. Now using formula (23) we can write the characteristic function of the set $\overline{M_1 \cup \cdots \cup M_r}$ in the form

$$f_{\overline{M_1 \cup \cdots \cup M_r}} = f_{\overline{M_1} \cap \cdots \cap \overline{M_r}} = f_{\overline{M_1}} \cdots f_{\overline{M_r}}.$$

Besides, we know that $f_{\overline{M_i}} = \mathbf{1} - f_{M_i}$ and we obtain

$$f_{\overline{M_1 \cup \cdots \cup M_r}} = (\mathbf{1} - f_{M_1})(\mathbf{1} - f_{M_2}) \cdots (\mathbf{1} - f_{M_r}).$$

We can now apply Viète's formula (13), by setting into it $x = \mathbf{1}$, $a_i = f_{M_i}$. We have already explained why this is possible. We obtain

$$\begin{aligned} f_{\overline{M_1 \cup \cdots \cup M_r}} = \mathbf{1} &- \sigma_1(f_{M_1}, \ldots, f_{M_r}) + \sigma_2(f_{M_1}, \ldots, f_{M_r}) \\ &- \cdots + (-1)^r \sigma_r(f_{M_1}, \ldots, f_{M_r}). \end{aligned}$$

Moreover, $\sigma_k(f_{M_1}, \ldots, f_{M_r})$ is the sum of all products $f_{M_{i_1}} \cdots f_{M_{i_k}}$ for all different indices $(i_1, \ldots, i_k)$ taken from $(1, \ldots, n)$. We know that $f_{M_{i_1}} \cdots f_{M_{i_k}} = f_{M_{i_1} \cap \cdots \cap M_{i_k}}$ and we obtain that

$$(24) \qquad f_{\overline{M_1 \cup \cdots \cup M_r}} = \mathbf{1} - f_{M_1} - \cdots - f_{M_r} + f_{M_1 \cap M_2} + \cdots + (-1)^r f_{M_1 \cap \cdots \cap M_r},$$

i.e. the sum of all functions $f_{M_{i_1} \cap \cdots \cap M_{i_k}}$ which are taken with the $+$ sign if k is even and with the $-$ sign if k is odd.

Notice that we have obtained something essentially more than the formula (21): we found the expression not for the number of elements $n(\overline{M_1 \cup \cdots \cup M_r})$ of the subset $\overline{M_1 \cup \cdots \cup M_r}$, but for its characteristic function which does not determine only the number of elements of the subset, but the subset itself. In particular, formula (21) has sense only when the set M is finite, while the relation (24) is true for a finite number of subsets of an arbitrary set M.

In order to deduce the relation (21) from it, we have to return from functions back to numbers. It is essential here that M be finite. For any function we define the number Sf as the sum of all values $f(a)$ of the function f at all elements $a \in M$: if $M = \{a_1, \ldots, a_n\}$, then $Sf = f(a_1) + \cdots + f(a_n)$. For example, for the functions f and g from Fig. 5 we have $Sf = 2$, $Sg = 1$, Clearly, for any two functions f, g we have $S(f + g) = Sf + Sg$. Indeed, the value of $f + g$ at a_i is $f(a_i) + g(a_i)$. Therefore, $S(f + g) = (f(a_1) + g(a_1)) + \cdots + (f(a_n) + g(a_n)) = (f(a_1) + \cdots + f(a_n)) + (g(a_1) + \cdots + g(a_n)) = Sf + Sg$. If f_N is the characteristic function of the subset N, then $f_N(a) = 1$ is true for the elements $a \in N$, and for the other elements a it is 0. Hence, $Sf_N = n(N)$.

If we now find the number Sf for the functions on the left and right-hand side of (24), using the established properties, we obtain exactly the relation (21).

Consider now two applications of formula (21). The first is a question studied long time ago by Euler, and it concerns the permutations of a set. We said at the end of the last Section (Remark 1) that this is the name for the arrangements of elements of a set M in a given order. The number of permutations is $n!$ if $n(M) = n$. At the end of Section 2 we wrote down, as an example, all the six permutations of the three element set $M = \{a, b, c\}$. In the general case we also write down all the

$n!$ permutations of the set M and denote by $(a_1, \dots, a_n)$ the first one. The question is: how many permutations do we have in which no element takes the same place as in the first one? This is precisely Euler's question. Solve it for the case $n = 3$ and the six permutations written at the end of Section 2. Verify that only two permutations satisfy the given condition, namely: (c, a, b) and (b, c, a).

In the general case we shall apply formula (21). Denote by $\mathcal{P}$ the set of all permutations of the elements of the set $M = \{a_1, \dots, a_n\}$. We have $n(\mathcal{P}) = n!$. Consider those permutations in which a_i stands at the same place as in the first permutation, i.e. at the i-th place. Denote the set of all such permutations by $\mathcal{P}_i$. Then our question becomes: find $n(\overline{\mathcal{P}_1 \cup \cdots \cup \mathcal{P}_n})$. Hence we have the same situation as we had before for the set $\mathcal{P}$ and its subsets $\mathcal{P}_1, \dots , \mathcal{P}_n$ (in formula (21) the set was denoted by M and its subsets by M_i). In order to apply the formula, we have to find the numbers $n(\mathcal{P}_{i_1} \cap \cdots \cap \mathcal{P}_{i_k})$. But the set $\mathcal{P}_{i_1} \cap \cdots \cap \mathcal{P}_{i_k}$ contains exactly those permutations in which $a_{i_1}, \dots , a_{i_k}$ take the same place as in the first permutation, namely they are the places $i_1, \dots , i_k$, respectively. Such a permutation differs from the first permutation only in the arrangement of elements in other places. In other words, the number of such permutations is equal to the total number of permutations of the set $\overline{\{a_{i_1}, \dots, a_{i_k}\}}$. Since $n(\overline{\{a_{i_1}, \dots, a_{i_k}\}}) = n - k$, applying the general formula we get $n(\mathcal{P}_{i_1} \cap \cdots \cap \mathcal{P}_{i_k}) = (n - k)!$. All the sets $\mathcal{P}_{i_1} \cap \cdots \cap \mathcal{P}_{i_k}$ for a fixed k give one term in the formula (21), and the number of such terms is equal to the number of subsets $\{a_{i_1}, \dots, a_{i_k}\} \subset \{a_1, \dots, a_n\}$ for a given k, that is to say, according to Theorem 3 it is C_n^k. Hence, the contribution of the terms which correspond to a given value of k is $C_n^k(n-k)!$ and substituting the value of the binomial coefficient we get $\dfrac{n!}{k!\,(n-k)!}(n-k)! = \dfrac{n!}{k!}$ and formula (21) in our case becomes

$$\begin{aligned} n(\overline{\mathcal{P}_1 \cup \cdots \cup \mathcal{P}_n}) &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!} \\ &= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{(-1)^n}{n!}\right). \end{aligned}$$

This is the formula founded by Euler. He was actually interested in the ratio of the founded number with the number of all permutations $n!$. This ratio is $1 - \dfrac{1}{1!} + \dfrac{1}{2!} + \cdots + \dfrac{(-1)^n}{n!}$, which, as n increases, can be shown to approach a fixed number, namely $1/e$, where e is the basis of natural logarithms (for those who already know what that is). The number $1/e$ is irrational and approximately equal to 0,36787 … .

