Number Restoration in the System of Residual Classes with a Minimum Number of Radices

O. A. FIN'KO

Krasnodar Higher Military Command-Engineering School of Rocket Troops, Russia

(Received May 5, 1997)

An approach is considered to the solution of the problem of consistency of problem-oriented computer arithmetics, in particular, non-positional and positional ones, by acting on the form of data representation. A rather simple algorithm and a device for number restoration are proposed in the two-modulus system of residual classes (SRC) using numbers with given properties as moduli.

Key words: arithmetic, algorithm, residue, radix, number.

The methods of problem-oriented arithmetics are useful in the solution of the problems of cryptology [1], correction of errors of special forms and nature [2], numerical processing signals and images [3], and information conversion [4]. In this sense SRC — the parallel arithmetic based on the Chinese theorem of residues (CTR) — is practised on a large scale [5].

The high complexity of performing non-modulus operations in SRC such as restoration of the positional form of a number, comparison, division, and scaling causes not only difficulties in the use of SRC but substantially decreases the speed and functional capabilities of a non-positional calculator. Under these circumstances, to solve this problem, it is sufficient to solve the problem of the effective number restoration in SRC. It allows other non-modulus operations to be performed with the help of an external positional calculator.

Recently specialists have called attention to SRC with a minimum number of radices based on the numbers of Mersenne \( M_i = 2^i - 1 \) and Fermat \( F_i = 2^i + 1 \) and \( D_i = 2^i \) [3, 6, 7]. Such SRC allows us to simplify substantially the performance of both modulus and non-modulus operations including the operations of number restoration. We consider in this connection the interpretation of the most widespread algorithm of number restoration based on CTR for the case of SRC with two radices (two-modulus SRC). Then we construct the algorithm which is oriented to the number restoration in SRC with a minimum number of radices.
The Chinese theorem of residues. In a two-modulus SRC, an integer non-negative number \( A \) can be represented by its least non-negative residues (from this point, residues) \( x_1 \) and \( x_2 \) in the system of mutually disjoint radices (moduli) \( m_1 \) and \( m_2 \): \( A = \{x_1, x_2\} \), with \( A < P = m_1 m_2 \).

According to CTR [5], the formula of number restoration can be written in the following form:

\[
A = |x_1 m_2 k_1 + x_2 m_1 k_2|_P^+. \tag{1}
\]

Expression (1) shows that the multipliers \( (\times m_1 k_2) \) and \( (\times m_2 k_1) \) can be found from comparison of \( m_2 k_1 \equiv 1 \pmod{m_1} \) and \( m_1 k_2 \equiv 1 \pmod{m_2} \).

If the binary number system is used for the representation of residues \( x_1 \) and \( x_2 \), then it is reasonable to use moduli of the form \( D_i \). Modulo \( M_i \) operations are similar to operations in the two's complement, and modulo \( F_i \) operations are substantially simpler than arbitrary modulo operations [3, 5]. It follows from the analysis of the computational complexity of the number restoration algorithm which uses expression (1) that two multipliers \( (\times m_1 k_2) \) and \( (\times m_2 k_1) \), and a modulo \( P \) adder \( (\sum \mod{P}) \) within the number range of SRC are required for its realization (Fig. 1). The most sophisticated operation is taking a sum to modulo \( P \).

To simplify the operations of taking a sum to modulo \( P \), we can use the properties of residues of the form \( M_i \), \( F_i \), and \( D_i \). Since the factorization of the radix of the form \( D_i \) includes a single simple factor 2, this radix cannot serve as the number range of SRC. Assume that \( m_1 = M_i \) and \( m_2 = F_i \). Then \( P = M_i F_i = M_{2i} \), and the operation of taking a sum by modulo \( M_{2i} \) — the number range of SRC — can be reduced to the summation in the two's complement. This gives very simple solution of the number restoration problem in the two-modulus SRC within the limits of CTR.

