Proceedings of the Steklov Institute of Mathematics, Vol. 211, 1995, pp. 169–183.
Translated from Trudy Matematicheskogo Instituta imeni V.A. Steklova, Vol. 211, 1995, pp. 186–202.

The Complexity of Computations

A. A. Karatsuba

Received January, 1995

INTRODUCTION

This paper is devoted to one of the problems in the history of mathematics, namely, the history of the appearance of the basic arithmetic operations and, more specifically, the appearance of multiplication.

I was repeatedly asked how the method of fast multiplication of multiplace numbers was found. In turn, I became interested in how the mankind arrived at the multiplication method that was the only known one before 1960 and was called the "ordinary", "well-known", "school", etc., multiplication. The aim of the present paper is to answer these questions.

I will use various mathematical notions and symbols that were not, of course, known in the ancient times when arithmetic appeared. These notions make it possible to understand more correctly and to interpret more meaningfully the essence of this matter from the mathematical standpoint.

The history of mathematics deals primarily with the mathematical problems that have attained a high degree of abstractness and a high degree of development. In this case the related mathematical notions have already been defined, the hypotheses and the proofs of the theorems have been stated, and the theories have been constructed. This substantially simplifies the task of the investigator because his position of that of his ancient opponent are equalized to a notable degree. Both of them can apply similar logical arguments, use literal notation, and so on. For instance, extensive investigations are devoted to the Pythagorean school, Euclid's *Elements*, and the works by Archimedes and Diophantus. However, it is interesting and significant to know when one or another notion (method or technique) was devised (found) and what caused the invention (discovery) of this notion (method or technique).

In what follows we will assume that the numbers are represented in the binary number system. The symbols 0 and 1 in this system are called bits. The operation of recording a sign, adding, subtracting, or multiplying two bits, or writing parentheses is regarded as one bit operation (sometimes called an elementary operation or, simply, an operation). When speaking about an operation, we will always mean a bit operation if this is clear from the context.

1. INFORMATION THEORY, COMPUTERS AND THEIR ROLE IN THE DEVELOPMENT OF CYBERNETICS

Information transmission theory and the creation of computers stimulated the development of mathematical cybernetics. Beginning with the 50s A.N. Kolmogorov worked actively in this area of mathematics, and he was the first to formulate problems on computational complexity (about

1956). Kolmogorov emphasized (see [1, p. 251]) that "...the series of my works on information theory was created late in the 50s and 60s under a strong influence of publications by Norbert Wiener and Claude Shannon (1948)."

2. ENTROPY AND THE COMPLEXITY OF THE TABULATION PROBLEM

By that time the notion of entropy of discrete sets introduced by Shannon had already been widely applied, for instance, in the works by Kolmogorov [2] and Vitushkin [3]. For example, Vitushkin wrote in his monograph [3, pp. 18, 19]:

"**Definition** (Shannon). Let X be a set consisting of n elements $x_1, x_2, \ldots, x_n$. The number $H(X) = \log n$ is called the entropy of the set X. Thus, the number $H(X)$ defined by the power of the set X shows of how many of (binary) places the most economical table for $x \in X$ must be formed."

In particular, given the positive integers less than 2^m, whose number is $2^m - 1$, it suffices to have m binary digits to represent these numbers in the binary number system.

In the above-mentioned monograph by Vitushkin some of his original works on estimating the tabulation complexity (i.e., the complexity of an approximate tabular representation) for different function classes are presented. Hence, a very clear idea of complexity had already existed at the end of the 50s.

3. COMPUTATIONAL COMPLEXITY

We will consider the simplest situation. Let $f = f(x)$ be a real-valued function of a real argument x, $a \le x \le b$, and let $f(x)$ satisfy on (a, b) the Lipschitz condition of order α, $0 < \alpha < 1$, $x_2 \in (a, b)$, i.e., let the inequality

$$|f(x_1) - f(x_2)| \le |x_1 - x_2|^\alpha$$

hold for $x_1, x_2 \in (a, b)$.

Let n be a positive integer.

Definition 1. To evaluate $f(x)$ at the point $x = x_0 \in (a, b)$ to within n places means to find a number A such that

$$|f(x_0) - A| \le 2^{-n}.$$

Definition 2. The infimum of the number of bit operations sufficient for evaluating $f(x)$ at the point $x = x_0$ to within n places is called the computational complexity for $f(x)$ at the point $x = x_0$.

Thus, the computational complexity for $f(x)$ at the point $x = x_0$ is a function of n and, of course, of $f(x)$ and x_0. We will denote this function by

$$S_f(n) = S_{f,x_0}(n)$$

and call it the computational complexity for f. The question arises as to what the behavior of $S_f(n)$ is as $n \to +\infty$ for a class of functions f or for some concrete functions f. The problem was stated in this way by Kolmogorov in about 1956 (perhaps not exactly in these words but, essentially, in this very form; for the statement of the problem see [4, 5]). In particular, Ofman, who is one of the

first investigators of $S_f(n)$, wrote in [5, p. 51]: "I obtained the presented results when working on a broader investigation program that was outlined by A.N. Kolmogorov. The further development turned out to be more difficult. Difficulties appear even in estimating the algorithmic complexity of the ordinary multiplication of binary m-digit numbers."