The second application of formula (21) is related to the properties of positive integers. Let n be a positive integer, and let $p_1, \dots , p_r$ be its prime divisors, different from each other. How many positive integers exist which are not greater than n and which are not divisible by any of the numbers p_i? This is again an application of formula (21). Denote by M the set of positive integers 1, 2, … , n and by M_i its subset whose elements are divisible by p_i. Clearly, our problem is equivalent to the evaluation of $n(\overline{M_1 \cup \cdots \cup M_r})$. Let us find the values of the terms $n(M_{i_1} \cap \cdots \cap M_{i_k})$ in formula (21). The set $M_{i_1} \cap \cdots \cap M_{i_k}$ consists of all positive integers $t \leqslant n$ which are divisible by prime numbers $p_{i_1}, p_{i_2}, \dots, p_{i_k}$. This is equivalent to the fact that t is divisible by their product $p_{i_1}p_{i_2}\dots p_{i_k}$. Let m be a divisor of n. How many are there positive integers $t \leqslant n$ which are divisible by m? Such numbers have the form $t = mu$, where u is a positive integer and the condition $t \leqslant n$ is equivalent to $u \leqslant n/m$. Hence, u may take the values 1, 2, $\dots$, n/m and the number of such numbers is n/m. If $m = p_{i_1}\cdots p_{i_k}$ this gives that $n(M_{i_1} \cap \dots \cap Mi_k) = \dfrac{n}{p_{i_1}\cdots p_{i_k}}$ and formula (21) becomes

$$n(\overline{M_1 \cup \dots \cup M_r}) = n - \frac{n}{p_1} - \dots - \frac{n}{p_r} + \frac{n}{p_1p_2} + \dots + (-1)^r \frac{n}{p_1\cdots p_r}.$$

The right-hand side can be written in the form

$$n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \dots + \frac{1}{p_1p_2} + \dots + (-1)^r \frac{1}{p_1\cdots p_r}\right).$$

The expression in brackets can be transformed by Viète's formula (applied simply to numbers), if we set $x = 1$, $\alpha_i = -1/p_i$. By (13) this expression will be

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Therefore, for the number of positive integers not greater than n and not divisible by $p_1, p_2, \dots, p_r$ we obtain

$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right). \tag{25}$$

We often meet the case when $p_1, \dots, p_r$ are all the prime divisors of n. In this case t is not divisible by any of p_i's if and only if it is relatively prime to n: if it had a common factor d with n, then this factor would have a prime divisor p_i which would divide both t and n. Therefore, formula (25) gives the number of all positive integers not greater than n and relatively prime to n, if we take $p_1, \dots, p_r$ to be all prime divisors of n. The expression (25) was found in this form by Euler, it is denoted by $\varphi(n)$, and is called Euler's function. For example, for $n = 675 = 3^3 \cdot 5^2$ we have $n(1 - \frac{1}{3})(1 - \frac{1}{5}) = 3^2 \cdot 5(3-1)(5-1) = 360$ numbers which are not greater than 675 and which are relatively prime to 675.

Suppose now that $p_1, \dots, p_r$ need not necessarily divide n. What is the number of positive integers $t \leqslant n$ which are not divisible by $p_1, \dots, p_r$? We can repeat the previous reasoning, but with one alternation. We have to find the number of positive integers $t \leqslant n$ divisible by $p_{i_1}\cdots p_{i_r}$. Let m be an arbitrary positive integer. How many are there positive integers $t \leqslant n$ which are divisible by m? Again put $t = mu$ with the condition $mu \leqslant n$. Hence, we have to take all numbers $u = 1, 2, \dots,$ such that $mu \leqslant n$. Let u be the last of them. Then $r = n - mu < m$, for in the opposite case such a number would also be $mu + m = n(u+1)$. But then $n = mu + r$ where $0 \leqslant r < m$—which is the formula for the division with remainder of n by m (see Theorem 4 of Chapter I). Hence the number u is equal to the quotient in the above division and it shall be denoted by $[n/m]$. Therefore, the number of positive integers not greater than n and divisible by m is $[n/m]$. We can now literally repeat the preceding argument and apply the formula (21). For the number of positive integers not greater than n and not divisible by $p_1, \ldots, p_r$ we obtain the expression

$$n - \left[\frac{n}{p_1}\right] - \left[\frac{n}{p_2}\right] - \cdots + \left[\frac{n}{p_1 p_2}\right] + \cdots + (-1)^r \left[\frac{n}{p_1 \cdots p_r}\right]. \tag{26}$$

It is not as explicit as the expression (25) but we can write it in the form of (25), as an approximation. Recall the formula for the division with a remainder: $n = mu+r$, where $0 \leqslant r < m$ and $u = [n/m]$. Dividing this by m we obtain $\dfrac{n}{m} = u + \dfrac{r}{m}$ and since $0 \leqslant r < m$, we get $\dfrac{n}{m} - 1 < \left[\dfrac{n}{m}\right] \leqslant \dfrac{n}{m}$. In other words, we can replace $[n/m]$ by n/m with an error less than 1. Make this replacement in all the terms of (26). What is the total error? Each term of (26) corresponds to a subset $\{i_1, \ldots, i_k\}$ of the set $\{1, \ldots, r\}$. According to Theorem 2, the number of such subsets is 2^r. Hence this is the number of terms in (26). Since each replacement produces an error less than 1, the total error will be less than 2^r. That is to say that the expression (26) differs from

$$n - \frac{n}{p_1} - \frac{n}{p_2} - \cdots + \frac{n}{p_1 p_2} + \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \tag{27}$$

by less than 2^r. We have met with the last expression before, and we know that it is equal to

$$n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

In this way we obtain that for the number N of positive integers not greater than n and not divisible by given prime numbers $p_1, \ldots, p_r$ the following inequality holds

$$\left| N - n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \right| < 2^r. \tag{28}$$

For example, if we have three prime numbers p, q, r then N is equal to $n\left(1 - \dfrac{1}{p}\right)\left(1 - \dfrac{1}{q}\right)\left(1 - \dfrac{1}{r}\right)$ with an error less than 8.

Problems

1. Verify the relations $M_1 \cap \cdots \cap M_k = (M_1 \cap \cdots \cap M_{k-1}) \cap M_k$ and $(M_1 \cap \cdots \cap M_k) \cup N = (M_1 \cup N) \cap \cdots \cap (M_k \cup N)$. The second of these is again analogous to the distribution law for numbers $(a_1 + \cdots + a_k)b = a_1 b + \cdots + a_k b$, but now the role of multiplication is taken by $\cup$ and the role of addition by $\cap$.

2. Verify that for each relation between subsets involving the operations $\cup$ and $\cap$, there exists another relation in which these two operations change places. In order to do this, prove that $\overline{M_1 \cup M_2} = \overline{M}_1 \cap \overline{M}_2$ and $\overline{M_1 \cap M_2} = \overline{M}_1 \cup \overline{M}_2$.

3. How many times does the function $\sin ax$ take the value 0 on the segment from 0 to $2\pi b$, where $0 < a < b$ and a, b are positive integers?

4. For positive integers $a_1, \dots, a_m$ the expression $\max(a_1, \dots, a_m)$ denotes the greatest and $\min(a_1, \dots, a_m)$ the smallest one of them. Let $N = \max(a_1, \dots, a_n)$. For the set $M = \{1, \dots, N\}$ define M_i as the subset consisting of those j's for which $a_j < a_i$. Applying formula (21), find the relation between $\max(a_1, \dots, a_n)$ and $\min(a_{i_1}, \dots, a_{i_m})$ where $\{a_{i_1}, \dots, a_{i_m}\}$ is a subset of $\{a_1, \dots, a_n\}$.

5. Apply formula (21) for the case when $M_i = \overline{\{\alpha_i\}}$. By evaluating directly all the terms which appear in it, obtain the relation

$$n - C_n^1(n-1) + C_n^2(n-2) + \dots + (-1)^{n-1}C_n^{n-1} \cdot 1 = 0.$$

6. Let M be a finite set and let h be an arbitrary function on M. For a subset $N \subset M$ define the number $S_h(N)$ as the sum of all values $h(a)$, for all $a \in N$. Prove the formula analogous to (21) where $n(M)$ is replaced everywhere by $h(N)$. Hint: multiply the relation (24) by the function h.

7. Find the sum of all positive integers not exceeding n and relatively prime to n. Hint: apply the result of Problem 6 with $h(k) = k$.

8. The same question for the sum of squares of these numbers.

9. Prove that in the right-hand side of inequality (28) we may replace 2^r by 2^{r-1}.

4. The language of probability

The theory of probability, like any other branch of mathematics, has its basic concepts which are not defined—like points or numbers. The first such a concept is the *event*. In this Section we shall consider the case when the number of events is finite. Usually, an event is the result of the occurrences of some simpler events which are said to be *elementary*. For instance, when we throw dice there are 6 possible elementary events: the appearance of number 1, number 2, number 3, number 4, number 5, number 6 on the top face. The event that we obtain an even number consists of three elementary events: either we obtain 2, or 4, or 6. The set of elementary events is simply a set (in this Section a finite set) whose elements have special names (elementary events). An event is a *subset* of the set of elementary events. The second basic concept is *probability*: it is a real number assigned to each elementary event. Therefore, if $M = \{a_1, \dots, a_n\}$ is the set of elementary events, then to define a probability means assigning to each element $a_i \in M$ a real number p_i, which is called the probability of the event a_i. Probabilities should satisfy two conditions: they should be nonnegative and the sum of probabilities of all elementary events should be equal to 1:

$$p_i \geqslant 0, \qquad p_1 + \dots + p_n = 1. \tag{29}$$

In other words, probability is a function $p(a)$ on the set of elementary events M with real values, satisfying the conditions $p(a) \geqslant 0$ for all $a \in M$ and the sum of all the numbers $p(a)$ for $a \in M$ is 1. These conditions play the role of axioms of probability. If N is an arbitrary event (recall that an event is a subset of the set M) then its probability is the sum of the numbers $p(a)$ for all $a \in N$. This probability is denoted by $p(N)$. In the special case when $N = M$, the corresponding event is said to be *certain*. The condition (29) shows that the probability of the certain event is 1. The condition $p(M) = 1$ is not as essential as the condition $p(M) > 0$. The arbitrary case can be reduced to the case $p(M) = 1$, by dividing all the probabilities by $p(M)$. We simply choose the probability of the certain event to be the unit of measuring other probabilities. We emphasize that the object studied by the theory of probability is the set (in our case finite) of elementary events with prescribed probabilities. This set and the probabilities are chosen according to the specific conditions of the considered problem. Afterwards, when they are defined, we can evaluate probabilities of other events. That is why the specialists in the theory of probability say that their task is to find probabilities of certain events using probabilities of other events.

