Exact and Robust Reconstruction of Integer Vectors Based on Multidimensional Chinese Remainder Theorem (MD-CRT)

Li Xiao, Xiang-Gen Xia, Fellow, IEEE, and Yu-Ping Wang, Senior Member, IEEE

Abstract—The robust Chinese remainder theorem (CRT) has been recently proposed for robustly reconstructing a large nonnegative integer from erroneous remainders. It has found applications in signal processing, including phase unwrapping and frequency estimation under sub-Nyquist sampling. Motivated by the applications in multidimensional (MD) signal processing, in this paper we propose the MD-CRT and robust MD-CRT for integer vectors. We derive the MD-CRT for integer vectors with respect to a general set of moduli, which allows to uniquely reconstruct an integer vector from its remainders, if it is in the fundamental parallelepiped of the lattice generated by a least common right multiple of all the moduli. For some special forms of moduli, we present explicit reconstruction formulae. We derive the robust MD-CRT for integer vectors when the remaining integer matrices of all the moduli left divided by their greatest common left divisor (gcd) are pairwise commutative and coprime. Two different reconstruction algorithms are proposed, and accordingly, two different conditions on the remainder error bound for the reconstruction robustness are obtained, which are related to a quarter of the minimum distance of the lattice generated by the gcd of all the moduli or the Smith normal form of the gcd.

Index Terms—Chinese remainder theorem (CRT), integer matrices, lattices, multidimensional (MD) frequency estimation, robust CRT, robust MD-CRT.

I. INTRODUCTION

The Chinese remainder theorem (CRT) is one of the most fundamental theorems in number theory, and has a long history going back to the early 1200’s [11]–[13]. Basically speaking, the CRT allows to uniquely reconstruct a large nonnegative integer from its remainders with respect to a set of small moduli, if the large integer is less than the least common multiple (lcm) of all the moduli. To date, there has been a surge in work on applying the CRT for partitioning a large task into a number of smaller but independent subtasks, which can be performed in parallel. For example, the CRT has been intensively utilized in the signal processing community in the context of cyclic convolution [4], [5], fast Fourier transform [6], [7], coprime sensor arrays [8]–[11], to name a few. It also finds applications in various other fields, such as computer arithmetic based on modulo operations (e.g., multiplication of very large numbers), coding theory (e.g., residue number system codes), and cryptography (e.g., secret sharing); see [11]–[13] and references therein.

Motivated by the applications of the CRT in phase unwrapping and frequency estimation under sub-Nyquist sampling, a robust remaindering problem has been raised and investigated in [12]–[19]. In these applications, signals are usually subject to noise, and thereby the detected remainders may be erroneous. Two significant questions underlying the robust remaindering problem are: 1) what is the reconstruction range of the large nonnegative integer? and 2) how large can the remainder errors be to ensure the robust reconstruction? It is well-known that the CRT is not robust against remainder errors, i.e., a small error in a remainder may result in a large error in the reconstruction solution. Directly applying the CRT to these applications will therefore yield poor performance. Recently, the robust CRT has been proposed in [12]–[14] and further systematically studied in [20]–[24], to solve the robust remaindering problem. The robust CRT claims that even though every remainder has a small error, a large nonnegative integer can be robustly reconstructed in the sense that the reconstruction error is upper bounded by the bound of the remainder errors. Beyond these applications aforementioned, the robust CRT has offered useful applications in multi-wavelength optical measurement [25]–[27], distance or velocity ambiguity resolution [28]–[31], fault-tolerant wireless sensor networks [32]–[34], error-control neural coding [35]–[37], etc. It is worth pointing out that the (robust) CRT has been generalized to (robustly) reconstruct multiple large nonnegative integers from their unordered remainder sets as well [38]–[44]. A thorough review of the robust CRT can be found in [45].

In this paper, we extend the CRT and robust CRT for integers to the multidimensional (MD) case, called the MD-CRT and robust MD-CRT for integer vectors, so that they can be utilized in MD signal processing. Note that MD signal processing here refers to true (nonseparable) MD signal processing, since separable MD signal processing is straightforward by handling their 1-dimensional counterparts separately along each dimension. First, we derive the MD-CRT for integer vectors with respect to a general set of moduli (namely a set of arbitrary nonsingular integer matrices). It is basically that given a set of nonsingular moduli \( \{ M_i \}_{i=1}^L \), an integer vector \( \mathbf{m} \in \mathcal{N}(\mathbf{R}) \) can be uniquely reconstructed from its remainders \( r_i \) for \( 1 \leq i \leq L \), where \( \mathbf{R} \) is a least common right multiple of all the moduli, and \( \mathcal{N}(\mathbf{R}) \) denotes the set of all integer vectors in the fundamental parallelepiped of the lattice generated by \( \mathbf{R} \). A reconstruction algorithm is proposed as well; see, for details, the proof of Theorem 1 in Section III. Notably, the MD-CRT for integer vectors was first presented in [46], [47] for a special case where the \( L \) moduli are given by \( M_i = U A_i U^{-1} \) for \( 1 \leq i \leq L \) with \( U \) being a unimodular matrix and \( A_i \)’s coprime diagonal...
integer matrices. For some other special forms of moduli, we further obtain explicit reconstruction formulae of the MD-CRT for integer vectors in this paper.

Moreover, we derive the robust MD-CRT for integer vectors when the $L$ nonsingular moduli are in the form of $M_i = M_i^\Gamma_i$ for $1 \leq i \leq L$, where $M$ is an arbitrary integer matrix, and $\Gamma_i$’s are pairwise commutative and coprime integer matrices. As in the robust CRT for integers in $[12] - [14], [20] - [24]$, we attempt to accurately determine all the folding vectors $n_i$’s (i.e., the quotient vectors of $m$ left divided by the moduli), and a robust reconstruction of $m$ can be calculated as the reconstruction obtained from anyone folding vector, i.e., $\tilde{m} = m_{\Gamma_i} + n_i$, for any $1 \leq i \leq L$, where $n_i$ denotes the $i$th erroneous remainder. We observe that the size of the remainder error bound for the reconstruction robustness is dependent upon the reconstruction algorithm. In other words, different reconstruction algorithms will lead to different conditions on the remainder error bound. We then propose two different reconstruction algorithms, and accordingly, obtain two different conditions on the remainder error bound for the reconstruction robustness, which are related to a quarter of the minimum distance of the lattice generated by $M$ or the Smith normal form of $M$.

The rest of this paper is organized as follows. In Section $\text{III}$ we recall some background knowledge needed to make this paper more self-contained. In Section $\text{III}$ we derive the MD-CRT for integer vectors with respect to a general set of moduli, and provide explicit reconstruction formulae when the moduli are in some special forms. In Section $\text{IV}$ we investigate the robust MD-CRT for integer vectors, and propose two different algorithms for robust reconstruction, resulting in two different conditions on the remainder error bound for the reconstruction robustness. We conclude this paper in Section $\text{V}$.

