Acknowledgment

The authors wish to thank J. A. Duffy, N. M. Herbst, and P. M. Will for their assistance in planning this display, D. J. Fraleigh and C. F. Marr who built the system, and N. M. Herbst, A. Odarchenko, G. H. Purdy, and R. N. Wolfe who did the programming.

References

[1] N. M. Herbst and P. M. Will, "An experimental laboratory for pattern recognition and signal processing," *Commun. Ass. Comput. Mach.*, vol. 15, pp. 231–244, Apr. 1972.

[2] R. J. Potter, "An optical character scanner," *Soc. Photogr. Instrumen. Eng. J.*, vol. 2, pp. 75–78, Feb.–Mar. 1964.

[3] M. R. Davis and T. O. Ellis, "The RAND tablet: A man-machine communication device," in *1964 Fall Joint Comput. Conf., AFIPS Conf. Proc.*, vol. 26. Washington, D. C.: Spartan, 1964, pp. 325–331.

[4] J. S. Birnbaum *et al.*, "An interactive graphics system for nuclear data acquisition," *IBM J. Res. Develop.*, vol. 13, pp. 52–60, Jan. 1969.

[5] R. J. Houldin, "IBM graphic display system," *Inform. Display*, pp. 34–40, Sept.–Oct. 1966.

[6] D. G. Fink, *Television Engineering Handbook*. New York: McGraw-Hill, 1951, pp. 1–12.

[7] H. H. Poole, *Fundamentals of Display Systems*. Washington, D. C.: Spartan, 1966, p. 284.

[8] N. H. Kreitzer, "Buffer store for an 1800 computer and experimental magnetic recording system," IBM RC 2362, Feb. 3, 1969.

Norman H. Kreitzer (M'65) was born in Cornwall, N. Y., on May 14, 1934. He received the B.S. degree in electrical engineering from the University of Vermont, Burlington, Vt., in 1956 and the M.E.E. degree from Syracuse University, Syracuse, N. Y., in 1961.

From 1956 to 1962 he worked for the General Electric Company, Syracuse, N. Y., on analog and digital circuit design for advanced military air weapons control systems. Since 1962 he has been employed at the Research Division of the IBM T. J. Watson Research Center, Yorktown Heights, N. Y. His assignments there have been in experimental and exploratory systems designs. His current interests are in terminal design and display technology.

William J. Fitzgerald (M'50) was born in New Haven, Conn., on July 14, 1926. He received the B.E.E. degree from Yale University, New Haven, Conn., in 1949, the M.E.E. degree from Rensselaer Polytechnic Institute, Troy, N. Y., in 1952 and the Ph.D. degree in electrical engineering from the University of California, Berkeley, in 1965.

He joined IBM in Poughkeepsie in 1951 and worked on power systems for the IBM 701, Sage System Direction Centers, and early transistorized computers. At IBM, Kingston, he was a Senior Engineer, Manager of Cryogenic Circuit Development and worked in graphic applications. Since 1968 he has worked at the IBM T. J. Watson Research Center, Yorktown Heights, N. Y., where he was Manager of the Advanced I/O Experimental Facility concerned with optical scanners and computer displays. His current interest is graphic applications.

General Division in the Symmetric Residue Number System

EISUKE KINOSHITA, HIDEO KOSAKO, AND YOSHIAKI KOJIMA

***Abstract*—In the residue number system, the arithmetic operations of addition, subtraction, and multiplication are executed in the same period of time without the need for interpositional carry. There is a hope for high-speed operation if residue arithmetic is used for digital computation. The division process, which is one of the difficulties of this operation, is developed in the symmetric residue number system. The method described here is iterative in nature and requires the availability of two tables of the symmetric residue representations of a certain kind of integer. An algorithm for general division is derived, and the way of choosing the entries which are used to find a quotient is discussed.**

***Index Terms*—Additive inverse, algorithm for general division, approximate dividend, approximate divisor, approximate quotient, division with zero remainder, multiplicative inverse, symmetric mixed-radix conversion, symmetric residue number system.**

Manuscript received April 19, 1971; revised July 31, 1972.

The authors are with the Department of Electronics, University of Osaka Prefecture, Osaka, Japan.

I. Introduction

In the residue number system, addition, subtraction, and multiplication are executed without the need for interpositional carry [1]–[3]. In particular, for the case of multiplication, the need for partial products is removed. Division, however, is such a complicated process that it is not easily mechanized. In spite of many investigations [3], [4], there is much left to study in the area of residue division.

Several kinds of representations for residue numbers [3], [5] have been proposed, each of which has merits and demerits. In the symmetric residue number system (SRNS), it is easy to find the additive inverse of a residue digit and to detect the sign of a residue number. The purpose of this paper is to propose a solution for the division process in the symmetric residue number system.

II. Symmetric Residue Arithmetic Fundamentals

Before considering the problem of general division, an introduction to symmetric residue arithmetic will now be given, sufficient to make this paper self-contained.

The symmetric residue of x modulo m, denoted $/x/_m$, is the least remainder in absolute value when an integer x is divided by another integer m (m is called a modulus; m is assumed positive here). A commonly used form of this condition is

$$x = \left\langle \frac{x}{m} \right\rangle m + /x/_m$$

where $/x/_m$ is an integer such that $-[(m-1)/2] \leqq /x/_m \leqq [m/2]$. The symbols [ ] indicate a rounding operation. The quantity $[m/2]$ is the integer value of the quotient $m/2$, for example.

For m odd, the quantity $\langle x/m \rangle$ is the closest integer to x/m. If m is even, the quantity $\langle x/m \rangle$ is again the closest integer to x/m, except that if x is of the form $nm/2$, where n is odd, the quantity $\langle x/m \rangle$ is the closest integer to $(x-1)/m$.