If the two events are given—and we recall that they are simply two subsets N_1 and N_2 of the set M—then their union $N_1 \cup N_2$ and intersection $N_1 \cap N_2$ are also events. From the definition it follows that $p(N_1 \cup N_2) \leqslant p(N_1) + p(N_2)$. The strict inequality may take place since in the sum $p(N_1) + p(N_2)$ the term $p(a)$ will appear twice if $a \in N_1 \cap N_2$. In fact we have

$$p(N_1 \cup N_2) = p(N_1) + p(N_2) - p(N_1 \cap N_2).$$

We came across this relation earlier (see Problem 6 of Section 3). In particular, if $N_1 \cap N_2 = \varnothing$, i.e. if N_1 and N_2 do not intersect, then the events N_1 and N_2 are said to be *mutually exclusive*. In that case $p(N_1 \cup N_2) = p(N_1) + p(N_2)$. A particular case is when $N_1 = N$ is an arbitrary subset and $N_2 = \overline{N}$ is its complement. We obtain that $p(N) + p(\overline{N}) = 1$ or $p(\overline{N}) = 1 - p(N)$. The event $\overline{N}$ is said to be *opposite* to N.

The basic object: the set M and the given function on M satisfying the axioms of probability (29) is called a *probability scheme*. It is denoted by $(M; p)$.

An important case of defining probability schemes is when all the elements of the set M have the same probability, i.e. when all the numbers p_i are equal. From the condition (29) it follows that all p_i's are equal to $1/n$. If $N \subset M$ is an arbitrary event then $p(N) = n(N)/n$. For example, this is the case when we throw dice, if the dice is considered to be homogeneous. In this case, all 6 elementary events which correspond to the possible appearances of the numbers 1, 2, ... , 6 on the top face have the same probability 1/6, and the event that an even number appears on the top face has probability $3 \cdot 1/6 = 1/2$.

If the dice is not homogeneous, we have no reason to give all elementary events equal probabilities. In this case we may define the probabilities experimentally, by throwing dice many times and noting the result. If after a large number n of throwing the number i appears k_i times, then the probability of the elementary event—the appearance of the number i—is taken to be k_i/n. Clearly, the conditions (29) will be satisfied. The number n depends on the accuracy we wish to attain. This gives another probability scheme $(M; p)$.

Analogous to the case of dice throwing is the popular problem of drawing balls from a bag. Suppose that the bag contains n identical balls and that we draw out one of them without looking. The drawing out of a ball is an elementary event. The phrase “identical balls” mathematically means that the probabilities of these events are equal. Hence, they are equal to $1/n$. Suppose now that in the bag we have balls of different colours: a black, and b white balls, where $a + b = n$. Then the event “a white ball is drawn from the bag” is a subset $N \subset M$. Since $n(N) = b$, we have $p(N) = b/n$—this is the probability that a white ball is drawn out.

Somewhat more involved is the dice problem, if dice is thrown twice. In this case an elementary event will be given by two numbers (a, b), where $1 \leqslant a \leqslant 6$, $1 \leqslant b \leqslant 6$ which show that in the first throwing we get a, and in the second b. The number of elementary events is 36. This can be represented by the Table 3, where on the horizontal we write all the possible outcomes of the first throwing, and on the vertical the outcomes of the second. For example, to the elementary event that the first throwing gives 5 and the second 4 corresponds the cell marked with an asterisk. The event that the first throwing gives 5 again has the probability 1/6. But it is no longer elementary: it is comprised of six elementary events which correspond to the cells of the vertical column above the number 5. They correspond to the appearance of any number i, $1 \leqslant i \leqslant 6$ on the top face of the dice in the second throwing, if 5 appeared in the first. Since the first throwing has no effect on the second, and the dice is supposed to be homogeneous, we conclude that all the six elementary events have equal probabilities, and since the probability of the event which they make is 1/6, then the probability of each one of them must be 1/36. Hence, we see that the probability of any elementary event is 1/36.

1						
2						
3						
4		*				
5						
6						
	6	5	4	3	2	1

Table 3

a							
1	7	6	5	4	3	2	
2	8	7	6	5	4	3	
3	9	8	7	6	5	4	
4	10	9	8	7	6	5	
5	11	10	9	8	7	6	
6	12	11	10	9	8	7	
	6	5	4	3	2	1	b

Table 4

Consider the event N_k: “the sum of the numbers obtained at the first and the second throwing is equal to k” (“the score is k”). For each pair (a, b) write in the corresponding cell the sum $a + b$ (Table 4). We see that 12 appears in one cell and so $n(N_{12}) = 1$ and also $n(N_{11}) = 2$, $n(N_{10}) = 3$, $n(N_9) = 4$, $n(N_8) = 5$, $n(N_7) = 6$, $n(N_6) = 5$, $n(N_5) = 4$, $n(N_4) = 3$, $n(N_3) = 2$, $n(N_2) = 1$. The greatest value has $n(N_7)$, and since $p(N_k) = n(N_k)/36$, we see that $p(N_7)$ has the greatest value among all $p(N_k)$’s. In other words, the event that the score 7 will be obtained in two throwing is the most probable.

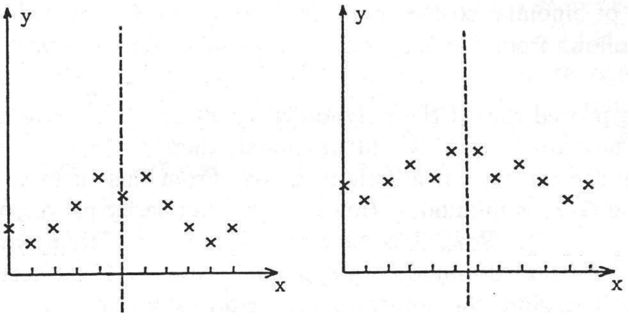
And what is the answer in the case of n throwing? Here the elementary events are given by sequences of n numbers $(a_1, \dots, a_n)$ where each one can take the values 1, ... , 6. The same reasoning as before shows that their probabilities are $1/6^n$. The event N_k: "the total score after n throwing is k" consists of those sequences which satisfy $a_1 + \dots + a_n = k$. Hence, we have to find which number k has the greatest number of representations of the form

$$k = a_1 + \dots + a_n, \qquad 1 \leqslant a_i \leqslant 6. \tag{30}$$

In order to do this, consider the polynomial $F(x) = (x + x^2 + \dots + x^6)^n$. Expanding it, we take from the i-th bracket the term x^{a_i} and as the result we obtain the term $x^{a_1+\dots+a_n}$. There are several terms of this form, and we collect them together. Therefore, the number of various representations (30) is equal to the coefficient of x^k in the polynomial $F(x)$, and our problem reduces to finding which term has the greatest coefficient. Since $F(x) = x^n G(x)$, where $G(x) = (1 + x + \dots + x^5)^n$, the coefficient of x^k in $F(x)$ is equal to the coefficient of x^{k-n} in $G(x)$, and it is enough to find the term with the greatest coefficient in $G(x)$.

Polynomial $G(x)$ has two properties from which the answer to the above question follows.