**Theorem.** An integer non-negative number \( A < m_1 m_2 \) which is represented in the two-modulus SRC with the help of residues \( x_1 \) and \( x_2 \) by the system of mutually disjoint moduli \( m_1 \) and \( m_2 \) such that \( m_1 < m_2 \), can be uniquely restored by the formula

\[
A = m_1 |\xi| x_1 - x_2 |_{m_2}^+ |_{m_2}^+ + x_1, \tag{2}
\]
where \( \xi = |(m_2 - m_1)^L(m_2)^{-1} |_{m_2}^+ \) (\( L(m_2) \) is the generalized Euler function).

**Proof.** Using the Euclidean algorithm, number \( A \) can be represented in the form

\[ A = m_1 n_1 + x_i \]  

or \( A = (m_2 - b) n_1 + x_i \), where \( b = m_2 - m_1 \).

Since \( A \equiv x_2 \pmod{m_2} \), then \((m_2 - b) n_1 + x_i \equiv x_2 \pmod{m_2} \). Taking into account that \( m_2 n_1 \equiv 0 \pmod{m_2} \), we can obtain \( b n_1 \equiv x_i - x_2 \pmod{m_2} \) or

\[ n_i \equiv b^{-1} (x_i - x_2) \pmod{m_2}. \]  

(4)

According to the Euler formula [8]:

\[ b^{-1} \equiv b^L(m_2)^{-1} \pmod{m_2}. \]  

(5)

Here, \( L(m_2) = [p_1^{\alpha_1-1}(p_1 - 1), ..., p_s^{\alpha_s-1}(p_s - 1)] \), where \( [y_1, ..., y_s] \) is the least common multiple of \( y_1, ..., y_s \); \( m_2 = p_1^{\alpha_1-1}, ..., p_s^{\alpha_s-1} \) is the canonical factorization of \( m_2 \). Substituting (4) into (3) and taking into account (5), we can obtain (2).

The technical realization of formula (2) involves a modulo \( m_2 \) subtractor to calculate difference \( |x_1 - x_2|_{m_2}^+ \), a modulo \( m_2 \) multiplier of the given difference by constant \( \xi \), a positional multiplier by radix \( m_1 \), and a positional adder to sum of \( x_1 \) [9].

Using radices of SRC possessing property \( m_2 - m_1 = 1 \), we can cancel \( \xi \) in (2), and using radices \( D_i \) and \( F_i \), we can obtain

\[ A = D_i |x_1 - x_2|_{F_i}^+ + x_i. \]  

(6)

Residues \( x_1, x_2 \) and the result of restoration of \( A \) are represented in the binary number system:

\[ x_1 = (a_{1}^{(1)}|_{\log_2 m_1}, ..., a_{1}^{(1)}); \]

\[ x_2 = (a_{1}^{(2)}|_{\log_2 m_2}, ..., a_{1}^{(2)}); \]

\[ A = (a_{1}^{(3)}|_{\log_2 p_1}, ..., a_{1}^{(3)}), \]

where \( a_{1}^{(i)} \) are binary digits; \( \lfloor y \rfloor \) denotes rounding \( y \) to the upper integer bound.
The device of number restoration in SRC which is given by mutually disjoint moduli $D_i$ and $F_i$, can be realized with the help of a modulo $F_i$ subtractor (B) (Fig. 2). Since the multiplication of a number given in the binary number system, by $D_i$ can be realized by shifting the number representation by $i$ digits to the side of the top digits, then the multiplication of difference $|x_1 - x_2|^+$, which is obtained at the B output, by radix $D_i$ and following summation of the result of multiplication by $x_1$ can be performed by appropriate partitioning of the higher and lower digits at the device output.

If subtractor B is tabular, then (6) can be strengthened without complicating the device:

$$A = D_i \left| \xi \right| x_1 - x_2 \left| \frac{+}{m} \right|^+ + x_1,$$

(7)

where

$$\xi = \left| (m - D_i)^{L(m)} - 1 \right|^+ m;$$

$m$ is the odd radix of SRC, which is mutually disjoint with $D_i$ and greater than $D_i$.