To find an upper estimate for $S_f(n)$, the algorithms are constructed with whose aid the quantity A is calculated. For a concrete algorithm, the number of bit operations used in this algorithm is estimated. This number is exactly an upper estimate for $S_f(n)$. Since the four arithmetical operations, namely, addition, subtraction, multiplication, and division are first of all used, it is necessary to know the number of bit operations which is sufficient for performing these operations. Definitions 1 and 2 imply that the numbers x_0 and A can be represented in the form of the integral part and $m = cn$ binary digits after the binary point, i.e.,

$$A = [A] + 0.\varepsilon_1\varepsilon_2 \ldots \varepsilon_m,$$

$$x_0 = [x_0] + 0.\delta_1\delta_2 \ldots \delta_m,$$

where $\varepsilon_j, \delta_j = 0$ or 1, $j = 1, 2, \ldots, m$, $m = cn$, and $c = c(\alpha) > 0$ is a constant. Since the integral parts $[A]$ and $[x_0]$ are fixed, and $n \to +\infty$, the operations are, in fact, performed on m-digit numbers or, after the replacement of m by n, on n-digit numbers.

Therefore, the primary problem in the complexity theory is the problem of estimating the number of bit operations sufficient for calculating the sum, difference, product, and quotient of two n-digit numbers a and b. Note that division (with a remainder) reduces to addition, subtraction, and multiplication of numbers (this problem will be discussed in greater detail somewhat later).

Thus, let a and b be two n-digit numbers (for simplicity, integers) represented in the binary number system. Their representation requires $2n$ bit operations. Consequently, the complexity of addition (subtraction) of two n-digit numbers is not less than $3n$. At the same time, when adding (subtracting) in an ordinary manner, we perform at most $4n$ bit operations. Hence, the order of the number of bit operations which are necessary and sufficient for performing addition and subtraction is the same.

The next problem relates to the number of operations sufficient for computing ab. It is easy to see (this was immediately pointed out by Kolmogorov) that this problem is equivalent to investigating the behavior of $S_f(n)$, where $f = f(x) = x^2$. Indeed, we have

$$ab = \frac{1}{4}((a+b)^2 - (a-b)^2),$$

and, hence, the complexity of computing ab reduces to the complexity of computing x^2. The function $S_f(n)$ for $f = x^2$ is denoted by $M(n)$. Thus, $M(n)$ is the complexity of computing a^2, where a is an n-digit number (or the complexity of multiplication of two n-digit numbers).

4. OML ALGORITHM AND ITS COMPLEXITY

The multiplication method, which is considered to be standard, is the long (column) multiplication. In what follows, we will refer to it as OML (Ordinary Multiplication). This method was created (found) very long ago. A similar method was already widely used as early as the times of ancient Sumerians and Egyptians, i.e., more than four thousand years ago, and there is every

reason to believe that it has existed for at least six millennia. The appearance of OML will be discussed below in greater detail. We shall now estimate $M(n)$ using the OML algorithm. Let the number a contain at least $n/2$ unities in its binary representation. Then the table of numbers that corresponds to a^2 and OML and must still be added up contains at least $n^2/2$ bits (and no more than $2n^2$ bits). No more than $8n^2$ operations are required for adding n at most $2n$-digit numbers. Thus, we derive the following estimates for $M(n)$:

$$4n \le M(n) \le 8n^2,$$

or, if we are interested only in an upper estimate, $M(n) = O(n^2)$.

5. KOLMOGOROV n^2 CONJECTURE

In 1956 (or a little earlier) Kolmogorov put forward the conjecture that the lower estimate for $M(n)$ is of the order of n^2. It is natural to call it the Kolmogorov n^2 conjecture. Probably, its appearance is based on the fact that throughout the history of mankind people have been using the OML whose complexity is $O(n^2)$, and if a more economical method existed, it would have already been found.

In particular, this conjecture was discussed at one of the meetings of the Moscow Mathematical Society in 1956. There Kolmogorov spoke about the "Czech" method for representing numbers (the Czech number system or, briefly, CSS) in a given system of residue classes and about the multiplication complexity in CSS. The CSS was suggested by the Czech researchers Svoboda and Valach in [6]. Let $p_1 < p_2 < \ldots < p_k$ be prime numbers. Then, every positive integer a that is less than $p_1 p_2 \ldots p_k$ can be uniquely represented in the (CSS) form

$$a \cong (a_1, a_2, \ldots, a_k),$$

where

$$a_j \equiv a \pmod{p_j}, \qquad 0 \le a_j < p_j, \quad j = 1, \ldots, k.$$

Addition, subtraction, and multiplication of numbers in CSS are performed digit by digit. Let us estimate multiplication complexity in CSS. Let a and b be n-digit positive integers, i.e., $a < 2^n$ and $b < 2^n$, let p_j be successive prime numbers beginning with $p_1 = 2$, and let k be the smallest positive integer satisfying the condition

$$2^n < p_1 p_2 \ldots p_k.$$

The definition of k and the well-known law of distribution of prime numbers imply that

$$\sum_{j=1}^{k-1} \log p_j \le n \log 2 < \sum_{j=1}^{k} \log p_j,$$

$$n \asymp \sum_{p \le k \log k} \log p \asymp k \log k,$$

i.e., k is of the order of $n/\log n$. Moreover, each number p_j is of the order of $j \log j$, i.e., each a_j is of the order of $j \log j$, $j \ge 2$. To find a^2,

$$a^2 \cong (a_1^2, a_2^2, \ldots, a_k^2),$$

we have to determine a_j^2, $1 \le j \le k$. The number of binary digits in a_j is of the order of $\log j$, the computational complexity for a_j^2 (we use OML) is $O(\log^2 j)$, and the computational complexity for a^2 in CSS is a quantity of the order of

$$\sum_{j=1}^{k} \log^2 j = O\Big(\frac{n}{\log n} \log^2 n\Big) = O(n \log n).$$

Vitushkin made the following remark concerning this estimates: "If the people lived in CSS, then the n^2 conjecture would not exist." Kolmogorov replied that number systems (NS) appeared in measurements and were meant for measuring quantities and, in particular, comparing the measured quantities (measurement is, in fact, nothing other than the comparison of a measured quantity to a standard). However, in CSS it is impossible to find out which of the two given numbers $a \cong (a_1, a_2, \dots, a_k)$ and $b \cong (b_1, b_2, \dots, b_k)$ is larger (smaller) until each of them is represented in a positional NS. It is clear that the conversion of a and b from a positional NS to CSS or vice versa requires a large number of operations, and therefore no improvement of the estimate for $M(n)$ can be obtained in this way.