**Notations:** Capital and lowercase boldfaced letters are used to denote matrices and vectors, respectively. Let $\mathbb{R}$ and $\mathbb{Z}$ denote the sets of reals and integers, respectively. We use $\mathbb{R}^D (\mathbb{Z}^D)$ and $\mathbb{R}^{D \times K} (\mathbb{Z}^{D \times K})$ to denote the sets of $D$-dimensional real (integer) vectors and $D \times K$ real (integer) matrices, respectively. For a matrix $A$, its transpose, inverse, inverse transpose, and determinant are denoted as $A^T$, $A^{-1}$, $A^{-T}$, and $\det(A)$, respectively. The $(i, j)$th element of a matrix $A$ is denoted by $A(i, j)$, and the $i$th element of a vector $a$ is denoted by $a(i)$. Given a set of scalars $a_1, a_2, \cdots, a_D$, we denote by $\text{diag}(a_1, a_2, \ldots, a_D)$ the diagonal matrix with $a_i$ being the $i$th diagonal element. A $D$-dimensional vector $a \in [c, d]^D$ means that the elements of $a$ are in the range $c \leq a(i) < d$ for $1 \leq i \leq D$ and $c, d \in \mathbb{R}$. The symbols $\mathbf{I}$ and $\mathbf{0}$ denote the identity matrix and the all-zero vector/matrix, respectively, with size determined from context. The relative complement of a set $\mathcal{A}$ with respect to a set $\mathcal{B}$ is written as $\mathcal{B}\setminus\mathcal{A}$.

**II. Preliminaries**

The preliminary knowledge involved in this paper is mainly related to some fundamental properties in elementary number theory. In the following, let us first recall the general concepts and notations for integer vectors and matrices $[43] - [51]$ that will be used in the subsequent analysis. Throughout this paper, all matrices are square matrices unless otherwise stated.

i) **Unimodular matrix:** A matrix $U$ is unimodular if it is an integer matrix and $|\det(U)| = 1$. For any unimodular matrix $U$, its inverse $U^{-1}$ is also unimodular because of $U^{-1} = \text{adj}(U)/\det(U)$ and $|\det(U^{-1})| = |\det(U)| = 1$, where $\text{adj}(U)$ stands for the adjugate of $U$ and is an integer matrix.

ii) **Divisor:** An integer matrix $A$ is a left divisor of an integer matrix $M$ if $A^{-1}M$ is an integer matrix. Similarly, an integer matrix $A$ is a right divisor of $M$ if $MA^{-1}$ is an integer matrix.

iii) **Greatest common divisor (gcd):** An integer matrix $A$ is a common left divisor (cdl) of $L (L \geq 2)$ integer matrices $M_1, M_2, \cdots, M_L$, if $A^{-1}M_i$ is an integer matrix for each $1 \leq i \leq L$. Note that $U^{-1}A^{-1}M_i$ is still an integer matrix for any unimodular matrix $U$, and thus $AU$ is also a cdl of $M_1, M_2, \cdots, M_L$. In particular, any unimodular matrix is a cdl. We call $B$ a greatest common left divisor (gcd) of $M_1, M_2, \cdots, M_L$, if any other cdl is a left divisor of $B$. Note that among all cdl’s, a gcd has the greatest absolute determinant and is unique up to postmultiplication by a unimodular matrix (because if $B$ is a gcd, so will be $BU$ for any unimodular matrix $U$). Similarly, a common right divisor (crd) and a greatest common right divisor (gcrd) of $M_1, M_2, \cdots, M_L$ can be defined, respectively.

iv) **Multiple:** A nonsingular integer matrix $A$ is a left multiple of an integer matrix $M$ if $A = PM$ for some integer matrix $P$. Similarly, a nonsingular integer matrix $A$ is a right multiple of $M$ if $A = MQ$ for some integer matrix $Q$.

v) **Least common multiple (lcm):** A nonsingular integer matrix $A$ is a common left multiple (clm) of $L (L \geq 2)$ integer matrices $M_1, M_2, \cdots, M_L$, if $A = PM$ for some integer matrix $P$, and each $1 \leq i \leq L$. We call $C$ a least common left multiple (lclm) of $M_1, M_2, \cdots, M_L$, if any other clm is a left multiple of $C$. Note that among all clm’s, an lclm has the smallest absolute determinant and is unique up to premultiplication by a unimodular matrix (because if $C$ is an lcm, so will be $UC$ for any unimodular matrix $U$). Similarly, a common right multiple (crm) and a least common right multiple (lcrm) of $M_1, M_2, \cdots, M_L$ can be defined, respectively.

vi) **Coprime:** Two integer matrices $M$ and $N$ are said to be left (right) coprime if their gcd (gcrd) is unimodular. In other words, $M$ and $N$ are left (right) coprime if they have no clms (crds) other than unimodular matrices.

vii) **The $N(M)$ notation:** Let $M$ be a $D \times D$ nonsingular integer matrix. The notation $N(M)$ is defined by $N(M) = \{k | k = Mx, x \in [0, 1]^D\}$, and $k \in \mathbb{Z}^D$. The number of elements in $N(M)$ equals $|\det(M)|$. In the 1-dimensional case (i.e., when $D = 1$), we have $N(M) = \{0, 1, \cdots, M - 1\}$.

The division theorem for integer vectors: A $D$-dimensional integer vector $m$ has a unique representation with respect to a $D \times D$ nonsingular integer matrix $M$ as $m = Mn + r$, or equivalently

$$m = r \mod M,$$

(1)

where $M$ is viewed as a modular, and integer vectors $n$ and $r \in N(M)$ are the folding vector and remainder of $m$ with respect to the modular $M$, respectively. For simplicity, we write $r$ in (1) as

$$r = \langle m \rangle_M.$$

(2)

Note that both divisors and multiples are always taken to be nonsingular integer matrices. We next introduce some needful
properties of integer matrices as follows.

**Proposition 1** ([49]): The remainder \( \langle \mathbf{m} \rangle_M \) of \( \mathbf{m} \) modulo \( \mathbf{M} \) as in (1) can be computed as

\[
\langle \mathbf{m} \rangle_M = \mathbf{m} - M[\mathbf{M}^{-1}\mathbf{m}],
\]

i.e., the folding vector \( \mathbf{n} \) is calculated as \( \mathbf{n} = [\mathbf{M}^{-1}\mathbf{m}] \), where the notation \([ \cdot ]\) denotes the floor operation that is performed on every element of the vector. Since \( \mathbf{M}^{-1} \) is in general a matrix with rational elements, it is subject to round-off errors due to the finite precision of computers. The term \( [\mathbf{M}^{-1}\mathbf{m}] \) is sensitive to these errors, particularly when the elements of \( \mathbf{m} \) are large. Hence, (3) is not appropriate for computing \( \langle \mathbf{m} \rangle_M \) in practice, and an alternative is given by

\[
\langle \mathbf{m} \rangle_M = \mathbf{M} (\text{adj}(\mathbf{M})\mathbf{m} \mod \det(\mathbf{M})) / \det(\mathbf{M}),
\]

where the modulo operation is performed on every element of \( \text{adj}(\mathbf{M})\mathbf{m} \). Clearly, expression (3) is not subject to such round-off errors, since all arithmetics are performed on integers.