Example 1

Let $m=33$, $x=185$. Then $\langle 185/33 \rangle = 6$. Hence,

$$/x/_m = x - \langle x/m \rangle m = 185 - 6 \times 33 = -13.$$

An SRNS is defined by the choice of N moduli $m_1, m_2, \cdots, m_N$. If these moduli are chosen to be pairwise relatively prime, for any integer x in the interval $[-[(M-1)/2], [M/2]]$ (it should be noted that the outer square brackets indicate a closed interval), the symmetric residue sequence $/x/_{m_1}, /x/_{m_2}, \cdots, /x/_{m_N}$ uniquely represents x; in symbols,

$$x \leftrightarrow \{/x/_{m_1}, /x/_{m_2}, \cdots, /x/_{m_N}\}$$

where

$$M = \prod_{i=1}^{n} m_i$$

and $/x/_{m_i}$ is called the ith symmetric residue digit of x.

The symmetric residue representation for addition, subtraction, or multiplication of two numbers in an SRNS is, as long as the operands and the result all fall in the interval $[-[(M-1)/2], [M/2]]$,

$$x * y \leftrightarrow \{//x/_{m_1} * /y/_{m_1}/_{m_1}, //x/_{m_2} * /y/_{m_2}/_{m_2}, \cdots, //x/_{m_N} * /y/_{m_N}/_{m_N}\}$$

where the symbol $*$ represents addition, subtraction, or multiplication of two numbers.

In an SRNS the quantity $/-/x/_{m_i}/_{m_i}$ is called the additive inverse of $/x/_{m_i}$ modulo m_i. For m_i odd, the quantity $/-/x/_{m_i}/_{m_i}$ is $-/x/_{m_i}$. If m_i is even, the quantity $/-/x/_{m_i}/_{m_i}$ is again $-/x/_{m_i}$, except that if $x=m_i/2$, the quantity $/-/x/_{m_i}/_{m_i}$ is defined to be $/-/x/_{m_i}+m_i/_{m_i} = /x/_{m_i}$.

Example 2

For $m_1=7$, $m_2=11$, and $m_3=13$, the interval of definition is $[-500, 500]$. Let $x=23$, $y=18$.

$$x \leftrightarrow \{2, 1, -3\}, \qquad y \leftrightarrow \{-3, -4, 5\}$$

Addition: Moduli: 7 11 13

$$\begin{array}{rcrrr} 23 & \longleftrightarrow & \{\ 2, & 1, & -3\} \\ +\ 18 & \longleftrightarrow & \{-3, & -4, & 5\} \\ \hline 41 & \longleftrightarrow & \{-1, & -3, & 2\} \end{array}$$

Subtraction:

$$\begin{array}{rcrrr} 23 & \longleftrightarrow & \{\ 2, & 1, & -3\} \\ -\ 18 & \longleftrightarrow & \{-3, & -4, & 5\} \\ \hline 5 & \longleftrightarrow & \{-2, & 5, & 5\} \end{array}$$

Multiplication:

$$\begin{array}{rcrrr} 23 & \longleftrightarrow & \{\ 2, & 1, & -3\} \\ \times\ 18 & \longleftrightarrow & \{-3, & -4, & 5\} \\ \hline 414 & \longleftrightarrow & \{\ 1, & -4, & -2\} \end{array}$$

If $-[(m_i-1)/2] \leqq a \leqq [m_i/2]$ and $/ab/_{m_i}=1$, a is called the multiplicative inverse of b modulo m_i and is denoted by $a=/\frac{1}{b}/m_i$. The quantity exists uniquely if and only if $(b, m_i)=1$ and $/b/_{m_i} \neq 0$.

Now, the very restricted area of division with zero remainder will be briefly described. Division with zero remainder is division where the dividend is known to be an integer multiple of the divisor and the divisor is known to be relatively prime to M. The symmetric residue representation for division with zero remainder is

$$\frac{x}{y} \leftrightarrow \left\{ \left/ \left/ \frac{1}{y} \right/_{m_1} \times /x/_{m_1} \right/_{m_1}, \left/ \left/ \frac{1}{y} \right/_{m_2} \times /x/_{m_2} \right/_{m_2}, \cdots, \left/ \left/ \frac{1}{y} \right/_{m_N} \times /x/_{m_N} \right/_{m_N} \right\}$$

if and only if y divides x without remainder and $(y, m_i)=1$, for all i.

Example 3

Let $m_1=7$, $m_2=11$, $m_3=13$, $x=432$, $y=18$.

$$x \leftrightarrow \{-2, 3, 3\}, \quad y \leftrightarrow \{-3, -4, 5\}$$

$$\left/ \frac{1}{-3} \right/_7 = 2, \quad \left/ \frac{1}{-4} \right/_{11} = -3, \quad \left/ \frac{1}{5} \right/_{13} = -5.$$

Hence, for 432/18, the symmetric residue representation is

$$\{/2 \times (-2)/_7, /(-3) \times 3/_{11}, /(-5) \times 3/_{13}\} = \{3, 2, -2\} \leftrightarrow 24.$$

The symmetric mixed-radix conversion (SMRC) process is used to convert from the residue code of a number to its symmetric mixed-radix representation. The mixed-radix representation is of great importance in residue computation because it gives an effective solution for sign sensing and magnitude determination. A number x may be expressed in symmetric mixed-radix form as

$$x = \alpha_N \prod_{i=1}^{N-1} m_i + \cdots + \alpha_3 m_1 m_2 + \alpha_2 m_1 + \alpha_1 \qquad (1)$$

where the α_j (symmetric mixed-radix coefficients) are integers such that $-[(m_j-1)/2] \leq \alpha_j \leq [m_j/2]$. For a given set of moduli, the mixed-radix representation of x is denoted by $\langle \alpha_N, \alpha_{N-1}, \cdots, \alpha_1 \rangle$. Any integer in the interval $[-[(M-1)/2], [M/2]]$ may be represented uniquely in this form. Inspection of (1) shows the sign of x to be given by the sign of the most significant nonzero coefficient.

