



Soviet-era science, translated into English

Reports of the Academy of Sciences of the USSR

1958

SovietRxiv

View the original and related papers at <https://sovietrxiv.org/items/ru-195801.33181>

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.

Abstract

Full Text

Reports of the Academy of Sciences of the USSR
1958. Vol. 121, No. 5

MATHEMATICS

V. N. TEITELBAUM

COMPARISON OF NUMBERS IN THE CZECH NUMBER SYSTEM

(Presented by Academician M. V. Keldysh on 10 IV 1958)

I. Statement of the problem. The Czech system¹ is here understood to mean a number system in which a number is represented by the collection of its least nonnegative residues modulo p_1, p_2, \dots, p_n . The numbers p_1, p_2, \dots, p_n are positive primes. We shall call their collection the **base**. The correspondence between integers and collections of residues is, in general, not one-to-one, but it becomes so if the set of numbers under consideration is restricted. For nonnegative numbers less than the product $p_1 p_2 \cdots p_n$, the correspondence is one-to-one.

Operations on numbers are performed by means of operations on their residues. If to each residue of the collection of residues representing a given number one assigns a definite digit position, then one may say that in the Czech system the first three arithmetical operations are carried out by digitwise operations. Addition is carried out by digitwise addition modulo, subtraction by subtraction modulo, multiplication by digitwise multiplication modulo. In this system there are no "difficulties of carrying from digit to digit," since the result in one digit does not depend on the results in neighboring digits.

Considering only nonnegative integers less than the product $p_1 p_2 \cdots p_n$, we shall set forth a method for comparing the magnitudes of two numbers represented in the Czech system—this is the aim of the present work. The method is applicable only if the number 2 is among the prime numbers of the base. In the contrary case another method is applicable (we do not present it here).

II. Notation and definitions.

1. We number the base numbers so that the condition

$$2 = p_1 < p_2 < \cdots < p_n. \quad (1)$$

is satisfied.

2. We shall write

$$a = (\alpha_1, \alpha_2, \dots, \alpha_n). \quad (2)$$

This means that $0 \leq a < p_1 p_2 \dots p_n$ and a has the given collection $\alpha_1, \alpha_2, \dots, \alpha_n$ of residues modulo p_1, p_2, \dots, p_n . The residue α_s will be called the residue of the s -th digit.

3. If the number a is less than the product of part of the prime numbers of the base,

$$0 \leq a < p_i p_{i+1} \dots p_n \quad (1 \leq i \leq n), \quad (3)$$

then a is determined by its residues modulo p_i, p_{i+1}, \dots, p_n . Therefore, for numbers satisfying condition (3), along with the general notation $a = (\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_n)$, we introduce the notation $(\alpha_i, \alpha_{i+1}, \dots, \alpha_n)$ and shall write

$$a = (\alpha_i, \alpha_{i+1}, \dots, \alpha_n). \quad (4)$$

4. Let

$$p_1 p_2 \dots p_n = M. \quad (5)$$

5. We shall distinguish numbers greater than $M/2$ and less than $M/2$.

- a) A **number of the first half** is a number a satisfying the condition:

$$0 \leq a < M/2. \quad (6)$$

- b) A **number of the second half** is a number a :

$$M/2 \leq a < M. \quad (7)$$

6. Let there be two numbers a and b ;

$$a = (\alpha_1, \alpha_2, \dots, \alpha_n); \quad (8)$$

$$b = (\beta_1, \beta_2, \dots, \beta_n). \quad (9)$$

Let us form such a collection of residues that each of its residues is congruent to the difference of the residues of the corresponding digits of the collections (8) and (9) modulo the corresponding modulus and is at the same time the least nonnegative number among the numbers satisfying this condition. Here is this collection:

$$\alpha_1 - \beta_1 + p_1 k_1, \alpha_2 - \beta_2 + p_2 k_2, \dots, \alpha_n - \beta_n + p_n k_n. \quad (10)$$