It is readily seen that when the involved matrices in MD signal processing are diagonal, most results in the 1-dimensional case can be straightforwardly extended to the MD case by handling their 1-dimensional counterparts separately along each dimension. As a simple example, when \( \mathbf{M} \) in (1) is diagonal, i.e., \( \mathbf{M} = \text{diag}(M_1, M_2, \ldots, M_D) \), then (1) is equivalent to

\[
m(i) \equiv r(i) \mod M_i \text{ for } 1 \leq i \leq D,
\]

where \( m(i) \) and \( r(i) \) denote the \( i \)-th elements of integer vectors \( \mathbf{m} \) and \( \mathbf{r} \), respectively. The division theorem for integer vectors is therefore reduced to that for integers. However, the involved matrices are often nondiagonal, and then extending 1-dimensional signal processing results to the MD case becomes nontrivial and requires more complex matrix operations. The Smith normal form introduced below is well known as a popular tool to diagonalize an integer matrix, and has been widely used to simplify several MD signal processing problems; see, for example, ([52], [53]).

**Proposition 2** (The Smith normal form ([49])): A \( D \times K \) integer matrix \( \mathbf{M} \) can be decomposed as

\[
\mathbf{UMV} = \begin{cases} 
\begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} & \text{if } K > D, \\
\Lambda & \text{if } K = D, \\
\Lambda & 0 \end{cases}
\text{ if } K < D,
\]

where \( \mathbf{U} \) and \( \mathbf{V} \) are \( D \times D \) and \( K \times K \) unimodular matrices, respectively, and \( \Lambda \) is a \( \min(K,D) \times \min(K,D) \) diagonal integer matrix, i.e., \( \Lambda = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_\gamma, 0, \ldots, 0) \) with \( \lambda_i \)'s being positive integers and \( \gamma \) being the rank of \( \mathbf{M} \). Also, \( \lambda_i \)'s satisfy \( \lambda_i|\lambda_{i+1} \), i.e., \( \lambda_i \) divides \( \lambda_{i+1} \), for each \( 1 \leq i \leq \gamma - 1 \). Under the conditions, \( \Lambda \) is unique for a given matrix \( \mathbf{M} \), while \( \mathbf{U} \) and \( \mathbf{V} \) are generally not. Moreover, \( \lambda_i \)'s are called the invariant factors and can be computed as

\[
\lambda_i = \frac{d_i}{d_{i-1}} \text{ for } 1 \leq i \leq \gamma,
\]

where \( d_i \) (called the \( i \)-th determinantal divisor) is the gcd of all \( i \times i \) determinantal minors of \( \mathbf{M} \) and \( d_0 = 1 \).

We can conveniently calculate the Smith normal form of an integer matrix using the codex. For example, we have

\[
\Lambda = \begin{pmatrix} 2 & 0 & 0 \\
0 & 6 & 0 \\
0 & 0 & 12 \end{pmatrix},
\]

\[
= \begin{pmatrix} 0 & 0 & 1 \\
0 & 1 & -3 \\
1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4 & 4 \\
-6 & 6 & 12 \\
10 & -4 & -16 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 \\
2 & 1 & -2 \\
0 & 1 & 3 \end{pmatrix}.
\]

Let us recall the division theorem with a nondiagonal matrix \( \mathbf{M} \in \mathbb{Z}^{D \times D} \) in (1). According to the Smith normal form of \( \mathbf{M} \) in (4), we can equivalently express (1) as a diagonal version:

\[
\mathbf{Um} \equiv \mathbf{Ur} \mod \Lambda.
\]

Thus, the Smith normal form in Proposition 2 provides a direct way to characterize nondiagonal matrices much closer to the separable case.

**Proposition 3** (The Bezout’s theorem ([50])): Let \( \mathbf{L} \) be a gcd of integer matrices \( \mathbf{M} \) and \( \mathbf{N} \). Then, there exist integer matrices \( \mathbf{P} \) and \( \mathbf{Q} \) such that

\[
\mathbf{MP} + \mathbf{QN} = \mathbf{L}.
\]

Similarly, let \( \mathbf{L} \) be a gcd of \( \mathbf{M} \) and \( \mathbf{N} \). Then, there exist integer matrices \( \mathbf{P} \) and \( \mathbf{Q} \) such that

\[
\mathbf{PM} + \mathbf{QN} = \mathbf{L}.
\]

On the basis of the Smith normal form in Proposition 2, we next introduce how to calculate a gcd \( \mathbf{L} \) of two given nonsingular \( D \times D \) integer matrices \( \mathbf{M} \) and \( \mathbf{N} \), and the accompanying integer matrices \( \mathbf{P} \) and \( \mathbf{Q} \) in the Bezout’s theorem (for details see ([50]). Define

\[
\mathbf{S} = \begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix},
\]

which is a \( D \times 2D \) integer matrix of rank \( D \). From Proposition 2 the Smith normal form of \( \mathbf{S} \) is

\[
\mathbf{U} \begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} \mathbf{V} = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix},
\]

where \( \mathbf{U} \) and \( \mathbf{V} \) are both unimodular matrices of sizes \( D \times D \) and \( 2D \times 2D \), respectively, and \( \Lambda \) is a \( D \times D \) diagonal integer matrix. Since \( \mathbf{U}^{-1} \) is also unimodular, we can write (12) as

\[
\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} \mathbf{V} = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix},
\]

\[
\text{where } \mathbf{L} = \mathbf{U}^{-1} \Lambda \text{ is a } D \times D \text{ integer matrix. Partitioning the } 2D \times 2D \text{ unimodular matrix } \mathbf{V} \text{ into } D \times D \text{ blocks, we have}
\]

\[
\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} \begin{pmatrix} \mathbf{V}_{11} & \mathbf{V}_{12} \\ \mathbf{V}_{21} & \mathbf{V}_{22} \end{pmatrix} = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix}.
\]

This implies

\[
\mathbf{MV}_{11} + \mathbf{NV}_{21} = \mathbf{L}.
\]

By rewriting (13) as

\[
\begin{pmatrix} \mathbf{M} & \mathbf{N} \end{pmatrix} = \begin{pmatrix} \mathbf{L} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{K}_{11} & \mathbf{K}_{12} \\ \mathbf{K}_{21} & \mathbf{K}_{22} \end{pmatrix}.
\]

\[1\text{http://www.numbertheory.org/php/smith.html}
we see that
\[ M = LK_{11}, \quad N = LK_{12}, \] (17)
where \( K_{ij} \) for \( 1 \leq i, j \leq 2 \) are all integer matrices due to the unimodularity of \( V \). Therefore, \( L \) is a gcd of \( M \) and \( N \). Then, we demonstrate that \( L \) is actually a gcd of \( M \) and \( N \). For any other gcd \( T \) of \( M \) and \( N \), i.e., \( M = TA \) and \( N = TB \) for some integer matrices \( A \) and \( B \), we have, from (15).

\[ T(AV_{11} + BV_{21}) = L, \] (18)
which means that \( T \) is a left divisor of \( L \). Hence, \( L \) is a gcd of \( M \) and \( N \), and is given by
\[ L = U^{-1}A. \] (19)
From (15), the integer matrices \( P \) and \( Q \) in (9) are given by
\[ P = V_{11}, \quad Q = V_{21}. \] (20)

In particular, when \( M \) and \( N \) are left coprime, their gcd \( L \) must be a unimodular matrix. Since \( L^{-1} \) is unimodular as well, we further right-multiply \( L^{-1} \) on both sides of (15), and get
\[ MV_{11}L^{-1} + NV_{21}L^{-1} = I. \] (21)

This equation is called the Bezout’s identity. In this case, we can regard \( I \) as a gcd of \( M \) and \( N \), and then the integer matrices \( P \) and \( Q \) in (9) in the Bezout’s identity are calculated as
\[ P = V_{11}L^{-1} = V_{11}A^{-1}U, \quad Q = V_{21}L^{-1} = V_{21}A^{-1}U. \] (22)

Similarly, following the above procedure, we can calculate a gcd \( L \) of \( M \) and \( N \), and the accompanying integer matrices \( P \) and \( Q \) in (10).