An arbitrary polynomial $f(x) = c_0 + c_1 x + \dots + c_n x^n$ is said to be *reciprocal* if its terms, equidistant from its ends, have equal coefficients, i.e. if $c_k = c_{n-k}$. If the coefficients c_i are represented by points with coordinates (i, c_i) in the plane, this property means that these points will be arranged symmetrically with respect to the middle: the line $x = n/2$. On Fig. 7a) we represent the case when n is even, and on Fig. 7b) the case when n is odd.



a) b)

Fig. 7

The polynomial $x^n f\left(\frac{1}{x}\right)$ has the same coefficients as the polynomial $f(x)$, but in the reversed order. Indeed, if $f(x) = a_0 + a_1 x + \dots + a_n x^n$, then $f\left(\frac{1}{x}\right) = a_0 + a_1 \frac{1}{x} + \dots + a_n \frac{1}{x^n}$ and $x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$. Therefore, the fact that $f(x)$ is a reciprocal polynomial, means that $x^n f\left(\frac{1}{x}\right) = f(x)$. This implies that the product of two reciprocal polynomials is also reciprocal. Indeed, if

$f(x)$ and $g(x)$ are reciprocal polynomials of degree n and m, then $x^n f\Big(\frac{1}{x}\Big) = f(x)$, $x^m g\Big(\frac{1}{x}\Big) = g(x)$. Multiplying these equalities we get $x^n f\Big(\frac{1}{x}\Big)x^m g\Big(\frac{1}{x}\Big) = f(x)g(x)$, i.e. $x^{n+m} f\Big(\frac{1}{x}\Big)g\Big(\frac{1}{x}\Big) = f(x)g(x)$, which means that the polynomial $f(x)g(x)$ is reciprocal. By induction we conclude that the product of any number of reciprocal polynomials is also reciprocal. Finally, since the polynomial $1 + x + \cdots + x^5$ is reciprocal, so is the polynomial $G(x) = (1 + x + \cdots + x^5)^n$.

The polynomial $f(x) = c_0 + c_1x + \cdots + c_nx^n$ is called *unimodal* if for some $m \leqslant n$ the following inequalities hold: $c_0 \leqslant c_1 \leqslant \ldots \leqslant c_m \geqslant c_{m+1} \geqslant \ldots \geqslant c_n$. That is to say, the coefficients c_i at first do not decrease, and from a certain moment they do not increase. If they are again represented by the points (i, c_i) then they will have "one hump" (Fig. 8).

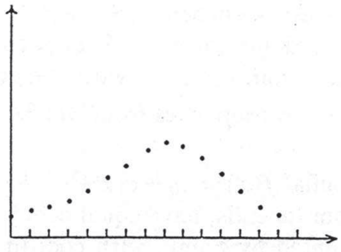


Fig. 8

For example, polynomial $(1 + x)^n$ is reciprocal: this follows from the property $C_n^m = C_n^{n-m}$ of binomial coefficients (see Section 3 of Chapter II). It is also unimodal: this follows from the property of binomial coefficients proved in Section 3 of Chapter II.

It can be proved that if the polynomials $f(x)$ and $g(x)$ have nonnegative coefficients, if they are reciprocal and unimodal, then $f(x)g(x)$ is unimodal. The proof is quite elementary, but a little involved. From this theorem it follows that the polynomial $G(x)$ is unimodal. However, you can easily prove yourself this special case (Problem 3). Now, it is easy to determine the term with the greatest coefficient in a reciprocal unimodal polynomial. Namely, if the term c_kx^k has the greatest coefficient, since the polynomial is reciprocal we have $c_{n-k} = c_k$ and there is the symmetric term c_kx^{n-k}. We can take that $k \leqslant n/2$ and $n - k \geqslant n/2$. Since the polynomial is unimodal, none of the terms c_ix^i where $k \leqslant i \leqslant n - k$ can have smaller coefficient, for otherwise there would be two "humps" on the graph. Hence, the greatest coefficient must be the middle coefficient $c_{n/2}$ if n is even or two "equally middle" coefficients $c_{\frac{n-1}{2}} = c_{\frac{n+1}{2}}$ if n is odd (though there may be other coefficients equal to them). In particular, we see that if n is even, then in $G(x)$ the term $x^{\frac{5n}{2}}$ has the greatest coefficient, and if n is odd then there are two terms of $G(x)$, $x^{\frac{5n-1}{2}}$ and $x^{\frac{5n+1}{2}}$ with equal greatest coefficients.

In the polynomial $F(x)$ this term is multiplied by x^n and has degree $\frac{5n}{2} + n = \frac{7n}{2}$ if n is even. If n is odd, there are two terms with equal coefficients with degree $\frac{5n-1}{2} + n = \frac{7n-1}{2}$ and $\frac{5n+1}{2} + n = \frac{7n+1}{2}$. Therefore, if dice is thrown n times the most probable score is $\frac{7n}{2}$ if n is even, and if n is odd there are two scores which are both most probable: $\frac{7n-1}{2}$ and $\frac{7n+1}{2}$.

Consider one more problem of the same type. A certain quantity of m physical particles are registered by n instruments, so that each particle can be registered by any instrument, and the registration of a particle by all instruments are taken to be equally probable. What is the probability that all instruments register at least one particle? An elementary event here is the registration of a particle by an instrument. Let the instruments be denoted by the elements a of the set M. We have $n(M) = n$. Numerate the particles by 1, 2, ... , m. Then an elementary event is the sequence $(a_1, \dots, a_m)$ where $a_i \in M$ and this sequence indicates that the i-th particle is registered by the instrument a_i. In other words, the set of elementary events is M^m in the sense of the definition given in Section 1. The condition of the problem states that all elementary events have equal probabilities. Since by Theorem 1, $n(M^m) = n^m$, the probability of each elementary event is $1/n^m$. We are interested in the subset $N \subset M^m$ which contains the sequences $(a_1, \dots, a_m)$ in which all the elements of M appear. For example, if $M = \{a, b, c\}$, $m = 4$, then $(a, b, c, a) \in N$, but the sequence (a, b, a, b) does not belong to N, since it does not contain c. Our problem is to find $n(N)$.

Denote by M_a the subset of M^m which consists of the sequences $(a_1, \dots, a_m)$ in which none of the a_i's is equal to a. Then clearly $N = \overline{\bigcup M_a}$, i.e. N is the complement of the union of all sets M_a for all $a \in M$. Therefore, $n(N) = n(M^m) - n(\bigcup M_a)$ and the values of the numbers $n(\bigcup M_a)$ are given by formula (21). Let us find the number $n(M_{a_1} \cap M_{a_2} \cap \dots \cap M_{a_r})$, where a_1, ... , a_r are different elements of the set M. Hence, we are dealing with the sequences $(c_1, \dots, c_m)$ in which none of the c_i's equals any of a_1, ... , a_r. In other words, c_i are arbitrary elements of the set $\overline{\{a_1, \dots, a_r\}}$, where $\overline{\{a_1, \dots, a_r\}}$ is the complement of $\{a_1, \dots, a_r\}$ with respect to M. The set of all such sequences is the set $(\overline{\{a_1, \dots, a_r\}})^m$ and the number of elements of this set is, by Theorem 1, $(n(\overline{\{a_1, \dots, a_r\}}))^m$. Since $n(\{a_1, \dots, a_r\}) = r$, $n(M) = n$, we have $n(\overline{\{a_1, \dots, a_r\}}) = n-r$ and $n(M_{a_1} \cap M_{a_2} \cap \dots \cap M_{a_r}) = (n-r)^m$. Hence, each term $n(M_{i_1} \cap M_{i_2} \cap \dots \cap M_{i_r})$ in formula (21) in our case is $(n-r)^m$. The number of terms for a given r is equal to C_n^r, as we know. Therefore, formula (21) gives

$$n(\bigcup M_a) = C_n^1(n-1)^m - C_n^2(n-2)^m + \dots + (-1)^n C_n^{n-1} \cdot 1^m.$$

For $N = \overline{\bigcup M_a}$ we obtain

$$n(N) = n(M^m) - n(\bigcup M_a) = n^m - C_n^1(n-1)^m + \dots + (-1)^{n-1} C_n^{n-1} \cdot 1^m.$$

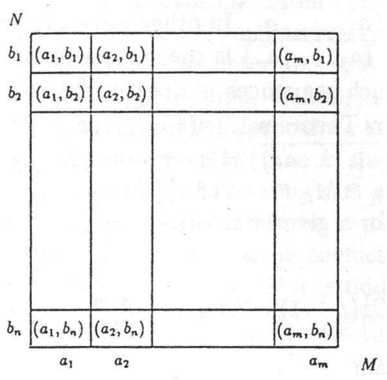
The requested probability is

$$\frac{n(N)}{n^m} = 1 - C_n^1 \left(\frac{n-1}{n}\right)^m + \cdots + (-1)^{n-1} C_n^{n-1} \left(\frac{1}{n}\right)^m . \tag{31}$$

In all the previous examples elementary events had equal probabilities $1/n$, where n is the number of elementary events. As a result, the evaluation of probabilities of other events reduced to the counting of the number of subsets—i.e. to a problem of combinatorics. We shall now consider examples which are more characteristic for the theory of probability.