The α_j are determined sequentially in the following way. Since all terms of (1) except the last are multiples of m_1, it follows that $/x/_{m_1} = \alpha_1$. To determine α_2, $x - \alpha_1$ is formed in its residue code and then divided by m_1. This division is actually division with zero remainder as previously explained. Then

$$\frac{x - \alpha_1}{m_1} = \alpha_N \prod_{i=2}^{N-1} m_i + \cdots + \alpha_3 m_2 + \alpha_2.$$

If this equation is taken modulo m_2, the only remaining term on the right side is α_2. Hence $/(x-\alpha_1)/m_1/_{m_2} = \alpha_2$. In this manner, by successively subtracting α_j and dividing by m_j, all the α_j can be determined.

Example 4

Moduli $m_1 = 7$, $m_2 = 11$, $m_3 = 13$. Symmetric residue representation of number to be converted is $\{3, -5, -2\} \leftrightarrow 479$.

III. General Division Algorithm in the SRNS

Consider the symmetric residue system consisting of the moduli such that

$$m_1 < m_2 \cdots < m_N.$$

If one of the moduli is even, let the modulus be m_1.

The method makes use of division of an approximate dividend by an approximate divisor. Since, in the general case, the dividend and the divisor are not equal to the approximate dividend and the approximate divisor, respectively, an error is introduced in the quotient. This error is then iteratively reduced to zero.

A. Principle of the Method

Let y be the divisor and let x_{i-1} be the dividend in the ith($i = 1, 2, \cdots$) iteration.

Approximate Divisor: The symmetric mixed-radix representation of y is assumed to be

$$y \leftrightarrow \langle 0, \cdots, 0, \beta_l, \beta_{l-1}, \cdots, \beta_1 \rangle$$

where β_l is the most significant nonzero mixed-radix coefficient of y. The approximate divisor $\bar{y}$ is chosen to be

$$\bar{y} = \beta_l (1/K) m_1 m_2 \cdots m_{l-1} \qquad (2)$$

where $K = 1/\{1 + \beta_{l-1}/(\beta_l m_{l-1})\}$ (if $l = 1$, then $K = 1$).

Approximate Dividend: The symmetric mixed-radix representation of x_{i-1} is assumed to be

$$x_{i-1} \leftrightarrow \langle 0, \cdots, 0, \alpha_k, \alpha_{k-1}, \cdots, \alpha_1 \rangle$$

where α_k is the most significant nonzero mixed-radix coefficient of x_{i-1}. The approximate dividend $\bar{x}_{i-1}$ in the ith iteration is chosen to be

$$\bar{x}_{i-1} = \alpha_k m_1 m_2 \cdots m_{k-1}. \qquad (3)$$

Approximate Quotient: A method for finding an ap-

SMRC

	Moduli: 7	11	13	
	3	-5	-2	$\alpha_1 = 3$
Subtract $\alpha_1 = 3$:		3	3	
		3	-5	
Multiply by $/\frac{1}{\overline{7}}/_{m_i}$:		$/\frac{1}{\overline{7}}/_{11} = -3$	$/\frac{1}{\overline{7}}/_{13} = 2$	
		2	3	$\alpha_2 = 2$
Subtract $\alpha_2 = 2$:			2	
			1	
Multiply by $/\frac{1}{\overline{11}}/_{m_i}$:			$/\frac{1}{\overline{11}}/_{13} = 6$	
			6	$\alpha_3 = 6$

proximate quotient Z_i in the ith iteration stage will be described.

1) If $k \geqq l+2$, then the approximation

$$Z_i \approx \frac{\tilde{x}_{i-1}}{\tilde{y}} = \alpha_k(Km_{l+1}m_{l+2} \cdots m_{k-1})\left(\frac{m_l}{\beta_l}\right)$$

is obtained from (2) and (3). Since Z_i must be an integer, Z_i is chosen to be

$$Z_i = (\operatorname{sgn} \beta_l)\alpha_k\langle \tilde{K}m_{l+1}m_{l+2} \cdots m_{k-1}\rangle\left\langle\frac{m_l}{|\beta_l|}\right\rangle,$$
$$\text{if } |\alpha_k| \neq 1, \text{ or } |\alpha_k| = 1 \text{ and } \alpha_k\alpha_{k-1} \geqq 0 \quad (4)$$
$$Z_i = (\operatorname{sgn} \beta_l)\alpha_k\langle \tilde{K}'m_{l+1}m_{l+2} \cdots m_{k-1}\rangle\left\langle\frac{m_l}{|\beta_l|}\right\rangle,$$
$$\text{if } |\alpha_k| = 1 \text{ and } \alpha_k\alpha_{k-1} < 0 \quad (4')$$

where $\tilde{K}$ or $\tilde{K}'$ is the approximate value of K, which will be illustrated later.