**Proposition 4 (18):** Let \( M \) and \( N \) be two nonsingular integer matrices. When \( MN = NM \), the following four statements are equivalent:
1) \( M \) and \( N \) are right coprime.
2) \( M \) and \( N \) are left coprime.
3) \( MN \) is an lcrm of \( M \) and \( N \).
4) \( MN \) is an lclm of \( M \) and \( N \).

**Remark 1:** As stated in Proposition 4 when \( M \) and \( N \) are commutative, i.e., \( MN = NM \), their left coprimeness and right coprimeness can imply each other, so we use the simpler term “coprimeness.” Similarly, when \( M \) and \( N \) are commutative and coprime, their product \( MN \) is both an lcrm and an lclm, so we use the simpler term “lcm.” Besides, for the 1-dimensional case, Propositions 3 and 4, respectively, reduce to “Let \( L \) be the gcd of integers \( M \) and \( N \). Then, there exist integers \( P \) and \( Q \) such that \( MP + NQ = L \)” and “Given two non-zero integers \( M \) and \( N \), \( MN \) is the lcm of \( M \) and \( N \) if and only if \( M \) and \( N \) are coprime,” which are well-known facts.

Given a \( D \times D \) nonsingular matrix \( M \) (which is not necessarily an integer matrix), the set of all integer linear combinations of the linearly independent columns of \( M \), i.e.,
\[ \text{LAT}(M) = \{ Mn | n \text{ is an integer vector} \}, \] (23)
is called the \( D \)-dimensional lattice generated by \( M \), denoted as \( \text{LAT}(M) \). The fundamental parallelepiped of \( \text{LAT}(M) \) is defined as the region:
\[ \mathcal{F}_{\text{LAT}(M)} = \{ Mx | x \in [0, 1)^D \}. \] (24)
The shape of \( \mathcal{F}_{\text{LAT}(M)} \) defined above depends on the generating matrix \( M \). All lattice cells of \( \text{LAT}(M) \) have the same volume equal to \( \lvert \det(M) \rvert \). One can observe that \( \mathcal{F}_{\text{LAT}(M)} \) and its shifted copies (i.e., the other lattice cells) form a partition of the whole real vector space \( \mathbb{R}^D \). When \( M \) is a nonsingular integer matrix, we obtain \( N(M) \subset \mathcal{F}_{\text{LAT}(M)} \), since \( \mathcal{F}_{\text{LAT}(M)} \) is the set of all real vectors of the form \( Mx \) with \( x \in [0, 1)^D \), while \( N(M) \) is only the set of all integer vectors of the form \( Mx \) with \( x \in [0, 1)^D \).

In other words, we have
\[ N(M) = \mathcal{F}_{\text{LAT}(M)} \cap \mathbb{Z}^D. \] (25)

Moreover, we state two important propositions about lattices, which we will use later, as follows.

**Proposition 5 (57):** Two nonsingular integer matrices \( M \) and \( N \) generate the same lattice, i.e., \( \text{LAT}(M) = \text{LAT}(N) \), if and only if \( M = NP \), where \( P \) is a unimodular matrix.

**Proposition 6 (57):** Given two nonsingular integer matrices \( M \) and \( N \), let \( C \) be an lcrm of \( M \) and \( N \). Then,
\[ \text{LAT}(M) \cap \text{LAT}(N) = \text{LAT}(C). \] (26)

### III. MD-CRT for integer vectors

The well-known CRT for integers allows the reconstruction of a nonnegative integer from its remainders with respect to a general set of moduli, and it has been successfully applied in 1-dimensional signal processing, cryptography, coding theory, parallel arithmetic computing, etc.; see [1]–[3] and references therein. In this section, as a natural extension of the CRT for integers, we investigate the MD-CRT for integer vectors, which provides a reconstruction algorithm for an integer vector from its remainders and possesses potential usefulness in MD signal systems. Before presenting the MD-CRT for integer vectors, let us first briefly revisit the CRT for integers as follows.

**Proposition 7 (CRT for integers [16]):** Given \( L \) moduli \( M_i \) for \( 1 \leq i \leq L \), which are arbitrary positive integers, let \( R \) be their lcm. For an integer \( m \in \mathbb{N}(R) \) (i.e., \( 0 \leq m < R \)), we can uniquely reconstruct \( m \) from its remainders \( r_i = \langle m \rangle_{M_i} \) as
\[ m = \left\{ \sum_{i=1}^{L} W_i \hat{W}_i r_i \right\}_R, \] (27)
where \( W_i = R / N_i \), \( \hat{W}_i \) is the modular multiplicative inverse of \( W_i \) modulo \( N_i \), i.e., \( W_i \hat{W}_i \equiv 1 \mod N_i \) (or equivalently, \( \hat{W}_i \) is some integer satisfying
\[ W_i \hat{W}_i + N_i Q_i = 1 \] (28)
for some integer \( Q_i \), if \( N_i \neq 1 \), else \( \hat{W}_i = 0 \), and \( N_1, N_2, \ldots, N_L \) are taken to be any \( L \) pairwise coprime positive integers such that \( R = N_1 N_2 \cdots N_L \) and \( N_i \) divides \( M_i \) for each \( 1 \leq i \leq L \). It is worth noting that when the moduli \( M_1, M_2, \ldots, M_L \) are pairwise coprime, we can take \( N_i = M_i \) for \( 1 \leq i \leq L \), and then Proposition 7 reduces to the CC CRT for integers with respect to pairwise coprime moduli.

We next extend the CRT for integers for the integer vector reconstruction problem. We call it the MD-CRT for integer vectors. The non-commutativity of matrix multiplication prevents many results for integers from being apparently established for integer vectors and matrices. For this reason, it is necessary for us to explicitly derive the MD-CRT for integer vectors in this...
paper. Before presenting the main results, we give the following lemma, which will be used in the sequel.

**Lemma 1:** Given integer matrices $M_1, M_2, \ldots, M_L$, we have the following results.

1) Let $B$ be an lcrm of $M_1, M_2, \ldots, M_{L-1}$, and $R$ be an lcrm of $B$ and $M_L$. Then, $R$ is an lcrm of $M_1, M_2, \ldots, M_L$.

2) Let $B$ be an lcrm of $M_1, M_2, \ldots, M_{L-1}$, and $R$ be an lcrm of $B$ and $M_L$. Then, $R$ is an lcrm of $M_1, M_2, \ldots, M_L$.