The B subtractor table can be formed according to the expression

$$\left| \xi \right| x_1 - x_2 \left| \frac{+}{m} \right|^+.$$

**Example.** SRC is given by moduli $D_4$ and $m = 21$. Then $\xi = (21 - 16)^{L(21)} - 1_21^+ = 53_21^+ = 17$.

Assume that residues $x_1 = 13$ and $x_2 = 18$ are given. Then according to (7), we can obtain $A = 16 \left| 17 \right| 13 - 18 \left| 21^+ \right| 13 = 333$. Indeed, $\left| 333 \right|_{16}^+ = 13$, $\left| 333 \right|_{21}^+ = 18$. 

Figure 2. The device of number restoration in the SRC which is given by mutually disjoint moduli $D_i$ and $F_i$. 


Application. The elaborated algorithms and the device of number restoration can be used as parts of specialized calculators functioning in a two-modulus SRC as well as parts of the arithmetic devices functioning in the positional-residual arithmetic [10] and the devices of number restoration in SRC with an arbitrary number of radices [11].

Number $A$ can be described in the positional-residual arithmetic by the polynomial

$$A = \sum_{i=0}^{n-1} (x_1, x_2) \cdot (D_i m)^i$$

where $n$ is the number of representation digits; $(x_1, x_2)$ is the order digit represented in the two-modulus SRC; $D_i m$ is a representation radix. Such a form for the representation of $A$ allows us to improve efficiency in performing non-modulus operators with any given accuracy using low-accurate (in the given case, two-modulus) SRC.

The urgency of using the algorithms based on (6) or (7), in the positional-residue arithmetic is caused by the origination of interdigit carries (up to $n$ carries) which take place in the realization of arithmetic operations (for example, addition).

To restore a number in SRC with an arbitrary number of radices, we can use the principle of recursive doubling and coming to the composite radices. For example, number $A$ can be represented by its residues $x_1, x_2, x_3, x_4$ by pairwise mutually disjoint and ordered radices $m_1, m_2, m_3, m_4$. Then the process of number $A$ restoration includes the two stages:

The first stage

- $x_1$
- $x_2$
- $x_3$
- $x_4$

The second stage

- $x_{11}$
- $x_{12}$
- $A$

where $x_{11} = |A|_{m_1, m_2}^+$ and $x_{12} = |A|_{m_3, m_4}^+$.

At the first stage, according to (2), we have

$$x_{11} = m_1 |\xi_{11} | x_1 - x_2 |_{m_2}^+ m_2 + x_1; \quad x_{12} = m_3 |\xi_{12} | x_3 - x_4 |_{m_4}^+ m_4 + x_3,$$

where $\xi_{11} = |(m_2 - m_1)^L(m_2)^{-1} |_{m_2}^+$; $\xi_{12} = |(m_4 - m_3)^L(m_4)^{-1} |_{m_4}^+$.
At the second stage we obtain \( A = m_1m_2 \mid \xi \mid x_{11} - x_{12} \mid _{m_3m_4}^+ \mid _{m_3m_4}^+ x_{11}, \) where \( \xi = (m_3m_4 - m_1m_2)^{\lfloor (m_3m_4)^{-1} \rfloor} \mid _{m_3m_4}^+ \) Residues \( x_{11} \) and \( x_{12} \) can be obtained using any technique of restoration, for example, according to CTR or by the tabular method.

The algorithm elaborated for number restoration in the two-modulus SRC enables very simple technical solutions to be found which outperform by a factor of two in terms of temporal and instrument characteristics the devices realizing the algorithm of number restoration in SRC based on CTR in its most profitable interpretation. The use of the SRC radix system with given properties can serve as the confirmation of a more general approach to the consistency of problem-oriented machine arithmetics which is based on the synthesis of data forms oriented to the solution of the consistency problem [4].

REFERENCES