2) If $k = l+1$, then

$$Z_i \approx \frac{\tilde{x}_{i-1}}{\tilde{y}} = \alpha_k(Km_l/\beta_l).$$

The approximate quotient Z_i in this case must be again an integer. Accordingly, the following approximation will be used to find Z_i:

$$Z_i = (\operatorname{sgn} \beta_l)\alpha_k\langle\langle \tilde{K}m_l\rangle/|\beta_l|\rangle,$$
$$\text{if } |\alpha_k| \neq 1, \text{ or } |\alpha_k| = 1 \text{ and } \alpha_k\alpha_{k-1} \geqq 0 \quad (5)$$
$$Z_i = (\operatorname{sgn} \beta_l)\alpha_k\langle\langle \tilde{K}'m_l\rangle/|\beta_l|\rangle,$$
$$\text{if } |\alpha_k| = 1 \text{ and } \alpha_k\alpha_{k-1} < 0. \quad (5')$$

3) If $k = l$, then

$$Z_i \approx \frac{\tilde{x}_{i-1}}{\tilde{y}} = \frac{\alpha_k}{\beta_l}.$$

In this case it is not sufficient to choose as the approximate quotient

$$Z_i = (\operatorname{sgn} \alpha_k)(\operatorname{sgn} \beta_l)\left\langle\frac{|\alpha_k|}{|\beta_l|}\right\rangle \quad (6)$$

because, in the case of $l \neq 1$, the direct use of (6) does not always terminate the iteration. A means of terminating the iteration is as follows.

If $\alpha_k\alpha_{k-1} \geqq 0$ and $\beta_l\beta_{l-1} < 0$, then α_k is increased by 1 in absolute value. If $\alpha_k\alpha_{k-1} < 0$ and $\beta_l\beta_{l-1} \geqq 0$, then α_k is decreased by 1 in absolute value. Otherwise α_k is left as it is. As a result, $0 \leqq |\alpha_k| \leqq [m_k/2]+1$ in this case. After this modification of α_k, (6) is used to obtain Z_i.

It should be noted that the case of $k = l$ does not require the use of K.

Once Z_i is found, this quantity is used in the recursive relationships

$$x_i = x_{i-1} - yZ_i, \qquad x_0 = x$$

and

$$Z_{i+1} \approx \frac{\tilde{x}_i}{\tilde{y}}$$

to obtain Z_{i+1}.

This iterative procedure is continued until $|x_i| < |y|$. If this occurs on the rth iteration,

$$Z = \left\langle\frac{x}{y}\right\rangle = \sum_{i=1}^{r-1} Z_i + Z'$$

where Z' is the correction factor such that

$$Z' = \begin{cases} 1, & \text{if } 2|x_{r-1}| > |y| \text{ and } x_{r-1}y > 0 \\ -1, & \text{if } 2|x_{r-1}| > |y| \text{ and } x_{r-1}y < 0 \\ 0, & \text{otherwise} \end{cases}$$

to obtain the closest integer to the complete quotient $\langle x/y\rangle$.

The validity of this method hinges on the following premises.

1) In the case of $k > l$, for any i, if the approximate quotient is so chosen that

$$0 < |Z_i| < \frac{2|x_{i-1}|}{|y|} \quad (7)$$

then the subscript k decreases to $k \leqq l$ after a finite number of iterations.

2) In the case of $k = l$, if $l \neq 1$, $|x_i|$ becomes less than $|y|$ after a finite number of iterations, except that $Z_i = 0, \pm 1$. If $l = 1$, then $|x_i| < |y|$.

These premises are proved by the authors.

It is evident that $|x_{i-1}| < |y|$ in the case of $k < l$.

B. Tables of Approximate Divisions

To obtain Z_i, the proposed method requires the availability of two tables in a special memory; one is of $\langle \tilde{K}m_{l+1}m_{l+2} \cdots m_{k-1}\rangle$, and the other is of $\langle m_l/|\beta_l|\rangle$, $\langle\langle \tilde{K}m_l\rangle/|\beta_l|\rangle$, or $\langle |\alpha_k|/|\beta_l|\rangle$, both of which are represented in the symmetric residue coding form.

Now, it will be shown that $2/3 \leqq K < 2$ for any set of moduli. It is easy to show that K takes its minimum value $K_{\min}$ when $\beta_l = 1$ and $\beta_{l-1} = [m_{l-1}/2]$. Moreover, K takes its maximum value $K_{\max}$ when $\beta_l = 1$ and $\beta_{l-1} = -[(m_{l-1})/2]$. Hence, for m_{l-1} odd,

$$K_{\min} = \frac{1}{1 + \dfrac{m_{l-1} - 1}{2m_{l-1}}} = \frac{1}{1 + \dfrac{1}{2} - \dfrac{1}{2m_{l-1}}} > \frac{2}{3}$$

and

$$K_{\max} = \frac{1}{1 - \dfrac{m_{l-1} - 1}{2m_{l-1}}} < \frac{1}{1 - \dfrac{m_{l-1}}{2m_{l-1}}} = 2.$$

Consequently,

$$2/3 < K < 2.$$

Likewise, for m_{l-1} even,

$$2/3 \leqq K < 2.$$

In the range $2/3 \leqq K < 2$, p values K_i $(i=1, 2, \cdots, p;$ $K_1 < K_2 < \cdots < K_p)$ are chosen at equal spacing over the interval K_1 to K_p. In addition to the K_i, p values K_i' are determined by $K_i' = K_i - \epsilon'$ $(i=1, 2, \cdots, p)$, where $\epsilon'(>0)$ is a correction factor of K_i when $k>l$, $|\alpha_k| = 1$ and $\alpha_k\alpha_{k-1} < 0$. Among the K_i or K_i', the closest value to K is used as K_i or K_i' according to circumstances. The way of determining K_i (or K_i') will be detailed in the Appendix.

In the following discussion, it will be assumed that there are q different values A_i $(i=1, 2, \cdots, q)$ in the union of the two sets $\{K_i\}$ and $\{K_i'\}$.

Table Composed of $\langle \tilde{K} m_{l+1} m_{l+2} \cdots m_{k-1} \rangle$: For such k and l as $k \geqq l+2$ $(l=1, 2, \cdots, N-2;$ $k=l+2, l+3, \cdots, N)$, there are $(N-2)(N-1)/2$ integers of the form $m_{l+1}m_{l+2} \cdots m_{k-1}$. The results of multiplying each integer of them by A_i $(i=1, 2, \cdots, q)$ are rounded off to an integer. The integers obtained in this way are represented in symmetric residue form to be made into a table. The entry in the table is obtained by means of K_i (or K_i'), k, and l.