**Proof:** It is obvious that $R$ is a crn of $M_1, M_2, \ldots, M_L$. Then, for any other crn $C$ of $M_1, M_2, \ldots, M_L$, we have $C = M_iQ$ for some integer matrix $Q$. Moreover, since $C$ is a crn of $M_1, M_2, \ldots, M_{L-1}$, and $B$ is an lcrm of $M_1, M_2, \ldots, M_{L-1}$, we know that $C$ is a right multiple of $B$, i.e., $C = BP$ for some integer matrix $P$. Thus, $C$ is a crn of $B$ and $M_L$. Since $R$ is an lcrm of $B$ and $M_L$, we know that $C$ is a right multiple of $R$, i.e., $C = RA$ for some integer matrix $A$. Therefore, $R$ is an lcrm of $M_1, M_2, \ldots, M_L$. The result in 2) can be similarly proved and its proof is omitted here.

We then have the following result.

**Theorem 1** (MD-CRT for integer vectors): Given $L$ moduli $M_i$ for $1 \leq i \leq L$, which are arbitrary nonsingular integer matrices, let $R$ be anyone of their lcrms. For an integer vector $m \in \mathbb{N}(R_i)$, we can uniquely reconstruct $m$ from its remainders $r_i = \langle m \rangle_{M_i}$.

**Proof:** Let $G_1$ and $R_1$ be a gcd and an lcrm of $M_1$ and $M_2$, respectively. Based on the Bezout’s theorem in Proposition 3, we have

$$M_1P_1 + M_2P_2 = G_1$$

for some integer matrices $P_1$ and $P_2$. Right-multiplying $G_1^{-1}$ on both sides of (29), we get

$$M_1P_1G_1^{-1} + M_2P_2G_1^{-1} = I.$$  

Let

$$m_1 = M_2P_2G_1^{-1}r_1 + M_1P_1G_1^{-1}r_2.$$  

We next prove that $m_1$ given in (31) is a solution of a system of congruences as follows:

$$\begin{cases} m \equiv r_1 \pmod{M_1} \\ m \equiv r_2 \pmod{M_2}. \end{cases}$$

From (30), we can rewrite (31) as

$$m_1 = (I - M_1P_1G_1^{-1})r_1 + M_1P_1G_1^{-1}r_2 = r_1 + M_1P_1G_1^{-1}(r_2 - r_1).$$

One can see from (32) that $M_1n_1 - M_2n_2 = r_2 - r_1$ holds for some integer vectors $n_1$ and $n_2$, and thus we have

$$G_1^{-1}M_1n_1 - G_1^{-1}M_2n_2 = G_1^{-1}(r_2 - r_1).$$

Since $G_1$ is a gcd of $M_1$ and $M_2$, we know that $G_1^{-1}M_1$ and $G_1^{-1}M_2$ are integer matrices, and thus $G_1^{-1}(r_2 - r_1)$ is an integer vector. Therefore, $m_1$ given in (31) is an integer vector, and we have, from (33),

$$m_1 \equiv r_1 \pmod{M_1}.$$  

Similarly, we can rewrite (31) as

$$m_1 = M_2P_2G_1^{-1}r_1 + (I - M_2P_2G_1^{-1})r_2 = r_2 + M_2P_2G_1^{-1}(r_1 - r_2),$$

and $m_1$ given in (33) satisfies

$$m_1 \equiv r_2 \pmod{M_2}.$$  

That is to say, $m_1$ given in (33) is a solution of the system of congruences in (32). Thus, we have $m - m_1 \in \text{LAT}(M_1)$ and $m - m_1 \in \text{LAT}(M_2)$. From Proposition 6, we have $m - m_1 \in \text{LAT}(R_1)$, i.e.,

$$m \equiv m_1 \pmod{R_1}.$$  

Based on the cascade architecture of the congruences, we can accordingly calculate a solution $m_2$ of

$$\begin{cases} m \equiv m_1 \pmod{R_1} \\ m \equiv r_3 \pmod{M_3}. \end{cases}$$

Let $R_2$ be an lcrm of $R_1$ and $M_3$, and we have

$$m \equiv m_2 \pmod{R_2}.$$  

Moreover, from Lemma 11, $R_2$ is an lcrm of $M_1, M_2,$ and $M_3$. Following the above procedure, we merge two congruences at a time until we calculate a solution $m_{L-1}$ of

$$\begin{cases} m \equiv m_{L-2} \pmod{R_{L-2}} \\ m \equiv r_L \pmod{M_L}. \end{cases}$$

where $R_{L-2}$ is an lcrm of $M_1, M_2, \ldots, M_{L-1}$. Let $R_{L-1}$ be an lcrm of $R_{L-2}$ and $M_L$, and we have

$$m \equiv m_{L-1} \pmod{R_{L-1}},$$

where we readily know from Lemma 11 that $R_{L-1}$ is an lcrm of $M_1, M_2, \ldots, M_L$. Without loss of generality, we can let $R_{L-1} = R$. So, we can get $m \in \mathbb{N}(R)$ as

$$m = \langle m \rangle_{M_{L-1}}R.$$  

Finally, we prove the uniqueness of the solution for $m$ modulo $R$. Assume that there exists another solution $m' \in \mathbb{N}(R)$ that satisfies $r_i = \langle m' \rangle_{M_i}$ for $1 \leq i \leq L$. Let $m'' = m - m'$. We know $m'' \equiv 0 \pmod{M_i}$ for $1 \leq i \leq L$, that is,

$$m'' \in \text{LAT}(M_1) \cap \text{LAT}(M_2) \cap \cdots \cap \text{LAT}(M_L).$$

From Proposition 6 and Lemma 11, we can easily know

$$\text{LAT}(M_1) \cap \text{LAT}(M_2) \cap \cdots \cap \text{LAT}(M_L) = \text{LAT}(R).$$

Hence, we have $m'' \in \text{LAT}(R)$, i.e.,

$$m'' = Rk$$

for some integer vector $k$. Since $m, m' \in \mathbb{N}(R)$ and $m'' = m - m'$, we have

$$m'' \in \{n \mid n = Rx, x \in (-1, 1)^D \}$$

and $n$ is an integer vector),

where $D$ is the length of $m''$. Since $R$ is nonsingular from the definition of lcrm, this implies $k = 0$ in (46), and thus $m'' = 0$. The proof is completed.

As it can be seen in the proof of Theorem 1, a reconstruction algorithm for the MD-CRT for integer vectors is given as well, which solves the first two congruences, uses that result as the remainder with respect to an lcrm of the first two moduli, and combines this new congruence with the third congruence, and so on. We assume that there exist $L$ pairwise commutative and coprime integer matrices, denoted by $N_1, N_2, \ldots, N_L$, such that $R = N_1N_2 \cdots N_LU$ for some unimodular matrix $U$ and $N_i$ is a
left divisor of $M_i$ for each $1 \leq i \leq L$ in Theorem[1]. Under this assumption, we can derive a simple reconstruction formula for the MD-CRT for integer vectors as follows.