Let (M, p) and (N, q) be two probability schemes. Suppose that they are defined by many times repeated experiments—different experiment for each scheme. The experiment used to define the probability scheme (M, p) will be called experiment A, and the one used for the scheme (N, q) will be called experiment B. Consider now the experiment consisting of consecutive experiments A and B, and let us try to use it to define a new probability scheme. A similar situation was encountered in connection with consecutive throwing dice (see Table 3). Let $n(M) = m$, $M = \{a_1, \dots, a_m\}$, $p(a_i) = p_i$, $n(N) = n$, $N = \{b_1, \dots, b_n\}$, $p(b_i) = q_i$. Then the new experiment defines the following elementary events: in the first experiment we have the event $a \in M$ and in the second $b \in N$. Hence, new elementary events correspond to the pairs (a, b), where $a \in M$, $b \in N$, or to elements of the set $X = M \times N$. What probabilities can be assigned to these elements? They can be reasonably defined if we introduce one more supposition. We shall take that the experiments A and B, used to define probability schemes (M, p) and (N, q) are *independent*. This means that the result of the second experiment (i.e. B) does not depend on the outcome of the first experiment (i.e. A). Using this condition it is possible to define the probabilities $p(a, b)$ of the events (a, b). Our reasoning will closely follow the one applied in connection with throwing dice two times (see Table 3).

As in that case (and as we did in Section 1), we represent the elements of the set in the form of the rectangular table



N					
b_1	(a_1, b_1)	(a_2, b_1)		(a_m, b_1)	
b_2	(a_1, b_2)	(a_2, b_2)		(a_m, b_2)	
b_n	(a_1, b_n)	(a_2, b_n)		(a_m, b_n)	
	a_1	a_2		a_m	M

Table 5

The event that the event a_i takes place in the first experiment has, by condition, probability p_i. It is not an elementary event, since it consists of elementary events (a_i, b_1), (a_i, b_2), … , (a_i, b_n), displayed in the i-th column of Table 5. As we agreed the probabilities of these events should not depend on the experiment A, but should be like the probabilities of b_1, … , b_n in the scheme (N, q). But here we arrive at a contradiction: the sum of probabilities of the events (a_i, b_1), (a_i, b_2), … , (a_i, b_n) is equal to p_i, and the sum of the probabilities of the events b_1, … , b_n is 1. In other words, the i-th column is itself a probability scheme, which must be "the same" as the scheme (N, q). But in this scheme the condition (29) is not fulfilled. We therefore have to make the following "correction": we divide the probabilities of all elementary events by the probability of the events p_i. We therefore obtain the probability scheme with probabilities $\dfrac{p((a_i, b_j))}{p_i}$. Since it should coincide with the probability scheme (N, q), we arrive at the equality $\dfrac{p((a_i, b_j))}{p_i} = q_j$, i.e. $p((a_i, b_j)) = p_i q_j$. Hence, we have, *by definition*

$$p(a_i, b_j) = p_i q_j. \tag{32}$$

In this way we obtain the new probability scheme: the sum of probabilities of elementary events which appear in the i-th column of Table 5 is equal to $p_i q_1 + \cdots + p_i q_n = p_i(q_1 + \cdots + q_n) = p_i$, and the sum of the probabilities of all elementary events is $p_1 + \cdots + p_m = 1$. Hence, the condition (29) is fulfilled.

This new probability scheme (X, r) is called the *product* of probability schemes (M, p) and (N, q). We can write it as follows: if the given schemes are (M, p) and (N, q), then $X = M \times N$ and $p((a, b)) = p(a)q(b)$. The product of probability schemes corresponds to the intuitive idea of the probability scheme defined by two consecutive experiments, *independent* from each other. The above reasoning was necessary to *explain* the motivation for the given definition. Formally, the *definition* is given by the simple equality (32).

Now for several probability schemes (M_1, p_1), … , (M_r, p_r) we define the product by induction

$$M_1 \times \cdots \times M_r = (M_1 \times \cdots \times M_{r-1}) \times M_r, \tag{33}$$

where $M_1 \times \cdots \times M_{r-1}$ is taken to be known, and the product of two schemes $M_1 \times \cdots \times M_{r-1}$ and M_r is defined above. Let us decipher this definition. As a set, $M_1 \times \cdots \times M_r$ is the product of sets M_1, M_2, … , M_r, defined in Section 1. Hence, it consists of arbitrary sequences $(a_1, \dots, a_r)$ where a_i can be any element of M_i. The probability of the elementary event $(a_1, \dots, a_r)$ is

$$p((a_1, \dots, a_r)) = p_1(a_1)p_2(a_2) \cdots p_r(a_r). \tag{34}$$

This can also be verified by induction on r. Indeed, according to definitions (33) and (32), we have $p((a_1, \dots, a_r)) = p(((a_1, \dots, a_{r-1}), a_r)) = p((a_1, \dots, a_{r-1}))p(a_r)$ and by induction hypothesis $p((a_1, \dots, a_{r-1})) = p_1(a_1)p_2(a_2) \cdots p_{r-1}(a_{r-1})$ and this implies (34). This equality can be described as follows: in the sequence $(a_1, \dots, a_r)$ replace each element by its probability and multiply the obtained numbers. This is the probability of the sequence.

We now apply the general construction to the special case of the probability scheme I^n where $i = \{a, b\}$ is the probability scheme consisting of two elementary events with probabilities $p(a) = p$, $p(b) = q$, with necessary conditions $p \geqslant 0$, $q \geqslant 0$, $p + q = 1$. We have already defined I^n as a set in Section 1. It consists of all possible "words" of the type $(a, a, b, b, b, a, b, \dots)$ in the "alphabet" of two letters: a and b. Hence, they will be the elementary events. Their probabilities are defined, according to the above reasoning, as follows: if the letter a appears in the "word" k times and the letter b appears $n-k$ times, then its probability is $p^k q^{n-k}$. Such a probability scheme is called *Bernoulli's scheme.* As we saw, it gives the probabilities of the events a and b in n times repeated experiment, when in each one the event a has probability p and the event b has probability q. Besides, we suppose that the outcome of an experiment does not affect the outcomes of later experiments.

For example, for $n = 3$ we have 8 elementary events (a, a, a), (a, a, b), (a, b, a), (a, b, b), (b, a, a), (b, a, b), (b, b, a), (b, b, b). Their respective probabilities are p^3, p^2q, p^2q, pq^2, p^2q, pq^2, pq^2, q^3. Notice that here the letter p does not denote the probability, but a fixed number, where $0 < p < 1$. The probability of the elementary event which corresponds to the sequence having k letters a and $n-k$ letters b is $p^k q^{n-k}$. These notations are too standard to be changed, but we have to pay attention to what the letter p denotes.

Let us find the probability of the event A_k which consists of a series of n experiments in which the event a occurs k times. These events consist of elementary events given by "words" $(b, a, b, b, b, a, a, \dots)$ in which a appears in exactly k places. The remaining $n-k$ places are occupied by b. By the general formula, such an elementary event has probability $p^k q^{n-k}$. Now how many elementary events make up the event A_k? This is the number of ways in which k elements can be chosen among n indices $1, 2, \dots, n$, i.e. the number of subsets with k elements of a set of n elements. According to Theorem 3, this is the binomial coefficient C_n^k. Therefore for the probability of the event A_k we obtain

$$p(A_k) = C_n^k p^k q^{n-k} = \frac{n!}{k!\,(n-k)!}\, p^k q^{n-k}. \tag{35}$$

Using this we can find the most probable number of occurrences of the event a. It is the value of k for which the expression in (35) has the greatest value. Write down the expressions (35):

$$1 \cdot q^n, \quad npq^{n-1}, \quad \frac{n(n-1)}{2} p^2 q^{n-2}, \quad \dots, \quad 1 \cdot p^n$$

and consider the ratio of two neighbouring terms:

$$\frac{p(A_{k+1})}{p(A_k)} = \frac{n!}{(k+1)!\,(n-k-1)!}\, p^{k+1} q^{n-k-1} \Big/ \frac{n!}{k!\,(n-k)!}\, p^k q^{n-k} = \frac{(n-k)p}{(k+1)q}$$

(after the cancellations, which you can easily check).