Table Composed of $\langle \langle \tilde{K} m_l \rangle / |\beta_l| \rangle$ *and* $\langle |\alpha_k| / |\beta_l| \rangle$: It is assumed that at least one of the A_i is equal to 1. Then $m_l/|\beta_l|$ is expressed in the form of $\tilde{K} m_l / |\beta_l|$.

Now consider the following two kinds of numbers.

1) The numbers $\langle A_i m_l \rangle / |\beta_l|$, where $\langle A_i m_l \rangle$ are the integers obtained by rounding off $A_i m_l$ $(l=1, 2, \cdots, N-1;$ $i=1, 2, \cdots, q)$.

2) The numbers $|\alpha_k|/|\beta_l|$ where $k=l$, $l=1, 2, \cdots, N$ and $0 \leqq |\alpha_k| \leqq [m_k/2]+1$.

Each of these numbers is rounded off to an integer. The mutually different integer values obtained in this way are represented in symmetric residue form to be made into the other table. The entry in this table is obtained by means of K_i (or K_i'), l and $|\beta_l|$, or $|\alpha_k|$ and $|\beta_l|$.

C. General Division Algorithm

The proposed method may be summarized by steps as follows (see flow chart, Fig. 1), where it is often convenient to use the notation $((x)) \leftrightarrow \{/x/_{m_1}, /x/_{m_2}, \cdots, /x/_{m_N}\}$.

1) Reset $((Z))$ to zero.
2) Perform the mixed-radix conversion on $((y))$.
3) If $l=N$, go to next step. If $l \neq N$, determine $\tilde{K}$ or $\tilde{K}'$.
4) Perform the mixed-radix conversion on $((x))$.
5) If $k<l$, go to step 10). If $k=l$, go to step 7). Otherwise compare k with $l+1$. If $k=l+1$, compute $((Z_i))$ using (5) or (5′). If $k \neq l+1$, compute $((Z_i))$ using (4) or (4′).
6) Add $((Z_i))$ to $((Z))$, subtract $((y))((Z_i))$ from $((x))$ and return to step 4).
7) If $l=1$, compute $((Z_i))$ using (6) and go to step 9). If $l \neq 1$, increase or decrease α_k by 1 in absolute value according to the sgn of $\alpha_k\alpha_{k-1}$ and $\beta_l\beta_{l-1}$. Compute $((Z_i))$ using (6).
8) If $((Z_i)) = ((0))$, go to step 10). If $((Z_i)) = ((\pm 1))$, go to next step. Otherwise return to step 6).
9) Add $((Z_i))$ to $((Z))$, subtract $((y))((Z_i))$ from $((x))$.
10) Compute the correction factor $((Z'))$ and add $((Z'))$ to $((Z))$.

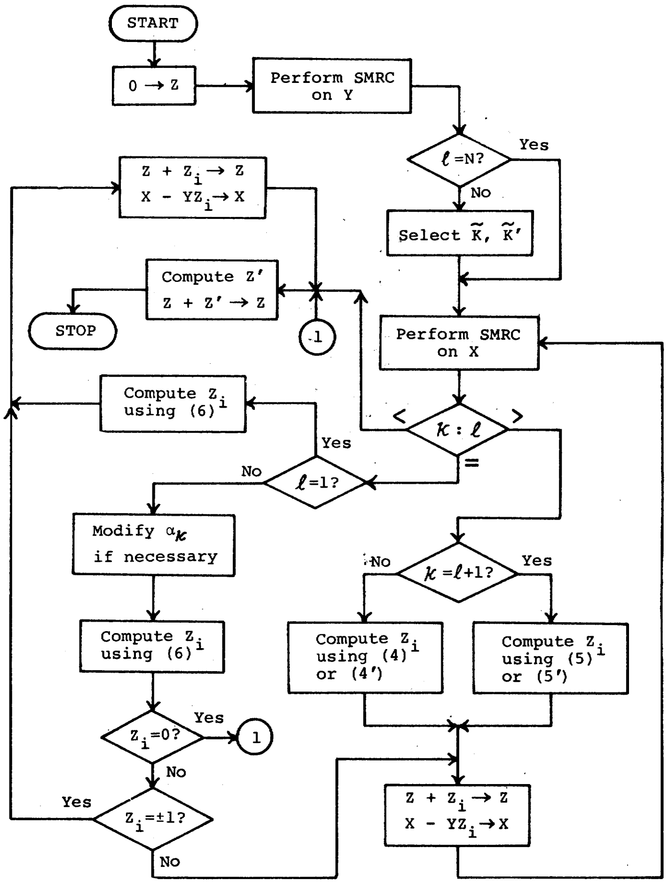


Fig. 1. Flow chart of residue division.

IV. Sample Problem

In the SRNS consisting of moduli 33, 35, 37, 41, 43, and 47 $([M/2]=1770532417)$, divide $x=356271687$ by $y=2887$.

The approximate values K_i are chosen, for instance, as $K_1=0.775$, $K_2=1.0$, $K_3=1.225$, $K_4=1.45$, $K_5=1.675$, and $K_6=1.9$. The correction factor ϵ' is chosen, for instance, as $\epsilon'=0.45$. Consequently, $K_1'=0.325$, $K_2'=0.55$, $K_3'=0.775$, $K_4'=1.0$, $K_5'=1.225$, and $K_6'=1.45$. (Material with respect to the choice of the values of K_i and K_i' is given in the Appendix.)