**Lemma 2:** Let $N_i$ for $1 \leq i \leq L$ be $L$ nonsingular integer matrices, which are pairwise commutative and coprime, i.e., $N_i N_j = N_j N_i$, and $N_i$ and $N_j$ are coprime for each pair of $i$ and $j$, $1 \leq i \neq j \leq L$. Then,

1. $N_i \cdot N_{i_2} \cdots N_{i_p}$ and $N_{i_2} \cdot N_{i_3} \cdots N_{i_p}$ are commutative and coprime for any subsets $\{i_1, i_2, \ldots, i_p\} \subset \{1, \ldots, L\}$ and $\{j_1, j_2, \ldots, j_q\} \subset \{1, \ldots, L\}$, i.e.,

$$N_i N_{i_2} \cdots N_{i_p} = N_{i_2} N_{i_3} \cdots N_{i_p}.$$

(48) We next prove their coprimeness. For easy presentation, we first look at a simple case when $L = 3$. In this case, we prove without loss of generality that $N_1 N_2$ and $N_1$ are coprime. Let $D$ be a gcd of $N_1 N_2$ and $N_3$. Since $N_1$ and $N_2$ are coprime, we have, from Bezout’s theorem in Proposition[2],

$$PN_1 + QN_3 = I,$$

(49) where $P$ and $Q$ are some integer matrices. Right-multiplying $N_2 D^{-1}$ on both sides of (49) and then commuting $N_2$ and $N_1$, we have

$$PN_1 N_2 D^{-1} + QN_2 N_3 D^{-1} = N_2 D^{-1}.$$  

(50) Considering that $D$ is a gcd of $N_1 N_2$ and $N_3$, i.e., $N_1 N_2 D^{-1}$ and $N_3 D^{-1}$ are integer matrices, we know from (50) that $N_2 D^{-1}$ is an integer matrix. That is to say, $D$ is a right divisor of $N_2$. As stated above, $D$ is a right divisor of $N_2$ and $N_3$ are coprime. So, $D$ must be a unimodular matrix. Thus, $N_1 N_2$ and $N_3$ are right coprime (equivalently coprime from Proposition[2] due to their commutativity). Accordingly, the above result can be readily generalized to the case when $L > 3$, and therefore, $N_1 N_2 \cdots N_{i_1}$ and $N_{i_2} N_{i_3} \cdots N_{i_p}$ are coprime.

2) Following Proposition[2] and the above 1), we obtain that $R_2 \triangleq N_1 N_{i_2}$ is an lcm of $N_1$ and $N_{i_2}$, and $R_2$ is commutative and coprime with $N_{i_2}$. So, $R_3 \triangleq R_2 N_{i_3} = N_1 N_{i_2} N_{i_3}$ is an lcm of $R_2$ and $N_{i_3}$, and $R_3$ is commutative and coprime with $N_{i_3}$. Moreover, $R_3$ is an lcm of $N_1$, $N_{i_2}$, and $N_{i_3}$ from Lemma[1]. Continue this procedure until $R_p \triangleq R_{p-1} N_{i_p} = N_1 N_{i_2} \cdots N_{i_p}$, which is an lcm of $R_{p-1}$ and $N_{i_p}$. From Lemma[1], $R_p$ is an lcm of $N_1$, $N_{i_2}$, ..., $N_{i_p}$, and similarly, we can deduce that $R_p$ is also an lcm of $N_1$, $N_{i_2}$, ..., $N_{i_p}$.

**Corollary 1:** Given $L$ moduli $M_i$ for $1 \leq i \leq L$, which are arbitrary nonsingular integer matrices, let $R$ be anyone of their lcrms. Let us assume that there exist $L$ pairwise commutative and coprime integer matrices, denoted by $N_1, N_2, \ldots, N_L$, such that $R = N_1 N_2 \cdots N_L$ for some unimodular matrix $U$ and $N_i$ is a left divisor of $M_i$ for each $1 \leq i \leq L$. For an integer vector $m \in \mathcal{N}(R)$, we can uniquely reconstruct $m$ from its remainders $r_i = \langle m \rangle_{M_i}$ as

$$m = \left\{ \sum_{i=1}^{L} W_i \hat{W}_i r_i \right\}_{R},$$

(51) where $W_i = N_1 \cdots N_{i-1} N_{i+1} \cdots N_L$, and if $N_i$ is not unimodular, $\hat{W}_i$ is some integer matrix satisfying

$$W_i \hat{W}_i + N_i Q_i = I$$

(52) for some integer matrix $Q_i$, and can be calculated by following the procedure (11)-(22) in advance; otherwise $\hat{W}_i = 0$.

**Proof:** Since $N_i$ is a left divisor of $M_i$ for each $1 \leq i \leq L$, there exists some integer matrix $P_i$ such that $M_i = N_i P_i$ for each $1 \leq i \leq L$. So, from the remainders $r_i = \langle m \rangle_{M_i}$, we have

$$m = N_i P_i n_i + r_i$$

(53) for $1 \leq i \leq L$, where $n_i$'s are unknown folding vectors. Regarding (53) as a system of congruences with respect to the moduli $N_i$'s, we then calculate the remainders $\xi_i \in \mathcal{N}(N_i)$ of $r_i$ modulo $N_i$, i.e.,

$$\xi_i = (r_i)_{N_i}, \quad 1 \leq i \leq L.$$  

(54) Therefore, we get

$$m \equiv \xi_i \mod N_i \quad 1 \leq i \leq L.$$  

(55) Since the moduli $N_1, N_2, \ldots, N_L$ in (55) are pairwise commutative and coprime, we know from Lemma[2] that $N_1 N_2 \cdots N_L$ is their lcm, and so is $R = N_1 N_2 \cdots N_L U$ for a unimodular matrix $U$. Therefore, we obtain from Theorem[1] that $m \in \mathcal{N}(R)$ can be uniquely reconstructed from its remainders $\xi_i$'s or $r_i$'s. Next, we prove that $m$ in (55) is actually a solution of the system of congruences in (55). We express $m$ equivalently as

$$m = R n + \sum_{i=1}^{L} W_i \hat{W}_i r_i$$

(56) for some integer vector $n$. Then, for each modulo-$N_j$ operation, we calculate

$$\langle m \rangle_{N_j} = \left\{ \sum_{i=1, i \neq j}^{L} W_i \hat{W}_i r_i + \sum_{i=1}^{L} W_i \hat{W}_i r_i \right\}_{N_j}$$

(57) $$= \left\{ \sum_{i=1, i \neq j}^{L} W_i \hat{W}_i r_i \right\}_{N_j}$$

(58) $$= \langle (I - N_j Q_j) r_i \rangle_{N_j}$$

(59) $$= (r_i)_{N_j}$$

(60) where the second equality is due to the commutativity of $N_j$'s, the third equality is obtained from (52), and (52) holds because $N_j$ is coprime with $W_i$ for each $1 \leq i \leq L$ from Lemma[2]. This completes the proof of the corollary.

In what follows, let us see in detail some special cases of the MD-CRT for integer vectors, where the $L$ nonsingular moduli are given by

$$M_i = M_i \Gamma_i \quad 1 \leq i \leq L,$$

(61) and $M_i$ and $\Gamma_i$'s are integer matrices. Clearly, the moduli given by (61) are in general not commutative. For the specific moduli in (61), we first prove the following lemma.