The natural character of assumptions similar to the n^2 conjecture was noted, for instance, by Babenko in [7, p. 5]: "It is well-known how important a good number system is for the development of science, and even in ancient Babylonia we find the excellent sexagesimal system for integers and fractions. As regards number systems and calculation techniques, it seems that the final and best solutions were found in science long ago."

6. DISPROOF OF THE n^2 CONJECTURE

In the autumn of 1960 a seminar on mathematical problems in cybernetics was held at the Faculty of Mechanics and Mathematics at Moscow University under the guidance of Kolmogorov, where Kolmogorov stated the n^2 conjecture and posed some problems concerning the estimation of the complexity of the solution of linear systems of equations and some other similar kinds of computations. I began to think actively about the n^2 conjecture, and exactly within a week I found that the algorithm with whose aid I hoped to derive a lower estimate for $M(n)$ provided an estimate of the form

$$M(n) = O(n^{\log_2 3}), \qquad \log_2 3 = 1.5849\dots.$$

After the next seminar I told Kolmogorov about the new algorithm and about the disproof of the n^2 conjecture. Kolmogorov was very agitated because this contradicted his very plausible conjecture. At the next meeting of the seminar, Kolmogorov himself told the participants about my method, and at this point the seminar was terminated. Later in 1962 Kolmogorov wrote a short article (probably in collaboration with Ofman) and published it in *Doklady Akad. Nauk SSSR*. The article was entitled: A. Karatsuba and Yu. Ofman, "Multiplication of Multiplace Numbers on Automata" (*Doklady Akad. Nauk SSSR*, vol. 145, No. 2, pp. 293–294). I learned about the article only when I was given its reprints. The unusual character of this publication was also characterized by the fact that Kolmogorov presented for publication two papers [5] and [8] simultaneously on February 13, 1962.

This started an intensive activity in this area of applied mathematics which was called "fast computations." It is still in progress. It will be discussed in greater detail below.

7. KML ALGORITHM AND ITS COMPLEXITY

In this section I present my algorithm for multiplying numbers. Now it is called the KML algorithm or, briefly, KML (Karatsuba Multiplication) (e.g., see [9]).

As was noted, multiplication of two numbers reduces to squaring a number. For instance, it is required to square an n-digit number a. Without loss of generality, we assume that $n = 2^m$. We represent a in the following form: $a = 2^{n_1}a_1 + a_2$, $2n_1 = n$, where a_1 and a_2 are n_1-digit numbers. We have

$$a^2 = (2^{n_1}a_1 + a_2)^2 = 2^n a_1^2 + 2^{n_1}2a_1a_2 + a_2^2.$$

Moreover,

$$2a_1a_2 = (a_1 + a_2)^2 - a_1^2 - a_2^2,$$

i.e.,

$$a^2 = 2^n a_1^2 - 2^{n_1}a_1^2 + 2^{n_1}(a_1 + a_2)^2 + a_2^2 - 2^{n_1}a_2^2. \tag{1}$$

Since a_1 and a_2 are n_1-digit numbers, the sum $a_1 + a_2$ is, at most, an $(n_1 + 1)$-digit number. Therefore it can be represented as

$$a_1 + a_2 = \varepsilon + 2a_3,$$

where $\varepsilon = 0$ or 1 and a_3 is an n_1-digit number. Consequently,

$$(a_1 + a_2)^2 = \varepsilon^2 + 4\varepsilon a_3 + 4a_3^2. \tag{2}$$

It follows from (1) and (2) that

$$a^2 = 2^n a_1^2 - 2^{n_1}a_1^2 + 2^{n_1+2}a_3^2 + 2^{n_1+2}\varepsilon a_3 + 2^{n_1}\varepsilon^2 + a_2^2 - 2^{n_1}a_2^2. \tag{3}$$

We will compute a^2 according to (3). Let $\varphi(n)$ be the number of (bit) operations sufficient for computing the square of an n-digit number with the use of relation (3). The right-hand side of (3) shows that it is necessary to square three n_1-digit numbers, namely, a_1, a_2, and a_3; this requires $3\varphi(n_1)$ operations. Then each of the resulting values must be multiplied by one of the numbers 2^n, 2^{n_1}, and 2^{n_1+2}, which requires at most $6n$ operations (multiplication by a power of 2 reduces to adding an appropriate number of zeros on the right of the multiplicand). Then it is necessary to add together (we mean an algebraic sum) seven, at most, $2n$-digit numbers, which requires no more than

$$4 \cdot 2n \cdot 4 + 4(2n + 2) \cdot 2 + 4(2n + 2) = 56n + 24$$

operations. Thus we derive for $\varphi(n)$ the inequality

$$\varphi(n) \le 3\varphi(n_1) + 6n + 56n + 24 \le 3\varphi(n_1) + 70n. \tag{4}$$