Here k_i satisfies the conditions

$$k_i = \begin{cases} 0, & \text{if } \alpha_i \geq \beta_i, \\ 1, & \text{if } \alpha_i < \beta_i. \end{cases} \quad (11)$$

But every collection of n residues determines a certain number. Therefore we shall write

$$c = (\alpha_1 - \beta_1 + p_1 k_1, \dots, \alpha_n - \beta_n + p_n k_n) \quad (k_i \text{ satisfies (11)}). \quad (12)$$

This number, generally speaking, does not coincide with the difference of the numbers a and b , since the difference may be negative, whereas $c \geq 0$ (by the condition). In order to reflect in the definition the way of obtaining the number c from the numbers a and b , we shall call the number c the **tabular difference** of the numbers a and b and introduce for the number c the special notation $[a - b]$; it is written:

$$c = [a - b] = (\alpha_1 - \beta_1 + k_1 p_1, \dots, \alpha_n - \beta_n + k_n p_n). \quad (13)$$

Definition. The number c is called the **tabular difference** of the numbers a and b with representations (8) and (9), if it has the representation (12).

III. **Lemma 1.** If $a \geq b$, then

$$a - b = [a - b]. \quad (14)$$

The proof is obvious.

Lemma 2. If $a \neq b$, then

$$[a - b] + [b - a] = M. \quad (15)$$

Proof. According to the definition of the tabular difference,

$$[a - b] \equiv \alpha_i - \beta_i \pmod{p_i}, \quad [b - a] \equiv \beta_i - \alpha_i \pmod{p_i} \quad (i = 1, 2, \dots, n). \quad (16)$$

From (16) it follows that $[a - b] + [b - a] \equiv 0 \pmod{p_i}$ ($i = 1, 2, \dots, n$), hence the number $[a - b] + [b - a]$ is divisible by each p_i , and therefore also by their product M . But $0 < [a - b] + [b - a] < 2M$ (according to II, 3 and Lemma 1), and this permits the proof to be considered complete.

Corollary. If $a \neq b$ and $[a - b] \neq M/2$, then $[a - b]$ and $[b - a]$ are numbers of different halves.

Theorem 1. *If a, b are numbers of one half, then the membership of the number $[a - b]$ in the numbers of the first half is a necessary and sufficient condition for $a \geq b$.*

Proof. Necessity. Let a and b be numbers of one half and $a \geq b$. Then $0 \leq a - b < M/2$; consequently (by Lemma 1) $0 \leq [a - b] < M/2$, as was required to prove.

Sufficiency. Let $0 \leq [a - b] < M/2$. If we assume that $b > a$, then, by necessity, $[b - a]$ is a number of the first half. This contradicts the corollary to Lemma 2.

After Theorem 1 has been proved, the question of comparing the magnitudes of numbers is reduced to the problem of determining to which half a given number belongs. Indeed, suppose two numbers a and b are given; suppose we can determine to which half a given number belongs. Then, if it is determined that a and b are numbers of different halves, the larger of them will be the number of the second half. If, however, it turns out that the numbers a and b belong to one half, then, forming the tabular difference $[a - b]$, we find to which half it belongs. If to the first, then $a \geq b$; if to the second, then $a < b$. It remains to solve the problem of determining the membership of a number in a given half.

Let us first determine how many numbers there are with identical sets of remainders

$$\alpha_2, \alpha_3, \dots, \alpha_n. \tag{17}$$

Lemma 3. *There exist two and only two numbers possessing the fixed set of remainders (17). These numbers are of opposite parity and belong to different halves.*

Proof. α_1 takes two values: 0 and 1. This proves the validity of the definite part of the assertion. The fact that the corresponding numbers belong to different halves is proved by the observation that the modulus of their difference must be divisible by the number $M/2$. Thus the lemma is proved.