**Lemma 3:** For the moduli $M_i$'s in (61), let $A$ be an lcm of $\Gamma_i$ for $1 \leq i \leq L$. Then, $M_i A$ is an lcm of $M_i$ for $1 \leq i \leq L$.

**Proof:** Since $A$ is an lcm of $\Gamma_i$ for $1 \leq i \leq L$, $M_i A$ is a crm of $M_i$ for $1 \leq i \leq L$. For any other crm $C$ of $M_i$'s, i.e.,

$$C = M_i \Gamma_i P_i$$

(62) for some integer matrices $P_i$ and $1 \leq i \leq L$, we have $M_i^{-1} C = \Gamma_i P_i$, i.e., $M_i^{-1} C$ is a crm of $\Gamma_i$'s. So, $M_i^{-1} C$ is a
right multiple of $A$, i.e., $M^{-1}C = AG$ for some integer matrix $G$. Hence, we have $C = MAG$. This is to say, $MA$ is an lcm of $M_i$’s.

Then, we present the following results.

**Corollary 2:** Given $L$ nonsingular moduli

$$M_i = M_\Gamma_i \text{ for } 1 \leq i \leq L,$$

where $M, \Gamma_1, \Gamma_2, \ldots, \Gamma_L$ are pairwise commutative and coprime integer matrices, let $R$ be any member of their lcm, i.e., $R = M_\Gamma_1 \Gamma_2 \cdots \Gamma_LU$ for any unimodular matrix $U$. For an integer vector $m \in \mathcal{N}(R)$, we can uniquely reconstruct $m$ from its remainders $r_i = (m)_{M_i}$ as in Corollary 1.

**Proof:** Considering that $\Gamma_i$’s are pairwise commutative and coprime, we know from Lemma 2 that $\Gamma_1 \Gamma_2 \cdots \Gamma_L$ is an lcm of $\Gamma_i$’s. It is known from Lemma 3 that $R = M_\Gamma_1 \Gamma_2 \cdots \Gamma_LU$ for any unimodular matrix $U$ is an lcm of $M_i$’s given by (59).

Without loss of generality, we let $N_1 = M_\Gamma_1$, $N_2 = \Gamma_2 \cdots, N_L = \Gamma_L$. Due to the fact that $M, \Gamma_1, \Gamma_2, \ldots, \Gamma_L$ are pairwise commutative and coprime, we obtain from Lemma 2 that $N_i$’s are pairwise commutative and coprime. In addition, it is also easily seen that $R = N_1 N_2 \cdots N_L U$, and $N_i$ is a left divisor of $M_i$ for each $1 \leq i \leq L$. Therefore, by Corollary 1 we can uniquely reconstruct $m \in \mathcal{N}(R)$ from the moduli $M_i$’s and its remainders $r_i = (m)_{M_i}$ by (55).

**Corollary 3:** Given $L$ nonsingular moduli

$$M_i = M_\Gamma_i \text{ for } 1 \leq i \leq L,$$

where $M$ is a unimodular matrix, and $\Gamma_i$’s are pairwise commutative and coprime integer matrices, let $R$ be any of their lcm, i.e., $R = M_\Gamma_1 \Gamma_2 \cdots \Gamma_L U$ for any unimodular matrix $U$. For an integer vector $m \in \mathcal{N}(R)$, we can uniquely reconstruct $m$ from its remainders $r_i = (m)_{M_i}$ as

$$m = \left( \sum_{j=1}^{L} W_i \bar{W}_j r_j \right) \mod R,$$

where $W_i = M_\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L$, and $\bar{W}_j$ is some integer matrix satisfying

$$W_i \bar{W}_j + M_i Q_i = I$$

for some integer matrix $Q_i$ and can be calculated by following the procedure (11)-(22) in advance.

**Proof:** Since $\Gamma_i$’s are pairwise commutative and coprime, $\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L$ and $\Gamma_i$ are known to be commutative and coprime from Lemma 2. We next prove that $W_i$ and $M_i$ are left coprime for each $1 \leq i \leq L$. Let $D$ be a gcd of $W_i$ and $M_i$. We then have $W_i = M_\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L D$ and $M_i = M_\Gamma_i D Q_i$ for some integer matrices $P$ and $Q_i$. Hence, we have

$$\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L = M_i^{-1} D P_i$$

as $M$ is unimodular. $M_i^{-1} D$ is an integer matrix and is a cld of $\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L$ and $\Gamma_i$. Since $\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L$ and $\Gamma_i$ are commutative and coprime, all of their clds are unimodular. Therefore, $M_i^{-1} D$ is a unimodular matrix, and so is $D$. That is to say, $W_i$ and $M_i$ are left coprime. Based on the Bezout’s theorem in Proposition 3 there exist integer matrices, denoted by $\bar{W}_i$ and $Q_i$, such that (65) holds for each $1 \leq i \leq L$, and we can calculate them by following the procedure (11)-(22). In addition, from Lemma 2 and Lemma 3 we know that $R = M_\Gamma_1 \Gamma_2 \cdots \Gamma_L U$ for any unimodular matrix $U$ is an lcm of

the moduli $M_i$’s given by (60). The remaining proof is similar to the proof of Corollary 1 and is omitted here.

**Remark 2:** Considering that $M$ in (60) is unimodular, we are able to propose an alternative proof of Corollary 3 below. From the remainders $r_i = (m)_{M_i}$, we have

$$m = M_\Gamma \bar{n}_i + r_i,$$

$$M_i^{-1} m = \Gamma_i n_i + M_i^{-1} r_i$$

for $1 \leq i \leq L$, where $n_i$’s are unknown folding vectors. Due to the unimodularity of $M$, $M_i^{-1} m$ and $M_i^{-1} r_i$’s are integer vectors. Thus, we can view (63) as a system of congruences with respect to the modulus $\Gamma_i$’s, i.e.,

$$M_i^{-1} m \equiv M_i^{-1} r_i \mod \Gamma_i$$

for $1 \leq i \leq L$. (64)

and then calculate the remainders $\zeta_i \in \mathcal{N}(\Gamma_i)$ of $M_i^{-1} r_i$ modulo $\Gamma_i$, i.e., $M_i^{-1} r_i \equiv \zeta_i \mod \Gamma_i$, for $1 \leq i \leq L$. From (64), we get

$$M_i^{-1} m \equiv \zeta_i \mod \Gamma_i$$

for $1 \leq i \leq L$. (65)

Since $M$ is unimodular and $m \in \mathcal{N}(M_\Gamma_1 \Gamma_2 \cdots \Gamma_L U)$ for any unimodular matrix $U$, we obtain $M_i^{-1} m \in \mathcal{N}(\Gamma_1 \Gamma_2 \cdots \Gamma_L U)$. Moreover, since $\Gamma_i$’s are pairwise commutative and coprime, we know from Lemma 2 that $\Gamma_1 \Gamma_2 \cdots \Gamma_L$ is their lcm. Therefore, $M_i^{-1} m$ can be uniquely reconstructed from its remainders $\zeta_i$’s in (65) according to Corollary 1 and so can be $m$.