Furthermore, setting $2n_{j+1} = n_j$, $j = 1, \ldots, m - 1$, we obtain

$$\varphi(n_j) \le 3\varphi(n_{j+1}) + 70n_j. \tag{5}$$

Since $n_{j+1} = 2^{m-j-1}$, we have $n_m = 1$ and, trivially, $\varphi(1) = 1$. Using (4) and (5) we can prove by induction that the inequality

$$\varphi(n) \le 3^j\varphi(n_j) + 3^{j-1} \cdot 70n_{j-1} + \ldots + 3 \cdot 70n_1 + 70n \tag{6}$$

holds for $j \geq 1$. Indeed, this is true for $j = 1$. Assuming that this relation holds true for j, we prove it for $j + 1 \leq m$. The substitution of (5) into (6) results in

$$\varphi(n) \leq 3^{j+1}\varphi(n_{j+1}) + 3^j \cdot 70n_j + 3^{j-1} \cdot 70n_{j-1} + \ldots + 3 \cdot 70n_1 + 70n,$$

which is what we had to prove.

We now set $j = m$, $\varphi(n_m) = \varphi(1) = 1$, and $n_j = 2^{m-j}$ in (6) and obtain

$$\varphi(n) \leq 3^m + 3^{m-1} \cdot 70n_{m-1} + 3^{m-2} \cdot 70n_{m-2} + \ldots + 3 \cdot 70n_1 + 70n$$

$$= 3^m + 3^{m-1} \cdot 70 \cdot 2 + 3^{m-2} \cdot 70 \cdot 2^2 + \ldots + 3 \cdot 70 \cdot 2^{m-1} + 70 \cdot 2^m$$

$$= 3^m\left(1 + 70 \cdot \frac{2}{3} + 70 \cdot \left(\frac{2}{3}\right)^2 + \ldots + 70 \cdot \left(\frac{2}{3}\right)^{m-1} + 70 \cdot \left(\frac{2}{3}\right)^m\right) < 70 \cdot 3^m \cdot \left(1 - \frac{2}{3}\right)^{-1} = 210 \cdot 3^m.$$

Since $n = 2^m$, $m = \log_2 n$, we have

$$\varphi(n) < 210n^{\log_2 3}, \qquad \log_2 3 = 1.5849\ldots.$$

In particular, it follows that

$$M(n) = O(n^{\log_2 3}),$$

i.e., the n^2 conjecture is disproved.

Note that when estimating $\varphi(n)$, we overestimated the related constants intentionally so that all calculations become as simple as possible. These calculations can be performed more economically, and this will result in a much smaller constant than 210. Practical application of KML will be discussed later.

There also exists an alternative version of KML, in which two n-digit numbers a and b are multiplied directly. As before, we represent a and b in the form

$$a = 2^{n_1}a_1 + a_2, \qquad b = 2^{n_1}b_1 + b_2, \qquad 2n_1 = n,$$

and find

$$ab = (2^{n_1}a_1 + a_2)(2^{n_1}b_1 + b_2) = 2^n a_1 b_1 + 2^{n_1}(a_2 b_1 + a_1 b_2) + a_2 b_2$$

$$= 2^n a_1 b_1 - 2^{n_1} a_1 b_1 + a_2 b_2 - 2^{n_1} a_2 b_2 + 2^{n_1}(a_1 + a_2)(b_1 + b_2). \tag{7}$$

In this relation we have three products of the form $a_1 b_1$, $a_2 b_2$, and $(a_1 + a_2)(b_1 + b_2)$. Each of the factors is at most an $(n_1 + 1)$-digit number. We again denote by $\varphi(n)$ the number of operations sufficient for computing products of two n-digit numbers with the use of relation (7) and obtain the inequality

$$\varphi(n) < 3\varphi(n_1) + cn,$$

where $c > 0$ is an absolute constant and $2n_1 = n$. This relation gives the estimate

$$\varphi(n) < c_1 n^{\log_2 3},$$

where $c_1 > 0$ is an absolute constant.

It is quite clear that by splitting a and b into a greater than two number of summands, we can derive a more accurate estimate for $M(n)$. A little later we will discuss in detail the further development of fast computations and some refined estimates for $M(n)$. Now we turn to the ancient history of fast computations.

8. ANCIENT ARITHMETIC

Homo sapience has been performing calculations beginning with the prehistoric times. These calculations were the most primitive: addition, subtraction, multiplication, and division of small numbers. Arithmetic and, along with it, mathematics appeared only when large numbers were encountered. Indeed, if a and b are small numbers (of the order of unity), then, in our terminology, the complexity of the operations $a+b$, $a-b$, and $ab = a+a+\ldots+a$ is $O(1)$, and there is no essential distinctions between them. However, if a and b are n-digit numbers, the additive operations, i.e., addition and subtraction, require $O(n)$ operations, whereas the computation of the product ab defined as a result of repeated addition requires $O(n2^n)$ operations. This fact characterizes the fundamental distinction between multiplication and addition or subtraction. The operation of division of a by b with a remainder, $a = bq + r$, $0 \le r < b$, is of the same complexity (division is performed as a successive subtraction of the numbers b from a, i.e., $a - (b + b + \ldots + b) = r$, $0 \le r < b$).

I also want to point out that at the present time it is known that some animals are capable of adding, subtracting, and, hence, multiplying small numbers.

When people started dealing with large numbers, it was quite natural that positional NS's were to appear first. A rather detailed study of this problem was carried out by specialists in the history of mathematics (e.g., see [7, 10–13]), and I will not dwell on it.