TABLE I

TABLE COMPOSED OF $(((\langle\tilde{K}m_{l+1}m_{l+2}\cdots m_{k-1}\rangle)))$ AND $(((\langle\tilde{K}'m_{l+1}m_{l+2}\cdots m_{k-1}\rangle)))$ FOR EXAMPLE SYSTEM

Πm_i \ K_i or K_i'	0.325	0.55	0.775	1.0	1.225	1.45	1.675	1.9
$m_2m_3m_4m_5$	((742003))	((1255697))	((1769391))	((2283085))	((2796779))	((3310473))	((3824167))	((4337861))
$m_2m_3m_4$	((17256))	((29202))	((41149))	((53095))	((65041))	((76988))	((88934))	((100880))
m_2m_3	((421))	((712))	((1004))	((1295))	((1586))	((1878))	((2169))	((2460))
m_2	((11))	((19))	((27))	((35))	((43))	((51))	((59))	((66))
$m_3m_4m_5$	((21200))	((35877))	((50554))	((65231))	((79908))	((94585))	((109262))	((123939))
m_3m_4	((493))	((834))	((1176))	((1517))	((1858))	((2200))	((2541))	((2882))
m_3	((12))	((20))	((29))	((37))	((45))	((54))	((62))	((70))
m_4m_5	((573))	((970))	((1366))	((1763))	((2160))	((2556))	((2953))	((3350))
m_4	((13))	((23))	((32))	((41))	((50))	((59))	((69))	((78))
m_5	((14))	((24))	((33))	((43))	((53))	((62))	((72))	((82))

TABLE II

TABLE COMPOSED OF $((((\langle\tilde{K}m_l\rangle/|\beta_l|)))$, $((((\langle\tilde{K}'m_l\rangle/|\beta_l|)))$, AND $(((\langle|\alpha_k|/|\beta_l|\rangle)))$ FOR EXAMPLE SYSTEM[a]

Storage location	Residue representation	Storage location	Residue representation	Storage location	Residue representation	Storage location	Residue representation
0	((0))	13	((13))	26	((26))	39	((45))
1	((1))	14	((14))	27	((27))	40	((50))
2	((2))	15	((15))	28	((29))	41	((51))
3	((3))	16	((16))	29	((31))	42	((53))
4	((4))	17	((17))	30	((32))	43	((54))
5	((5))	18	((18))	31	((33))	44	((59))
6	((6))	19	((19))	32	((34))	45	((62))
7	((7))	20	((20))	33	((35))	46	((66))
8	((8))	21	((21))	34	((36))	47	((69))
9	((9))	22	((22))	35	((37))	48	((70))
10	((10))	23	((23))	36	((39))	49	((72))
11	((11))	24	((24))	37	((41))	50	((78))
12	((12))	25	((25))	38	((43))	51	((82))

[a] Each location in the memory is assigned an address; the selection of the address is assumed to be performed by means of K_i (or K_i'), l and $|\beta_l|$, or $|\alpha_k|$ and $|\beta_l|$.

Tables, such as Table I and Table II, must be provided for approximate divisions in advance.

First perform the mixed-radix conversion on $((y))$ as follows:

$$y \leftrightarrow \langle 0, 0, 0, 2, 17, 16\rangle, \quad l = 3, \quad \beta_l = 2, \quad \beta_{l-1} = 17,$$

$$K = 1/(1 + \beta_{l-1}/(\beta_l m_{l-1})) = 0.8046.$$

Hence,

$$\tilde{K} = 0.775, \quad \tilde{K}' = \tilde{K} - \epsilon' = 0.325.$$

The quantities $(((\langle m_l/|\beta_l|\rangle))) = ((18))$, $((((\langle\tilde{K}m_l\rangle/|\beta_l|\rangle))) = ((14))$, and $((((\langle\tilde{K}'m_l\rangle/|\beta_l|\rangle))) = ((6))$ are read out from Table II.

First Iteration: Perform the mixed-radix conversion on $((x))$:

$$x \leftrightarrow \langle 5, -12, 14, -9, 12, -9\rangle, \quad k = 6, \quad \alpha_k = 5.$$

From Table I, $(((\langle Km_{l+1}m_{l+2}\cdots m_{k-1}\rangle))) = (((\langle 0.775m_4m_5\rangle)))$ $= ((1366))$. Therefore,

$$((Z_1)) = ((\alpha_k))(((\langle\tilde{K}m_{l+1}m_{l+2}\cdots m_{k-1}\rangle)))\left(\left(\left\langle\frac{m_l}{|\beta_l|}\right\rangle\right)\right)$$

$$= ((5))((1366))((18)) = ((122940))$$

$$((x_1)) = ((x)) - ((y))((Z_1))$$

$$= ((356271687)) = ((2887))((122940))$$

$$= ((1343907)).$$

TABLE III
AVERAGE AND STANDARD DEVIATION OF THE NUMBER OF ITERATIONS FOR THE EXAMPLES

k	l	Number of Examples	Average	Standard Deviation
6	1	100	7.18	1.60
6	2	100	6.21	1.40
6	3	100	4.93	1.06
6	4	100	3.66	0.81
6	5	100	1.98	0.45
6	6	100	0.34	0.48
Total		600	4.22	2.22

Second Iteration:

$$x_1 \leftrightarrow \langle 0, 1, -10, 17, -16, 15 \rangle,\ k = 5,\ \alpha_k = 1,\ \alpha_{k-1} < 0.$$

From Table I, $(((\langle \tilde{K}' m_4 \rangle))) = (((\langle 0.325 m_4 \rangle))) = ((13))$. Therefore,

$$((Z_2)) = ((1))((13))((18)) = ((234))$$
$$((x_2)) = ((1343907)) - ((2887))((234)) = ((668349)).$$

