RESIDUE ARITHMETIC WITH RATIONAL OPERANDS

R. T. Gregory
Department of Computer Science
The University of Tennessee
Knoxville, TN 37916

ABSTRACT

A method is described for doing residue arithmetic when the operands are rational numbers. A rational operand \( a/b \) is mapped onto the integer \( [a - b^{-1}]/p \) and the arithmetic is performed in GF(p). A method is given for taking an integer result and finding its rational equivalent (the one which corresponds to the correct rational result).

Let \( I_p = \{0, 1, 2, \ldots, p-1\} \) be the set consisting of the least positive residues modulo \( p \), where \( p \) is an odd prime. If \( I \) represents the set of integers, the mapping \( I_p : I \rightarrow I_p \), defined by \( [a]/p = r \) if and only if \( a \equiv r \pmod{p} \) and \( 0 \leq r < p \), establishes the \( p \) disjoint residue classes modulo \( p \) \( R_0, R_1, \ldots, R_{p-1} \). We can generalize the concept by forming generalized residue classes \( Q_0, Q_1, \ldots, Q_{p-1} \), where \( Q_i \) is the set of rational numbers of the form \( a/b \) which are mapped onto \( i \in I_p \) by the mapping \( [a/b]/p = [a - b^{-1}]/p \), where \( b^{-1} \) is the multiplicative inverse of \( b \) modulo \( p \). Obviously, \( R_i \subseteq Q_i \) for \( i = 0, 1, \ldots, p-1 \).

Since not every rational number \( a/b \) is such that \( b^{-1} \) exists, we define

\[
\hat{Q} = \bigcup_{i=0}^{p-1} Q_i
\]

(1)

to be the set of all rational numbers mapped onto \( I_p \) by the mapping \( I_p \). It is proved in (2) that \((\hat{Q}, +, \cdot)\) is a commutative ring with identity and that

(2) \( I_p : \hat{Q} \rightarrow I_p \)

is a homomorphism with respect to addition and multiplication. In other words, \( I_p \) is a homomorphic image of \( \hat{Q} \) and so arithmetic operations in the ring \((\hat{Q}, +, \cdot)\) are equivalent to the corresponding arithmetic operations in the finite field \((I_p, +, \cdot)\).

The mapping (2) is onto but it is not one-to-one since each \( i \in I_p \) is the image of an infinite set of rational numbers \( Q_i \). Hence, the mapping does not have an inverse. It turns out that if \( N \) is the largest integer satisfying

(3) \( N \leq [((p-1)/2)]^2 \),

then there is at most one element of the set

(4) \( F_N = \{ a/b : 0 \leq |a| \leq N, 0 < b \leq N \} \)

in any given \( Q_i \). These order-\( N \) Farey fractions, \( F_N \), enable us to establish a one-to-one and onto mapping with their images \( \hat{I}_p \subset I_p \).

5. Example Let \( p = 19 \) and \( I_{19} = \{0, 1, 2, \ldots, 18\} \). Then \( N = 3 \) and the mapping \( I_{19} : F_3 \rightarrow \hat{I}_{19} \) is exhibited in the following "symmetric" array.

\[
\begin{array}{cccccccccc}
0 & 1 & 2 & 3 & -3/2 & -1/2 & 2/3 & -1/3 & 1/3 & -2/3 \\
0 & 1 & 2 & 3 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18
\end{array}
\]

Notice that 4, 5, 14, and 15 are not elements of \( \hat{I}_{19} \).

6. Example Consider the computation

\[
x = 1/3 - 2/3 = 1/3 + (-2/3).
\]

If \( p = 19 \), then \( N = 3 \), and we can use the mapping in Example 5 to write

\[
|x|_{19} = |1/3 + (-2/3)|_{19} = |13 + 12|_{19} = 6.
\]

Since 6 \( \in \hat{I}_{19} \), we use the inverse mapping in Example 5 to obtain \( x = -1/3 \).

If the result of an arithmetic operation is an integer in \( I_p \) which is not also in \( \hat{I}_p \), we have pseudo-overflow*. This implies that the rational number corresponding to the integer result is not an order-\( N \) Farey fraction. In other words either the numerator or the denominator (or both) have become larger than \( N \) in absolute value. Pseudo-overflow causes us no difficulty if it occurs during an

*This term was suggested by T. M. Rao.
intermediate calculation as long as the final answer is an element of $F_N$.

7. Example Consider the computation

$$x = \frac{1}{2} - \frac{2}{3} - \frac{1}{6} = \frac{1}{2} + (-\frac{2}{3}) + (-\frac{1}{6}).$$

Notice that the sum of the first two rational numbers is not in $F_3$ and $-1/6$ is not in $F_3$. However, the final result is in $F_3$ and so pseudo-overflow presents no problem. Thus,

$$|x|_{19} = |10 + 12 + 3|_{19} = 6,$$

which implies $x = -1/3$.

The following theorem gives us an algorithm for carrying out the mapping $\mathbb{I}_p \rightarrow F_N$ if either the denominator in $a/b$ or a multiple of the denominator can be found.

8. Theorem Suppose we map $x = a/b$ from $F_N$ onto the integer $|ab^{-1}|_p$ in $\mathbb{I}_p$. We obtain the inverse mapping as follows: If $kb$ can be found, with the integer $k$ satisfying $0 < k \leq N$, then

$$ka = \lfloor kb|x|_p/p \rfloor,$$

where $\lfloor \cdot \rfloor$ gives us the symmetric residue modulo $p$, and we have

$$a/b = ka/kb.$$

Proof See [3].

With this algorithm we have no need for storing the table exhibited in Example 5. Obviously, if $p$ is extremely large (that is, large enough so that $N$ is very large), then a practical number system for error-free computation can be established using the order-$N$ Farey fractions along with the finite field $(\mathbb{I}_p, +, \cdot)$. For example $2^{61} - 1$ is a Mersenne prime and, if we choose $p = 2^{61} - 1$, then $N = 2^{20} - 1$. For a computer with a word length of 32 bits, $p$ requires two words but $N$ fits into a single word very nicely.

For a related discussion see [4].

References