People added, subtracted, multiplied and divided numbers. The first division techniques were rather primitive, and the divisors were small numbers or some special kinds of numbers. Everything that is connected with division has also been investigated in detail in [10, 11]. For the time being, we will consider only the additive operations and multiplication. Note that these operations reached us in its original form. The place and time of their appearance were not determined exactly. The most ancient sources are the Sumerian cuneiform inscriptions, the Egyptian papyrus of Rhind, and the so-called Moscow papyrus, which is believed to be two centuries older than the Rhind papyrus. Future archeological discoveries may indicate that arithmetic appeared much earlier. There are hypotheses that in Africa there exist developed ancient civilizations which are no less than 20 thousand years old. An indirect confirmation of these hypotheses is given by the photographic surveys of the American austronauts. However, all this is an object for future investigations. At present I want to consider only one problem, namely, an example of multiplication in the Rhind papyrus (see [10]). In all other sources the authors present their own examples to demonstrate the calculation methods of the ancients. I will present some facts from the works on this subject.

The information about the Rhind papyrus in the monograph by Van der Waerden [10] is the following. The papyrus was written in Egypt about 1800 B.C. "The scribe Ahmose asserts that it stems from the original written in the Middle Kingdom (2000–1800 B.C.)." It contains 84 problems devoted to calculation techniques and uses the decimal number system. Van der Waerden writes in his book: "Addition of these numbers encounters no difficulties because it is only necessary to calculate the numbers of unities, tens, hundreds, etc. Duplication is a special case of addition, and it is not difficult either. However, of extreme peculiarity is Multiplication.

It is performed by means of duplication and addition of the resulting values. As an example, we first present the multiplication 12×12 in Problem No. 32 of the Rhind papyrus in the hieroglyphic representation (which must be read from right to left) and then in modern representation." I present

here only the modern version:

1	12	
2	24	
/4	48	
/8	96	Sum is 144.

"Quadruplication and octuplication yield a 12-fold increase of the given number 12. The numbers that must be successively added together are marked by a backslash on the right (on the left in the "translation"). The result 144 is preceded by the hieroglyph *dmd* representing a scroll with a seal." Then Van der Waerden writes: "This Egyptian multiplication method is a basis of the entire calculation technique. It must be very ancient, but in this very form it was preserved until the Hellenistic epoch, and in the Greek schools it was called the "Egyptian" calculation. Even in the Middle Ages 'duplatio' (duplication) was considered to be as an independent operation."

Another source is the monograph by Struik [13] where the Rhind papyrus containing 84 problems is mentioned and also the Moscow papyrus (25 problems), which is probably two centuries older. They present calculation techniques. Struik writes: "On the basis of this number system the Egyptians constructed primarily additive arithmetic, i.e., it is mainly aimed at reducing all multiplications to repeated additions. For instance, multiplication by 13 is obtained by multiplying first by 2, then by 4, then by 8, and then adding together the results of the multiplications by 4 and by 8 and the original number. For example, to compute 13×11 they wrote

*1	11
2	22
*4	44
*8	88

and then added together all numbers marked by the asterisk, which gave 143.

Here we see an interpretation of Egyptians' method, rather than the original example from the papyrus. I also give a quotation from the paper by Bashmakova and Yushkevich (see [12, p. 29]): "The Egyptian system is also of interest due to the role that the number 2 plays in it. Originally it probably served as the base of the number system... Survivals of the binary system are reflected in Egyptians' multiplication method, which reduced to successive duplication and addition. For instance, to multiply the number n by 15, the Egyptians used the following (schematic) pattern: $n \cdot 15 = n(1 + 2 + 2^2 + 2^3) = n \cdot 1 + n \cdot 2 + n \cdot 2^2 + n \cdot 2^3$, i.e., they represented the factor in the binary system and then performed the multiplication by each binary digit separately."

In what follows, we will refer to the Egyptian multiplication method as EML.

9. COMPLEXITY OF THE EML ALGORITHM

It is easy to formalize the EML and estimate its complexity. We represent b in the form of the binary expansion

$$b = 2^{n_1} + 2^{n_2} + \ldots + 2^{n-1},$$

where

$$0 \le n_1 < n_2 < \ldots < n - 1.$$

Then ab can be represented as

$$ab = a \cdot 2^{n_1} + a \cdot 2^{n_2} + \ldots + a \cdot 2^{n-1}. \tag{8}$$

Beginning with a, we apply successive addition to obtain

$$2a, 2^2a, \ldots, 2^{n_1}a, \ldots, 2^{n_2}a, \ldots, 2^{n-1}a,$$

i.e., in this way all terms on the right-hand side of (8) are found. On adding these terms together, we determine ab. Each of the terms is, at most, an $2n$-digit number, and the number of the terms is less than n. Therefore, the number of operations sufficient for computing the sum is $O(n^2)$. To find each of the numbers $2a$, 2^2a, etc., we need $O(n)$ operations, and, finally, the calculation of $2^{n-1}a$ also requires $O(n)$ operations because each time we add together at most $2n$-digit numbers. Consequently, to obtain the terms on the right-hand side of (8), it suffices to perform $O(n^2)$ operations. Hence, the complexity of EML is $O(n^a)$ and coincides with that of OML.

10. OML AS A DIRECT CONSEQUENCE OF EML

It is easy to see that if the terms on the right-hand side of (8) are obtained not by a successive addition, but by adding an appropriate number of zeros on the right of a, then we obtain OML instead of EML. I believe that people arrived at OML immediately after the symbol 0 appeared.