IV. Determining the membership of a number in a given half. A number of the first half is determined by the set of remainders (17). If we can find what parity the number of the first half possessing the given remainders $\alpha_2, \alpha_3, \dots, \alpha_n$ has, then, comparing it with the parity of the proposed number $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ (which is determined by the number α_1), we shall (by Lemma 3) learn to which half this number belongs: in the case of coincidence of parities, to the first; in the opposite case, to the second.

The process of determining the parity of a number of the first half from the set $\alpha_2, \alpha_3, \dots, \alpha_n$ is as follows. Let $0 \leq a < p_i p_{i+1} \dots p_n$ ($2 \leq i < n$); then

(according to II, 3) $a = (\alpha_i, \alpha_{i+1}, \dots, \alpha_n)$. We want to obtain from a the nearest number, not exceeding a , that is divisible by p_i . Clearly such a number is $a - \alpha_i$: $0 \leq a - \alpha_i < p_i p_{i+1} \dots p_n$. Its representation in the Czech system (by Lemma 1) will be the tabular difference $[a - \alpha_i]$.

The number $[a - \alpha_i]$, like $a - \alpha_i$, is less than the product $p_i p_{i+1} \dots p_n$; therefore it is determined by the last $n - i + 1$ remainders and has the form

$$[a - \alpha_i] = \tag{18}$$

$$(0; \alpha_{i+1} - \alpha_i + k_{i+1} p_{i+1}; \alpha_{i+2} - \alpha_i + k_{i+2} p_{i+2}; \dots; \alpha_n - \alpha_i + k_{np} n).$$

The integer

$$\frac{[a - \alpha_i]}{p_i}$$

is less than the product $p_{i+1} p_{i+2} \dots p_n$; consequently, it is determined by the last $n - i$ digits. Its representation

$$\frac{[a - \alpha_i]}{p_i} = \left(\frac{\alpha_1 - \alpha_i + k_{i+1} p_{i+1}}{p_i} (p_{i+1}); \frac{\alpha_{i+2} - \alpha_i + k_{i+2} p_{i+2}}{p_i} (p_{i+2}); \dots; \frac{\alpha_n - \alpha_i + k_{np} n}{p_i} (p_n) \right), \tag{19}$$

where $\frac{a}{b} (p)$ denotes the quotient modulo p . Then, finding the number divisible by p_{i+1} nearest to this new number, by subtracting the $(i + 1)$ -st residue of the number $\frac{[a - \alpha_i]}{p_i}$ from all the digits of this number and dividing by p_{i+1} , and continuing this process of subtraction and division, we obtain a nonnegative number x , less than p_n . At this point the process is completed. The number x will have the form (in the notation system II, 3)

$$x = (r_n) \quad (r_n \text{ is the residue of } x \text{ modulo } p_n). \tag{20}$$

It is clear that $x = r_n$. Therefore the parity of the number x coincides with the parity of the number r_n . Thus, the parity of the last quotient is known to us. But in carrying out the process of decreasing the given number, one can record the change of parity (it changes only under subtractions). Therefore the parity of the last quotient immediately determines the parity of the original number. This, as was already said, solves the problem of comparing the magnitudes of numbers.

How many operations does the method require? If it is known that the two proposed numbers are numbers of one half, then one subtraction operation and

$(n - 2) \cdot 2$ subtraction and division operations must be performed. Thus, if the bases of the system are the prime numbers $2, 3, 5, \dots, 31$, then the total number of operations will be $1 + 2(11 - 2) = 19$. If it is not known whether the numbers belong to one half, then $1 + 6(n - 2)$ operations are necessary—this is the maximum number. It is clear that the process may also end earlier. This will be revealed if, in the course of the process, one of the quotients takes the form

$$\underbrace{\alpha_i, \alpha_i, \dots, \alpha_i}_{(n-i+1) \text{ digits}}.$$

Received
8 IV 1958

CITED LITERATURE

1. A. Svoboda, M. Valach, *Stroje na zpracovani informazi*, Sborn. 3, 1955.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.