Third Iteration:

$$x_2 \leftrightarrow \langle 0, 0, 16, -13, -12, 0 \rangle, \quad k = 4, \quad \alpha_k = 16.$$
$$((Z_3)) = ((\alpha_k))(((\langle \tilde{K}' m_l \rangle / |\beta_l|))) = ((16))((14)) = ((224))$$
$$((x_3)) = ((21661)).$$

Fourth Iteration:

$$x_3 \leftrightarrow \langle 0, 0, 1, -18, -9, 13 \rangle, \quad k = 4, \quad \alpha_k = 1, \quad \alpha_{k-1} < 0.$$
$$((Z_4)) = ((\alpha_k))(((\langle \tilde{K}' m_l \rangle / |\beta_l|))) = ((1))((6)) = ((6))$$
$$((x_4)) = ((4339)).$$

Fifth Iteration:

$$x_4 \leftrightarrow \langle 0, 0, 0, 4, -9, 16 \rangle, \quad k = 3, \quad \alpha_k = 4, \quad \alpha_{k-1} < 0.$$

Since $\alpha_k \alpha_{k-1} < 0$ and $\beta_l \beta_{l-1} > 0$, α_k must be reduced to 3. The quantity $(((\langle 3/2 \rangle))) = ((1))$ is read out from Table II. Hence,

$$((Z_5)) = ((1))$$
$$((x_5)) = ((1452)).$$

Sixth Iteration:

$$x_5 \leftrightarrow \langle 0, 0, 0, 1, 9, 0 \rangle, \quad k = 3.$$

Since $\alpha_k \alpha_{k-1} > 0$ and $\beta_l \beta_{l-1} > 0$, $(((\langle 1/2 \rangle))) = ((0))$ is read out from Table II. Hence,

$$((Z_6)) = ((0)).$$

Since $Z_6 = 0$, but $2x_5 > y$ and $x_5 y > 0$, then $((Z')) = ((1))$. Hence,

$$((Z)) = \sum_{i=1}^{5} ((Z_i)) + ((Z')) = ((122940)) + ((234)) + ((224)) + ((6)) + ((1)) + ((1)) = ((123406)).$$

Table III lists the average and the standard deviation of the number of iterations for finding the quotients of 600 division examples in the preceding residue system. The k and the l are the subscripts of the α_k and the β_l which are the most significant nonzero symmetric mixed-radix coefficients of the dividend and the divisor, respectively. The dividend and the divisor were produced by a method of generating uniformly distributed pseudorandom numbers.

V. CONCLUSION

The preceding work was intended to demonstrate how information processing might be done to speed up residue division. An improved residue division algorithm has been proposed. The algorithm is iterative in nature. It finds the quotient by summing the entries stored in a special memory. To reduce the number of iterations required, it was proposed that each of these entries be an integer determined by multiplying the product of the moduli by a certain coefficient. The number of iterations required for finding the result of residue division was investigated on 600 examples in the symmetric residue system consisting of moduli 33, 35, 37, 41, 43, and 47 (see Table III). Within the limits of these examples, the average number of iterations was reduced by one third compared with the method which had been used (the proposed method requires about 4 iterations, whereas the method previously in use requires 15 iterations on the average [3]).

APPENDIX

CHOICE OF THE VALUE OF K_i (OR K_i')

It will be described here how the K_i (or K_i') should be determined to get the desired quotient.

Let $\epsilon(\geqq 0)$ denote the error generated when K is approximated to $\tilde{K}$, and let R denote the least upper bound of ϵ when (7) is satisfied by Z_i computed by using (4) or (5). Table IV lists a rigid selection of R values in the case of $|\alpha_k| \neq 1$, or $|\alpha_k| = 1$ and $\alpha_k \alpha_{k-1} \geqq 0$. It is necessary, first of all, to calculate the minimum value $R_{\min}$ of the R in Table IV for given moduli. Then, the value ϵ and K_i are determined so that they satisfy the following inequalities:

$$K_{i+1} - K_i \leqq 2\epsilon < 2R_{\min}, \qquad i = 1, 2, \cdots, p - 1$$

TABLE IV

VALUES OF R FOR $|\alpha_k| \neq 1$, OR $|\alpha_k| = 1$ AND $\alpha_k\alpha_{k-1} \geqq 0$

R Values for $0 < \lvert Z_i \rvert < \dfrac{2\lvert x_{i-1}\rvert}{\lvert y\rvert}$	
$\dfrac{6\beta_l m_{l-1} m_l}{(2m_l+\beta_l)\left(2\beta_l m_{l-1} + 2\left[\frac{m_{l-1}}{2}\right]+1\right)} - \dfrac{\beta_l m_{l-1}}{\beta_l m_{l-1} + \left[\frac{m_{l-1}}{2}\right]} - \dfrac{1}{2m_{l+1}}$,	$l = 2, 3, \cdots, N-2; \beta_l = 2, [m_l/2]$
$\dfrac{3\beta_l m_{l-1}}{2\beta_l m_{l-1} + 2\left[\frac{m_{l-1}}{2}\right]+1} - \dfrac{\beta_l m_{l-1}}{\beta_l m_{l-1} + \left[\frac{m_{l-1}}{2}\right]} - \dfrac{1+2\epsilon_1{}^{a}\beta_l}{2m_l}$,	$l = 2, 3, \cdots, N-1; \beta_l = 1, 2, [m_l/2]$

[a] $\epsilon_1 = \begin{cases} 0, & \beta_l = 1 \\ \frac{1}{2}, & \beta_l \neq 1. \end{cases}$

TABLE V

VALUES OF R' FOR $|\alpha_k| = 1$ AND $\alpha_k\alpha_{k-1} < 0$

R' Values for $0 < \lvert Z_i \rvert$
$\dfrac{\beta_l m_{l-1}}{\beta_l m_{l-1} + \left[\frac{m_{l-1}}{2}\right]} - \dfrac{1+2\epsilon_1\beta_l}{2m_l} - \epsilon$, $l = 2, 3, \cdots, N-1; \beta_l = 1, 2, [m_l/2]$
$1 - \dfrac{1+\left[\frac{m_l}{2}\right]}{2m_l}$