11. EML AS A THEORETICAL REALIZATION OF THE WEIGHING ON BEAM SCALES

The basis for the appearance of EML was probably the weighing on beam scales with two pans. The fastest way for obtaining the weight $a \cdot 2^{n-1}$ consists in that, with the initial weight a on the left pan, one first obtains a on the right and thus receives a weight $2a$; proceeding from $2a$, one finds $2 \cdot 2a = 2^2a$, and so on, until $2^{n-1}a$ is obtained. With all weights of the form $a, 2a, 2^2a, \ldots, 2^{n-1}a$ at one's disposal, one finds a weight ab, where b is an arbitrary n-digit number, by adding. This is just the EML algorithm, whose later modification is OML. Note that beam scales and the weighing on them also contributed to the appearance of the binary number system.

Further conjectures in this direction lead to some new conclusions. Beam scales and the beams themselves appeared simultaneously with Homo sapience and even earlier. The simplest pair of scales is a man's two arms, and, hence, the very structure of the human body, i.e., the existence of arms, served as a basis for the appearance of the binary NS and the EML and OML methods.

I believe that the invention of beams, beam scales is as important for the mankind as the invention of the wheel.

12. MODERN STATE OF FAST COMPUTATIONS

Let us discuss briefly the further development of fast computations and the modern state of this line of investigation (after 1962). First of all we will show that division reduces to addition, subtraction, and multiplication of numbers.

It has been mentioned, that division of a number a by a number b with a remainder, i.e., the calculation of the numbers q and r in the relation

$$a = qb + r, \qquad 0 \le r < b,$$

reduces to addition, subtraction, and multiplication, and if a and b are at most n-digit numbers, then the complexity of the division of a by b is of the order of $O(M(n))$.

First, one computes the number $1/b$ to within 2^{-n-1}, i.e., the numbers $\varepsilon_1, \ldots, \varepsilon_{n+1}$ in the relation

$$\frac{1}{b} = 0, \varepsilon_1 \ldots \varepsilon_{n+1} + \theta \cdot 2^{-n-1}, \qquad |\theta| \le 1.$$

In this case q is equal to one of the following three numbers: $[a \cdot 0, \varepsilon_1 \ldots \varepsilon_{n+1}] \pm 0.1$. Consequently, the determination of q requires $O(M(n))$ operations. The numbers $\varepsilon_1, \ldots, \varepsilon_{n+1}$ can be found with the aid of the following lemma.

Lemma. *Let* $1/2 < x < 1$ *and* $s = 1/x$. *If*

$$|s - s_k| < 2^{-k},$$

then, for $s_{2k} = xs_k^2 - 2s_k$, *we have*

$$|s - s_{2k}| < 2^{-2k}.$$

The number 3/2 is taken as the first approximation, i.e., as s_1. The division is performed in [7] in this way (see also [14, 15]).

13. ON SOME FAST ALGORITHMS STIMULATED BY KML

The KML algorithm is a source and a prototype of all fast multiplications (for a brief survey of the history of this problem see [15]). This first of all relates to the Strassen algorithm for matrix multiplication (1969), which, in essence, is the application of KML to multiplication of matrices (see [16]). In this case, addition, subtraction, multiplication of two matrix elements, recording of a matrix element, and recording of an arithmetical operation are regarded as a single operation..

Indeed, as is known, matrices are multiplied "blockwise", i.e., if A and B have the form

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \qquad B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix},$$

where A and B are $n \times n$ matrices, $n = 2^m$, and A_{ij} and B_{ij} are $n_1 \times n_1$ matrices, $2n_1 = n$, respectively (the "blocks" of the matrices A and B), then we have

$$AB = C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix},$$

where C_{ij} are $n_1 \times n_1$ matrices such that

$$C_{11} = A_{11}B_{11} + A_{12}B_{21},$$

etc. Relations for the matrices C_{ij} show that their determination requires 8 multiplications of $n_1 \times n_1$ matrices and 4 additions. This algorithm provides an estimate of the form $O(n^3)$ for the multiplication of two $n \times n$ matrices. However, the ordinary multiplication of matrices also requires $O(n^3)$ operations. Strassen [16] found an identity which requires 7 rather than 8, multiplications of blocks and 18 additions. The Strassen identity has the following form.

Let

$$\begin{aligned}
\text{I} &= (A_{11}+A_{22})(B_{11}+B_{22}),\\
\text{II} &= (A_{21}+A_{22})B_{11},\\
\text{III} &= A_{11}(B_{12}-B_{22}),\\
\text{IV} &= A_{22}(-B_{11}+B_{21}),\\
\text{V} &= (A_{11}+A_{12})B_{22},\\
\text{VI} &= (-A_{11}+A_{21})(B_{11}+B_{12}),\\
\text{VII} &= (A_{12}-A_{22})(B_{21}+B_{22}).
\end{aligned}$$

Then

$$\begin{aligned}
C_{11} &= \text{I}+\text{IV}-\text{V}+\text{VII},\\
C_{21} &= \text{II}+\text{IV},\\
C_{12} &= \text{III}+\text{V},\\
C_{22} &= \text{I}+\text{III}-\text{II}+\text{VI}.
\end{aligned}$$

Therefore, if $\psi(n)$ is the complexity of multiplication of two $n \times n$ matrices, then the application of the Strassen identity results in

$$\psi(n) \le 7\psi(n/2) + cn,$$

$$\psi(n) \le c_1 n^{\log_2 7}, \qquad \log_2 7 = 2,807\ldots,$$

where $c > 0$ and $c_1 > 0$ are absolute constants. It is clear that the Strassen estimate can be refined by partitioning the factors A and B into smaller blocks and finding a greater number of dependent multiplications. By now this has been performed by many authors, but the attempts to obtain $\psi(n) = O(n^{2+\varepsilon})$, where $\varepsilon > 0$ is an arbitrary number, have yet failed (1995).