If this ratio is greater than 1, then the $(k+1)$-st number is greater than the k-th; if it is 1, then the two numbers are equal, and if it is less than 1, then the $(k+1)$-st number is less than the k-th. The ratio will be greater than 1 if $\dfrac{(n-k)p}{(k+1)q} > 1$, i.e. $(n-k)p > (k+1)q$ or $np > k(p+q)+q$. Having in mind that $p+q=1$, we can write this inequality in the form $np > k+1-p$, i.e. $(n+1)p-1 > k$. If $k > (n+1)p-1$, then the ratio $p(A_{k+1})/p(A_k)$ is smaller than 1. Finally, if $k = (n+1)p-1$, then $p(A_{k+1}) = p(A_k)$. Therefore, as k takes values less than $(n+1)p-1$, as we move from the k-th number to the $(k+1)$-st, we obtain greater numbers. We distinguish between two cases.

a) The number $(n+1)p-1$ is not an integer. Then the greatest number $p(A_m)$ is obtained for the greatest integer m which does not exceed $(n+1)p$. Moreover, $m \neq (n+1)p-1$ and for greater values of k such number $p(A_k)$ is smaller than the preceding one. Therefore, there is one most probable number of occurrences of the event a—that is the greatest integer m which does not exceed $(n+1)p-1$.

b) The number $(n+1)p-1$ is an integer. Then the number $p(A_k)$ increases if $k < m = (n+1)p-1$. Further, $p(A_{m+1}) = p(A_m)$ and for $k > m+1$ the numbers $p(A_k)$ decrease. Hence, the numbers $p(A_k)$ increase until they reach a maximum, then we have one or two numbers equal to this maximum, and then they decrease. In other words, they have "one hump" as in Fig. 8. This means that the polynomial generated by them, namely $q^n+np^{n-1}qt+\dfrac{n(n-1)}{2}p^{n-2}q^2t^2+\cdots+p^nt^n$ is unimodal. Using the binomial formula, we can write this polynomial in the form $(q+pt)^n$. How can one detect that it is unimodal when it is written in such a simple form? I do not know that such a method exists.

In the simplest case, when $p = q = \dfrac{1}{2}$, we obtain that if $(n+1)\dfrac{1}{2}-1$ is not an integer, i.e. if n is even, then $(n+1)\dfrac{1}{2}-1 = \dfrac{n}{2}-\dfrac{1}{2}$ and $m = \dfrac{n}{2}$. Therefore, there is one most probable number of occurrences of the event a—this is $m = \dfrac{n}{2}$. This means that it is most likely that both events a and b occur n times. It is not surprising, since such an answer is suggested by symmetry. If n is odd, then $m = (n+1)\dfrac{1}{2}-1 = \dfrac{n-1}{2}$ is an integer, and there are two most probable occurrences of the event a: $\dfrac{n-1}{2}$ (in which case b occurs $\dfrac{n+1}{2}$ times) and $\dfrac{n+1}{2}$ (in which case b occurs $\dfrac{n-1}{2}$ times) and this is also quite natural. But for all other values of p we obtain the answer which would be difficult to predict. Here is a problem from a textbook on probability.

After many years of observations it was concluded that the probability that it will rain on the July 1st is 4/17. Find the most probable number of rainy July 1st's in the next 50 years. We have $n = 50$, $p = 4/17$, $m = (n+1)p-1 = 11$. Hence, the most probable numbers of rainy July 1st's are 11 and 12 (with equal probabilities).

The values of probabilities $C_n^kp^k(1-p)^{n-k}$, $k = 0, 1, \ldots, n$ have many important properties. On Fig. 9, taken from a course of the theory of probability, these values are represented for the cases $p = 1/3$, $n = 4$, 9, 16, 36 and 100.

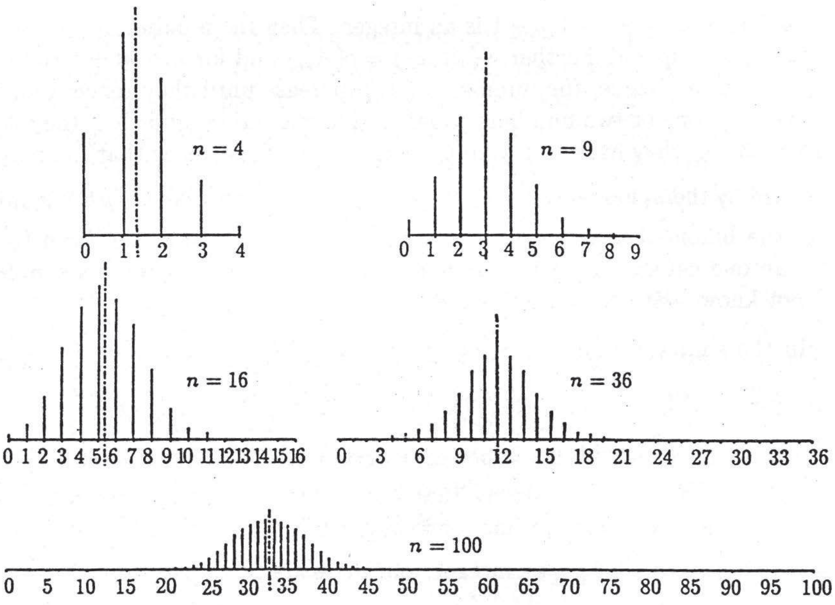


Fig. 9

You see that as n increases, they are not arranged chaotically, but rather they approach a smooth curve. In order to see this better, modify each figure as follows: move the greatest number to the y-axis, decrease the distance between the points on the x-axis (this change of scale was done in Fig. 9) and finally decrease all the numbers proportionally with respect to the greatest number. After this, it turns out that as n increases our points more and more closely approach a certain curve—namely, the graph of the function $y = \dfrac{1}{\sqrt{2\pi}} c^{x^2}$, where π is the ordinary ratio of the perimeter and the diameter of a circle and c (for those who know that e is the basis of natural logarithms) is equal to $1/\sqrt{e}$.

This assertion, called *Laplace's theorem*, gives, in essence, a more subtle property of binomial coefficients. But in order to prove this theorem we would have to explain the phrase "approaches more and more closely", i.e. we would have to introduce the concept of the limit, and we shall not go into this.

Problems

1. In an arbitrary probability scheme (M, p) consider k events: $M_1 \subset M, \dots, M_k \subset M$. Express the probability $p(M_1 \cup M_2 \cup \cdots \cup M_k)$ of the event $M_1 \cup M_2 \cup \cdots \cup M_k$ in terms of the probabilities $p(M_{i_1} \cap \cdots \cap M_{i_r})$ of the events $M_{i_1} \cap \cdots \cap M_{i_r}$.

2. Prove that if the polynomial $f(x)$ is reciprocal and unimodal, then the polynomial $f(x)(1 + x)$ also has these two properties.

3. Prove that if the polynomial $f(x)$ is reciprocal and unimodal, then so is the polynomial $f(x)(1+x+x^2+x^3+x^4+x^5)$. Deduce then that the polynomial $(1+x+x^2+x^3+x^4+x^5)^n$ is unimodal.

4. Verify that the answer to the problem of m particles and n instruments is $\dfrac{n!}{n^n}$ if $n=m$. What relation between binomial coefficients is obtained if the formula (32) is applied in this case?

5. There are n identical balls in a bag, m white and $n-m$ black balls. We draw out at random r balls. What is the probability that we draw k white and $r-k$ black balls? Hint: "at random" means that the probabilities of any draws of r balls are equal.

6. Prove that if the probability p in Bernoulli's scheme is an irrational number, then there exists exactly one most probable number of occurrences of the event a.

7. The ratio of the most probable number of occurrences of an event a in Bernoulli's scheme and the number n is called the *most probable section.* Prove that, as the number n increases indefinitely, then the most probable section approaches more and more closely the probability p of the event a.