TABLE VI

VALUES OF R'' FOR $|\alpha_k| = 1$ AND $\alpha_k\alpha_{k-1} < 0$

R'' Values for $\lvert Z_i \rvert < \dfrac{2\lvert x_{i-1}\rvert}{\lvert y\rvert}$	
$\dfrac{-4\beta_l m_{l-1} m_l}{(2m_l+\beta_l)\left(2\beta_l m_{l-1} - 2\left[\frac{m_{l-1}-1}{2}\right]+1\right)} + \dfrac{\beta_l m_{l-1}}{\beta_l m_{l-1} - \left[\frac{m_{l-1}-1}{2}\right]} + \dfrac{1}{2m_{l+1}} + \epsilon$;	$l = 2, 3, \cdots, N-2; \beta_l = 2, [m_l/2]$
$\dfrac{-2\beta_l m_{l-1}}{2\beta_l m_{l-1} - 2\left[\frac{m_{l-1}-1}{2}\right]+1} + \dfrac{\beta_l m_{l-1}}{\beta_l m_{l-1} - \left[\frac{m_{l-1}-1}{2}\right]} + \dfrac{1+2\epsilon_1\beta_l}{2m_l} + \epsilon$,	$l = 2, 3, \cdots, N-1; \beta_l = 1, 2, [m_l/2]$
$\dfrac{1}{4} + \dfrac{1}{4m_l}$	

$$2/3 - \epsilon \leqq K_1 \leqq 2/3 + \epsilon$$

and

$$2 - \epsilon \leqq K_p \leqq 2 + \epsilon.$$

Next, let $\epsilon'(>0)$ be the correction value of K in the case of $|\alpha_k| = 1$ and $\alpha_k\alpha_{k-1} < 0$, and let R' and R'' be the least upper bound and the greatest lower bound, respectively, of ϵ' when (7) is satisfied by Z_i computed by using (4′) or (5′). Table V and Table VI list rigid selections of R' and R'' values, respectively. Now, it is essential to calculate the minimum value $R_{\min}'$ of the R' in Table V and the maximum value $R_{\max}''$ of the R'' in Table VI, using the ϵ previously obtained. Then, the values ϵ' and K_i' are determined so that

$$R_{\max}'' < \epsilon' < R_{\min}'$$

and

$$K_i' = K_i - \epsilon', \qquad i = 1, 2, \cdots, p.$$

For the example system in Section IV, $R_{min}=0.18663$. If ϵ is chosen as $\epsilon=0.1125$, $R_{min}'=0.54668$, $R_{max}''=0.37059$. Hence ϵ' is chosen, for instance, as $\epsilon'=0.45$.

References

[1] H. L. Garner, "The residue number system," *IRE Trans. Electron. Comput.*, vol. EC-8, pp. 140–147, June 1959.

[2] H. Takahashi and Y. Ishibashi, "A new method for exact calculation by a digital computer," *Inform. Process. Jap.*, vol. 1, pp. 28–42, 1961.

[3] N. S. Szabó and R. I. Tanaka, *Residue Arithmetic and Its Applications to Computer Technology.* New York: McGraw-Hill, 1967.

[4] Y. A. Keir, P. W. Cheney, and M. Tannenbaum, "Division and overflow detection in residue number systems," *IRE Trans. Electron. Comput.*, vol EC-11, pp. 501–507, Aug. 1962.

[5] A. Sasaki, "Addition and subtraction in the residue number system," *IEEE Trans. Electron. Comput.*, vol. EC-16, pp. 157–164, Apr. 1967.

Eisuke Kinoshita was born in Osaka, Japan, in 1932. He received the B.S. degree in mathematics from Hiroshima University, Hiroshima, Japan, in 1960.

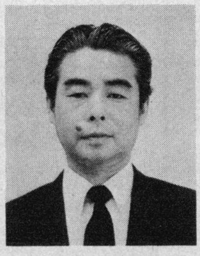
He taught mathematics for two years at a high school in Osaka and since 1962 has been a Research Assistant in the Department of Electronics, University of Osaka Prefecture, Osaka. His current research interests lie in the areas of digital systems and computer arithmetics.

Mr. Kinoshita is a member of the Institute of Electrical Engineers of Japan and the Information Processing Society of Japan.

Hideo Kosako (S'58–M'62) was born in Osaka, Japan, on November 15, 1930. He received the B.E. and M.E. degrees in electrical engineering from the University of Osaka Prefecture, Osaka, Japan, in 1953 and 1957, respectively, and the Ph.D. degree in electrical communication engineering from Osaka University, Osaka, in 1960.

He joined the faculty of Osaka University in 1960. Since 1961 he has been an Associate Professor in the Department of Electronics at the University of Osaka Prefecture. During 1968–1969 he was a Visiting Professor of Electrical Engineering at the University of Arizona, Tucson. His teaching and research interests include hybrid computing systems and simulations.

Dr. Kosako is a member of the Institute of Electronics and Communication Engineers of Japan.



Yoshiaki Kojima (SM'57) was born in Osaka, Japan, on September 29, 1923. He received the B.E. and Ph.D. degrees in electrical engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1946 and 1961, respectively.

From 1946 to 1950 he was with the Sharp Corporation, Japan. In 1950 he joined the staff of the University of Osaka Prefecture, Osaka, and since 1963 he has been a Professor in the Department of Electronics. His present research interests include the areas of logical operation systems.

Dr. Kojima is a member of the Institute of Electronics and Communication Engineers of Japan, the Information Processing Society of Japan, and the Institute of Electrical Engineers of Japan.