It should be mentioned that Strassen was on probation for several months in 1965 under the guidance of Kolmogorov who familiarized him with the entire area of computational complexity and all the achievements in this field.

Another fast method is the algorithm of fast (discrete) Fourier transform discovered by Cooley and Tukey in 1965 [17], which, I believe, was also stimulated by KML. In particular, Schönhage, Grotefeld, and Vetter [9] write about the KML method as a prototype of all types of fast multiplications.

14. REFINEMENT OF KML

As was mentioned, by splitting a into a large number of terms, i.e., representing a in the form

$$a = a_0 + 2^m a_1 + 2^{2m} a_2 + \ldots + 2^{rm} a_r,$$

where $a_0, a_1, a_2, \ldots, a_r$ are m-digit numbers and $rm = n$, we have

$$a^2 = \left(\sum_{j=0}^{r} a_j 2^{mj}\right)^2 = \sum_{s=0}^{2r} c_s 2^{ms},$$

where

$$c_s = \sum_{\substack{j+\nu=s\\ 0\le j,\nu\le r}} a_j a_\nu.$$

The coefficients c_s can be found from the system of equations

$$(a_0 + a_1 x + a_2 x^2 + \ldots + a_r x^r)^2 = \sum_{s=0}^{2r} c_s x^s,$$

where one should set $x = 0, \pm 1, \ldots, \pm 2r$. By selecting the optimal value of r, we can find the corresponding estimate for $M(n)$. In this way, the estimate for $M(n)$ was refined by the three authors: Toom [18], Cook [19], and Schönhage [20]. The improved estimate is of the form

$$M(n) = O(ne^{c\sqrt{\log n}}), \tag{9}$$

where $c > 0$ is an absolute constant. Note that Schönhage used a special residue arithmetic, which allowed him to diminish the constants in (9).

Finally, in 1971 Schönhage and Strassen [21] constructed an algorithm with an upper estimate for $M(n)$ that is at present the best:

$$M(n) = O(n \log n \log\log n).$$

The construction of the Schönhage-Strassen algorithm is essentially based on the application of the fast Fourier transform (for computing c_s).

15. FAST COMPUTATION OF ALGEBRAIC AND SIMPLEST TRANSCENDENTAL FUNCTIONS

If $y = f(x)$ is an algebraic function, then we have

$$S_f(n) = O(M(n)).$$

The proof of this relation is essentially based on the Newton method of tangents; (see [7, 14]). If $y = f(x)$ is a simplest transcendental functions (e.g., $f(x) = e^x$, the inverse of e^x, a trigonometric function, or some superposition of these functions and algebraic functions), then we have

$$S_f(n) = O(M(n) \log n). \tag{10}$$

The proof of this relation essentially uses an iterative method, elliptic integrals, AGM (the Gaussian algorithm of arithmetic and geometric means), and the Landen transformation (see [22, 23]).

16. FAST COMPUTATION OF HIGHER TRANSCENDENTAL FUNCTIONS

If $y = f(x)$ is a higher transcendental function (the Euler gamma function, a Bessel function, a hypergeometric function, etc.), then we have

$$S_{f,x_0}(n) = O(M(n) \log^2 n). \tag{11}$$

Some results relating to this subject were published by Borwein and Borwein in [24] without presenting the computation algorithms and with an indication that these are iterative algorithms. In recent years E.A. Karatsuba suggested a new method for fast computation of the simplest and higher transcendental functions, which is not iterative, admits of paralleling, and called it FEE (fast evaluation of functions of the type of the Siegel E-functions) [25–27]. In particular, in these papers an interesting fact was revealed, namely estimate (11) is obtained for these functions on the condition that the parameters of the computed functions and the value of x_0 are algebraic numbers (which is an exact analog of the well-known theorems in the theory of algebraic numbers).

17. IMPLEMENTATION OF FAST ALGORITHMS

It is difficult to give an exhaustive survey of implementations of fast algorithms and, in particular, KML, because, for instance, the KML algorithm, which has a very simple logical structure, can be realized with the aid of a microcircuit, and it is impossible to trace these implementations if they are not reflected in the project. Here I only point out the above-mentioned excellent monograph by Schönhage, Grotefeld, and Vetter [9], which presents the authors' results on the possibility of implementation of KML and the Schönhage-Strassen multiplication algorithm.

In May 1981 I gave my manuscript of a short article "Actual Computations" to Professor V.A. Mel'nikov, one of the leading supercomputer researchers in the USSR, where I suggested some realizations of fast computation algorithms for elementary functions, the simplest transcendental functions, and, of course, for KML. I have no information about any actual technological realization of these algorithms.

18. LOWER ESTIMATES

The problem of lower estimates for $S_f(n)$ and, in particular, for $M(n)$, remains unsolved. In this area, nothing but some trivial results of the type

$$n < M(n)$$

are known. There are many results concerning lower estimates under some constraints on the algorithms used (e.g., see [7]), but this is quite a different line of investigation. We can state the following hypotheses:

$$\text{(I)} \quad \sup_n \frac{M(n)}{n} = +\infty;$$

$$\text{(II)} \quad \sup_n \frac{M(n)}{n \log n} > 0;$$

$$\text{(III)} \quad \sup_n \frac{S_f(n)}{n^2} > 0,$$

where $f(x) = \Gamma(x)$, $x_0 = \pi$. However, at present no approaches to their proof are known.