APPENDIX

Inequalities of Chebyshev

We shall again consider a question regarding Bernoulli's scheme which was treated at the end of Section 4. As we said there, Bernoulli's scheme practically arises in the situation when we have several times repeated experiment which can have only two outcomes. For example, suppose that we have an asymmetric (non-homogeneous) coin. The question we pose is: if this coin is spun onto the ground will the top face be "head" or "tail"? In order to arrive at an answer, we make a large series of spins—say, 1000—and if "head" appears k times, we say that the probability of its appearance is $p=k/1000$. After that we can apply our definition of Bernoulli's scheme (I^n,p) and we can find other probabilities within that scheme, e.g. formula (35). But is our abstraction satisfactory? Does it represent sufficiently accurately the reality with which we started: a long series of independent spins? In our abstraction—Bernoulli's scheme—we cannot ask: how many times will the event a occur in the scheme I^n? Since we only operate with the language of probability, we can only pose questions regarding certain probabilities. But the concept of probability is connected with reality by our conviction that an event which has a very small probability practically does not occur. In other words, if the probability of a certain event is sufficiently small, we can in practice proceed as if we knew that it will not occur. Of course, the sense of the words "sufficiently small" has to be made precise in each concrete situation. According to this, we can fix a certain number $\varepsilon>0$ and consider the following event A_ε: in our Bernoulli's scheme (I^n,p) the event a occurred k times where $\left|\dfrac{k}{n}-p\right|>\varepsilon$. That is to say, the occurrence of the event A_ε means that the "frequency" k/n of occurrences of the event a differs from the supposed probability by more than ε. It is natural to expect that for a fixed ε the probability $p(A_\varepsilon)$ of the event A_ε will become smaller and smaller as n increases indefinitely. It would mean that the difference between the "frequency" k/n and the probability p for large n can be ignored. Jacob Bernoulli considered this problem already at the beginning of the 18th century, and he realized that finding the probability $p(A_\varepsilon)$ is a purely mathematical problem connected with the properties of binomial coefficients. He proved that the probability $p(A_\varepsilon)$ indeed becomes sufficiently small as n increases. In the 19th century Chebyshev proved not only this particular Bernoulli's statement, but he also found a simple explicit inequality for the probability $p(A_\varepsilon)$. We shall expose here his theorem. This is the first time in our text that we come across the work of a Russian mathematician. P. L. Chebyshev lived in the period from 1821 till 1894, and was the founder of the Petersburg mathematical school.

Let us write now in the form of an algebraic formula the expression we are investigating. In Section 4 we considered Bernoulli's scheme (I^n, p) and we found the probability of the event A_k which takes place if in the series of experiments the event a, for which $p(a) = p$ occurs k times (formula (35)):

$$p(A_k) = C_n^k p^k q^{n-k}. \tag{1}$$

We now have a given number ε and we are interested in the event A_ε which takes place if an event A_k with index k occurs where k satisfies the inequality $\left|\frac{k}{n} - p\right| > \varepsilon$. We want to find the probability $p(A_\varepsilon)$ of the event A_ε. Recall that an event (in particular, A_k or A_ε) is a subset of the set I^n. It is clear that the subsets A_k with different indices do not intersect and that A_ε is the union of all subsets A_k for those k's for which $\left|\frac{k}{n} - p\right| > \varepsilon$. Therefore, the probability $p(A_\varepsilon)$ is the sum of probabilities $p(A_k)$ with such indices k. Since $p(A_k)$ is given by (1), this means that we have obtained an explicit, although a bit complicated, expression for the probability $p(A_\varepsilon)$ of the event A_ε. It is more convenient to write the condition $\left|\frac{k}{n} - p\right| > \varepsilon$, which defines our indices k in the equivalent form

$$|k - np| > \varepsilon n. \tag{2}$$

In this way we arrive at the sum

(3)

S_ε – the sum of all expressions $C_n^k p^k q^{n-k}$ for all k, $1 \leqslant k \leqslant n$, satisfying (2).

We see that the probability $p(A_\varepsilon)$ of the event A_ε is equal to S_ε.

Now we can formulate Chebyshev's theorem.

Chebyshev's theorem. *For the probability $p(A_\varepsilon)$ of the event A_ε that the number of occurrences of k events a in Bernoulli's scheme (I^n, p), satisfying the condition $\left|\frac{k}{n} - p\right| > \varepsilon$, the following inequality holds*

$$p(A_\varepsilon) < \frac{pq}{\varepsilon^2 n}. \tag{4}$$

The inequality (4) is sometimes written in the form

$$p\left(\left|\frac{k}{n}-p\right|>\varepsilon\right)<\frac{pq}{\varepsilon^2 n}.$$

It is clear that for given p $(q=1-p)$ and ε, the right-hand side of the inequality (4) decreases as n increases, which is what we wanted to prove. This particular result is called *Bernoulli's theorem.*

As we saw, the probability $p(A_\varepsilon)$ is equal to the S_ε, defined by (3), and so inequality (4) is equivalent to the inequality

$$S_\varepsilon<\frac{pq}{\varepsilon^2 n}.$$

The proof of Chebyshev's theorem is based upon explicit evaluation of certain sums which we formulate in the form of a lemma.

Lemma *For the probabilities $p(A_k)$, defined by the relation (1), we have*

(5) $$p(A_0)+p(A_1)+p(A_2)+\cdots+p(A_n)=1$$

(6) $$p(A_1)+2p(A_2)+3p(A_3)+\cdots+np(A_n)=np$$

(7) $$p(A_1)+2^2p(A_2)+3^2p(A_3)+\cdots+n^2p(A_n)=n^2p^2+npq.$$

Proof. Denote the left-hand sides of the equalities (5), (6) and (7) by σ_0, σ_1 and σ_2, respectively. We have already seen in Section 4 that, according to the binomial formula, the probabilities $p(A_k)$ are the coefficients of the polynomial $(pt+q)^n$. That is to say, if we put

(8) $$p(A_0)+p(A_1)t+\cdots+p(A_n)t^n=f(t),$$

then

(9) $$f(t)=(pt+q)^n.$$

Setting $t=1$ into (8) and (9), and using the fact that $p+q=1$, we obtain $\sigma_0=1$, i.e. equality (5).

Consider the derivative $f'(t)$ of the polynomial $f(t)$. From the formula (9), using the rule (19) of Section 2 of Chapter II we obtain that

(10) $$f'(t)=np(pt+q)^{n-1}$$

since $(pt+q)'=p$, by formula (15) of Chapter II. On the other hand, applying formula (15) of Chapter II for $f'(t)$ to the polynomial $f(t)$ given by (8), we obtain

(11) $$f'(t)=p(A_1)+2p(A_2)t+3p(A_3)t^2+\cdots+np(A_n)t^{n-1}.$$

Formulas (10) and (11) together lead to:

(12) $$p(A_1)+2p(A_2)t+3p(A_3)t^2+\cdots+np(A_n)t^{n-1}=np(pt+q)^{n-1}.$$

Set $t = 1$ into both sides of (12). Since $p + q = 1$, we obtain the equality (6).

Now multiply both sides of (12) by t. We find

$$(13) \qquad p(A_1)t + 2p(A_2)t^2 + 3p(A_3)t^3 + \cdots + np(A_n)t^n = np(pt + q)^{n-1}t.$$

Let us find the derivatives of both sides of (13). The derivative of the left-hand side is found by means of formula (15) of Chapter II. We obtain the polynomial

$$p(A_1) + 2^2p(A_2)t + \cdots + n^2p(A_n)t^{n-1}.$$

The derivative of the right-hand side can be evaluated by the rule d) for the derivative of a product from Section 2, Chapter II. Write the right-hand side of (13) in the form of a product: $(np(tp+q)^{n-1}) \cdot t$. By rule d) the derivative of this expression is $(np(tp+q)^{n-1})' \cdot t + (np(tp+q)^{n-1}) \cdot t'$. By formula (15) of Chapter II, we have $t' = 1$; by rule c) of Section 2 of Chapter II we have $(np(tp + q)^{n-1})' = np((tp + q)^{n-1})'$ and by formula (19) of Chapter II we have $((tp+q)^{n-1})' = (n-1)(tp+q)^{n-2}p$ since $(tp + q)' = p$, by formula (15) of Chapter II. Therefore, equating the derivatives of the left and right-hand sides of (13) we obtain

$$(14) \quad p(A_1) + 2^2p(A_2)t + \cdots + n^2p(A_n)t^{n-1} = np(pt+q)^{n-1} + n(n-1)p^2(tp+q)^{n-2}.$$

Set $t = 1$ into (14). On the left we get σ_2. On the right (in view of $p + q = 1$) we get $np + n(n - 1)p^2 = n^2p^2 + np(1 - p) = n^2p^2 + npq$ (since $1 - p = q$).