CONCLUSION

In connection with the presented investigation that trace a way from the ancient times to the present day, I want to emphasize an important fact related to the modern development of mathematics. In recent decades, many investigators published a great number of mathematical works. Whereas the classics of mathematics regarded the science of mathematics as an objective reflection of reality, many of the new investigators do not share this opinion. They proclaim that mathematics is a result of pure imagination. Their task is to invent a notion, a theory, a proof, etc. As to the classics, they held to a quite different viewpoint on the work of a mathematician, which was reflected in their statements of the type "I found a solution to the problem," "I found a proof", "I found a notion", etc. These two words to "invent" and to "find" demonstrate a profound distinction between the two tendencies in mathematics and between the two approaches to the mathematical investigation.

I express my deep gratitude to D.V. Senchenko for valuable remarks.

REFERENCES

1. Kolmogorov, A.N., *Informatsionnaya teoriya i teoriya algoritmov* (Information Theory and Theory of Algorithms), Moscow: Nauka, 1987.
2. Kolmogorov, A.N., On Some Asymptotic Characteristics of Completely Bounded Metric Spaces, *Dokl. Akad. Nauk SSSR*, 1956, vol. 108, no. 3, pp. 385–388.
3. Vitushkin, A.G., *Otsenka slozhnosti zadachi tabulirovaniya* (Estimation of Complexity for the Tabulation Problem), Fizmatgiz, 1959.
4. Kolmogorov, A.N., Some Approaches to Estimation of Complexity of Approximate Representation and Computation of Functions, *Proc. Intern. Congr. Math. Stokholm*, 1963, pp. 369–376.
5. Ofman, Yu.P., On Asymptotic Complexity of Discrete Functions, *Dokl. Akad. Nauk SSSR*, 1962, vol. 145, no. 1, pp. 48–51.
6. Svoboda, A. and Valach, M., *Stroje zpracov. inform.*, 1955, vol. 3, pp. 247–295.
7. Knuth, D., *The Art of Computer Programming*, vol. 2, *Seminumerical Algorithms*, Reading (MA): Addison-Westley Publ. Comp.; Menlo Park (CA), London: Don Mills, Ont., 1969.
8. Karatsuba, A. and Ofman, Yu., Multiplication of Multiplace Numbers on Automata, *Dokl. Acad. Nauk SSSR*, 1962, vol. 145, no. 2, pp. 293–294.
9. Schönhage, A., Grotefeld, A.F.W., and Vetter, E., *Fast Algorithms*, Wissenschaftsverlag, 1994.
10. Van der Waerden, B.L., *Ontowakende Wetenschap*, Groningen, 1950.
11. Neugenbauer, O., *Forleisungen über Geschichte der antiken mathematische Wissenschaften*, Berlin: 1934.
12. Bashmakova, I.G. and Yushkevich, A.P., *Proiskhozhdenie sistem schisleniya. Entsiklopediya elementarnoi matematiki*, vol. 1, *Arifmetika* (Origin of Number Systems. Encyclopedia of Elementary Mathematics, vol. 1, Arithmetic), Moscow, Leningrad: Gostekhteorizdat, 1951.
13. Struik, D.J., *Abriss der Geschichte der Mathematik*, Berlin, Berlin: Veb Deutcher Verlag der Wissenschaften, 1963.
14. Benderskii, A.A., Fast Calculations, *Dokl. Akad. Nauk SSSR*, 1975, vol. 223, no. 5, pp. 1041–1043.
15. Karacuba, A.A., Berechnungen und die Kompliziertheit von Beziehungen, *Elektron. Informationsverarb. und Kybern*, 1975, no. 10–12, pp. 603–606.
16. Strassen, V., Gaussian Elimination Is Not Optimal, *Numer. Math.*, 1969, vol. 4, no. 4, pp. 354–356.
17. Cooley, J.W. and Tukey, J.W., An Algorithm for the Machine Calculation of Complex Fourier Series, *Math. Comput.*, 1965, vol. 19, pp. 293–301.
18. Toom, A.A., On the Complexity of a Circuit of Functional Elements Realizing Multiplication of Integers, *Dokl. Akad. Nauk SSSR*, 1963, vol. 150, no. 2, pp. 496–498.
19. Cook, S.A., On the Minimum Computation Time of Functions, *Ph D Thesis*, New York: Harvard Univ., 1966, pp. 51–77.
20. Schönhage, A., Schnelle Multiplikation großer Zahlen, *Computing*, 1966, vol. 1, pp. S. 182–196.
21. Schönhage, A. and Strassen, V., Schnelle Multiplikation großer Zahlen, *Computing*, 1971, vol. 7, no. 3/4, pp. 281–292.
22. Brent, R.P., Fast Multiple-Precision Evaluation of Elementary Functions, *Assoc. Comput. Math.*, 1976, vol. 23, pp. 242–251.
23. Borwein, J.M. and Borwein, P.B., *Pi and AGM. A Study in Analytic Number Theory and Computational Complexity*, New York: Wiley, 1987.
24. Borwein, J.M. and Borwein, P.B., On the Complexity of Familiar Functions and Numbers, *SIAM Rev.*, 1988, vol. 30, no. 4, pp. 589–601.
25. Karatsuba, E.A., On Fast Evaluation of Transcendental Functions, *Dokl. Akad. Nauk SSSR*, 1991, vol. 318, no. 2, pp. 278, 279.
26. Karatsuba, E.A., Fast Evaluation of Transcendental Functions, *PPI*, 1991, vol. 27, no. 4, pp. 87–110.
27. Karatsuba, Catherina A., Fast Evaluation of Bessel Functions, *Integral Transforms and Special Functions*, 1993, vol. 1, no. 4, pp. 269–276.