We can now turn to the proof of Chebyshev's theorem. Chebyshev's device was to write inequality (2), which defines the necessary indices, in the form

$$\left|\frac{k - np}{\varepsilon n}\right| > 1,$$

i.e.

$$\left(\frac{k - np}{\varepsilon n}\right)^2 > 1,$$

and then to multiply each term $p(A_k)$ in the sum S_ε by $\left(\frac{k - pn}{\varepsilon n}\right)^2$, which is greater than 1, and therefore increases the sum. After that he considered the *total* sum $\overline{S}_\varepsilon$ of *all* terms $\left(\frac{k - pn}{\varepsilon n}\right)^2 p(A_k)$, $k = 0, 1, \ldots, n$, and not only those for indices k which satisfy (2). It is clear that the sum $\overline{S}_\varepsilon$ differs from the sum S_ε by a certain number of positive terms, and so it must be greater than S_ε.

Hence, $S_\varepsilon < \overline{S}_\varepsilon$. Now, by quite elementary transformations (using the Lemma) we can evaluate the sum $\overline{S}_\varepsilon$ exactly, and thus we obtain the wanted inequality for the sum S_ε.

Therefore, we have to find the sum $\overline{S}_\varepsilon$ of all terms $\left(\frac{k - pn}{\varepsilon n}\right)^2 p(A_k)$ for $k = 0, 1, \ldots, n$. Their common denominator $(\varepsilon n)^2$ can be taken out and the expressions $(k - pn)^2$ can be expanded: $(k - pn)^2 = k^2 - 2npk + p^2n^2$. Every term in the sum $\overline{S}_\varepsilon$ (after $(\varepsilon n)^2$ has been taken out) gives three terms. The sum of the first terms is σ_2 on the left of (7). The sum of the second terms, after the common factor $-2pn$ has been taken out, is the sum σ_1 defined by (6). Finally, the sum of the third terms, after p^2n^2 has been taken out is σ_0, defined by (5). Adding up all the obtained equalities, we find the expression for the sum $\overline{S}_\varepsilon$:

$$\overline{S}_\varepsilon = \frac{1}{\varepsilon^2 n^2}(\sigma_2 - 2pn\sigma_1 + p^2n^2\sigma_0).$$

Substituting the values obtained for σ_2, σ_1 and σ_0 in the Lemma, we find

$$\overline{S}_\varepsilon = \frac{1}{\varepsilon^2 n^2}(n^2p^2 + npq - 2p^2n^2 + p^2n^2) = \frac{pq}{\varepsilon^2 n}. \tag{15}$$

As we saw, $S_\varepsilon < \overline{S}_\varepsilon$ and therefore $S_\varepsilon < \dfrac{pq}{\varepsilon^2 n}$ and the proof of Chebyshev's inequality is finished.

Let us briefly analyse the method which lies in the essence of this proof. The sum S_ε which we want to estimate has a perfectly simple form. The difficulty lies in the fact that the sum is formed by terms which are chosen according to a rather strange criterion (the indices k have to satisfy (2)). The first thing that comes to mind is to ignore these conditions and to take the sum of *all* terms. This sum is easily evaluated: according to the Lemma, it is equal to 1. But it is too large and does not lead to the equality we want. Chebyshev's device was to introduce the additional factor $\left(\dfrac{k-np}{\varepsilon n}\right)^2$ and only *after* that to consider the sum of all terms, ignoring the restriction (2). In this process the terms which appear in the sum S_ε are increased, but those which do not are decreased so much that the total sum $\overline{S}_\varepsilon$ becomes sufficiently small (namely, for the terms which do not appear in S_ε we have $\left(\dfrac{k-np}{\varepsilon n}\right)^2 < 1$).

We have met here with a phenomenon which is very often present in mathematics. Namely, important and interesting inequalities usually follow from an *identity* after an obvious estimate. This obvious estimate in our case is the inequality $S_\varepsilon \leqslant \overline{S}_\varepsilon$ and the identity is the relation (15) which gives the explicit expression for the sum $\overline{S}_\varepsilon$. This is how inequalities of fundamental importance in mathematics are proved. But sometimes they are proved in a different way—this might indicate that there is an underlying identity which we do not yet know.

Return once more to the formulation of Chebyshev's theorem. As we already explained, we are considering the event that in Bernoulli's scheme I^n the event a occurs k times, where either $k > np + n\varepsilon$, or $k < np - n\varepsilon$; in other words, we do not consider the event that in Bernoulli's scheme the event a occurs k times where $np - n\varepsilon \leqslant k \leqslant np + n\varepsilon$. We found that the first event has small probability (for large n), not exceeding $pq/\varepsilon^2 n$. This means that the second event has greater probability, not less than $1 - (pq/\varepsilon^2 n)$. For example, consider a series of large number of repetitions of one experiment under constant conditions. Suppose that one experiment can have only two outcomes—a and b, where the probability of a is p. This situation (if the number of experiments is n) is described, as we saw, by Bernoulli's scheme (I^n, p). The experiment may be, for instance testing a large set of objects (animals, technical details, etc) for a given property, knowing that p-th part of the set has this property. The scheme I^n describes the possible results of the testing. According to Chebyshev's theorem, in the series of n experiments the number of occurrences of the outcome a will be between $np - n\varepsilon$ and $np + n\varepsilon$ with a probability greater than $1 - \dfrac{p(1-p)}{\varepsilon^2 n}$. Here, ε can be any number which we can choose as we like. For example, let $p = \dfrac{3}{4}$. Choosing $\varepsilon = \dfrac{1}{100}$, we see that in the series of n experiments the number k of occurrences of the event a will satisfy the inequality $\dfrac{3}{4}n - \dfrac{n}{100} \leqslant k \leqslant \dfrac{3}{4}n + \dfrac{n}{100}$ with the probability not less than

$$1 - \frac{\frac{3}{4}\cdot\frac{1}{4}}{\left(\frac{1}{100}\right)^2 n}.$$

Since $\dfrac{3}{4^2} < \dfrac{2}{10}$, this probability is not less than

$$1 - \frac{\frac{2}{10}}{\left(\frac{1}{100}\right)^2 n} = 1 - \frac{2000}{n}.$$

For $n = 200\,000$, this probability will be not less than 0,99. The number of occurrences of the event a after 200 000 experiments which have this large probability will be between 148 000 and 152 000 (since $\dfrac{3}{4}n = 150\,000$, $n \cdot \dfrac{1}{100} = 2000$, $np - n\varepsilon = 148\,000$, $np + n\varepsilon = 152\,000$).

Conversely, using Chebyshev's theorem we can estimate the number of experiments to be made in order to obtain the probability p accurately enough. Suppose that we want to determine it with accuracy up to 1/10 and that the probability it is equal to the obtained number is not less than 0,99. According to Chebyshev's theorem we have to put $\varepsilon = 1/10$ and to use the inequality

$$\frac{pq}{\left(\frac{1}{10}\right)^2 \cdot n} < 0{,}01.$$

Notice that $q = 1-p$, and for any p such that $0 \leqslant p \leqslant 1$, we have $pq = p(1-p) \leqslant 1/4$. This follows from the fact that the geometric mean is not greater than the arithmetic mean of the numbers p, q, which is 1/2. Therefore, it is enough that n should satisfy the inequality

$$\frac{\frac{1}{4}}{\left(\frac{1}{10}\right)^2 \cdot n} < 0{,}01$$

which implies $n > 2500$.

Problems

1. In the set of some objects, 95% of them have a certain property. Prove that among 200 000 objects, the number of those which have this property is between 189 000 and 191 000 with probability not less than 0,99.

2. Modify Problem 1 so that the portion of objects which have a certain property is not known. What is the probability that after testing 100 objects we can determine it with accuracy up to 0,1?

3. For any positive integer $r \leqslant n$ find the sum of all terms

$$k(k-1)\cdots(k-r+1)p(A_k)$$

for $k = 1, \ldots, n$.

4. For $r \leqslant 4$ evaluate the sums σ_r consisting of terms $k^r p(A_k)$ for all $k = 0, 1, 2, 3, 4$. Do this in two different ways: a) by the reasoning of the proof of the Lemma, and b) by expressing the sums σ_r in terms of sums evaluated in Problem 3 for $r = 1, 2, 3, 4$.

5. Try to improve the inequality (4) in Chebyshev's theorem, applying the factor $\left(\frac{k-np}{n\varepsilon}\right)^4$ instead of $\left(\frac{k-np}{n\varepsilon}\right)^2$. The improvement will be that n^2 will appear in the denominator of the right-hand side of the inequality instead of n.

I. R. Shafarevich,
Russian Academy of Sciences,
Moscow, Russia