In particular, when $M$ in (60) is the identity matrix, i.e., $M = I$, Corollary 3 reduces to the CC MD-CRT for integer vectors with respect to pairwise commutative and coprime moduli (i.e., nonsingular integer matrices), as stated below, in comparison with the CC CRT for integers with respect to pairwise coprime moduli (i.e., positive integers).

**Theorem 2 (CC MD-CRT for integer vectors):** Given $L$ nonsingular moduli $M_i$ for $1 \leq i \leq L$, which are pairwise commutative and coprime integer matrices, let $R$ be any of their lcm, i.e., $R = M_1 M_2 \cdots M_L U$ for any unimodular matrix $U$. For an integer vector $m \in \mathcal{N}(R)$, we can uniquely reconstruct $m$ from its remainders $r_i = (m)_{M_i}$ as in Corollary 3 with $M = I$.

We next see another special case of the MD-CRT for integer vectors, where the $L$ nonsingular moduli can be simultaneously diagonalized by using two common unimodular matrices, i.e.,

$$M_i = UA_i V \in \mathcal{Z}^{D \times D}$$

for $1 \leq i \leq L$ (66)

with $A_i$’s being diagonal integer matrices, and $U$ and $V$ being unimodular matrices. For each $1 \leq i \leq L$, write $A_i$ as $A_i = \text{diag}(A_i(1, 1), A_i(2, 2), \ldots, A_i(D, D))$. Let

$$A = \text{diag}(A(1, 1), A(2, 2), \ldots, A(D, D)),$$

and $A(j, j)$ be the lcm of $A_1(j, j), A_2(j, j), \ldots, A_L(j, j)$ for each $1 \leq j \leq D$. It is readily verified that $A$ is an lcm of $A_i$ for $1 \leq i \leq L$.

We next prove that $A$ is also an lcm of $A_i V$ for $1 \leq i \leq L$. Since $A$ is an lcm of $A_i$’s, we have $A = A_i P_i$ for some integer matrices $P_i$’s. Due to the unimodularity of $V$, we have $A = A_i V V^{-1} P_i$, and $V^{-1} P_i$ is an integer matrix for each $1 \leq i \leq L$. So, $A$ is a crm of $A_i V$ for $1 \leq i \leq L$. For any other crm $Q$ of $A_i V$ for $1 \leq i \leq L$, we have $Q = A_i V Q_i$ for some integer matrices $Q_i$’s, which indicates that $Q$ is a crm of $A_i$’s. Thus, $Q$ is a right multiple of $A$, i.e., $A$ is an lcm of $A_i V$ for $1 \leq i \leq L$.
Furthermore, from Lemma 3 we obtain that $UA$ is an lcm of $M_i$’s given by (65). Let $R$ be anyone of the lcm’s of $M_i$’s, i.e., $R = UAB$ for any unimodular matrix $B$. For an integer vector $m \in N(R)$ and its remainders $r_i = (m)_{M_i}$, we have

$$m = UA_iV_n + r_i$$

$$U^{-1}m = A_iV_n + U^{-1}r_i \quad \text{for } 1 \leq i \leq L.$$  \hspace{1cm} (68)

Due to the unimodularity of $U$, $U^{-1}m$ and $U^{-1}r_i$’s are integer vectors. Hence, we can view (68) as a system of congruences with respect to the moduli $A_i$’s, i.e.,

$$U^{-1}m \equiv U^{-1}r_i \mod A_i \quad \text{for } 1 \leq i \leq L.$$  \hspace{1cm} (69)

and then calculate the remainders $\zeta_i \in N(A_i)$ of $U^{-1}r_i$ modulo $A_i$, i.e., $U^{-1}r_i \equiv \zeta_i \mod A_i$, for $1 \leq i \leq L$. From (69), we get

$$U^{-1}m \equiv \zeta_i \mod A_i \quad \text{for } 1 \leq i \leq L.$$  \hspace{1cm} (70)

Since $m \in N(UAB)$ for any unimodular matrix $B$ and $U$ is a unimodular matrix, we obtain $U^{-1}m \in N(AB)$. Furthermore, since $A_i$’s are diagonal integer matrices, it is always ready to find $L$ pairwise commutative and coprime integer matrices (i.e., coprime diagonal integer matrices), denoted by $N_1, N_2, \ldots, N_L$, such that $A = N_1N_2\cdots N_L$ and $N_i$ is a left divisor of $A_i$ for each $1 \leq i \leq L$. Therefore, from Corollary 1, we can uniquely reconstruct such $m$. When $m$ is restricted to $m \in N(UA)$, i.e., the unimodular matrix $B$ is taken to be the identity matrix, the reconstruction of $m$ is equivalent to that via the $D$ independent conventional CRT for integers as follows. Let $a = U^{-1}m \in \mathbb{Z}^D$. Due to $m \in N(UA)$, we obtain $a \in N(A)$. That is to say, every element $a(j)$ of $a$ satisfies $a(j) \in N(A(j, j))$ (i.e., $0 \leq a(j) < A(j, j)$) for $1 \leq j \leq D$. Therefore, via the CRT for integers, we can uniquely reconstruct $a(j)$ for each $1 \leq j \leq D$ in the following system of congruences:

$$a(j) \equiv \zeta_i(j) \mod [A_i(j, j)] \quad \text{for } 1 \leq i \leq L.$$  \hspace{1cm} (71)

Based on the above analysis, we have the following result.

**Corollary 4:** Let $L$ nonsingular moduli $M_i$ for $1 \leq i \leq L$ be given by (66), and $R$ be anyone of their lcm’s, i.e., $R = UAB$ for any unimodular matrix $B$, where $A$ is given by (67). For an integer vector $m \in N(R)$, we can uniquely reconstruct $m$ from its remainders $r_i = (m)_{M_i}$ as in Corollary 1. Interestingly, when $B$ is the identity matrix, i.e., $R = UA$, the reconstruction of $m \in N(R)$ is equivalent to that via the $D$ independent conventional CRT for integers.

In particular, when the $D \times D$ nonsingular moduli $M_i$’s can be simultaneously diagonalized as

$$M_i = UA_iU^{-1} \quad \text{for } 1 \leq i \leq L,$$  \hspace{1cm} (72)

where $U$ is a $D \times D$ unimodular matrix, and $A_i$’s are diagonal integer matrices that are pairwise coprime, it is readily verified that the moduli are pairwise commuting and coprime. Note that $A_i$ and $A_j$ are coprime if and only if the corresponding diagonal elements $A_i(k, k)$ and $A_j(k, k)$ are coprime for each $1 \leq k \leq D$. For this case, as a direct consequence of Theorem 2 or Corollary 4, we obtain the following result, which has been presented in (46), (47).

**Corollary 5 (47):** Let $L$ nonsingular moduli $M_i$ for $1 \leq i \leq L$ be given by (72), and $R$ be anyone of their lcm’s, i.e., $R = UA_1A_2\cdots A_LB$ for any unimodular matrix $B$. For an integer vector $m \in N(R)$, we can uniquely reconstruct $m$ from its remainders $r_i = (m)_{M_i}$ as in Theorem 2.

We conclude this section by showing an example to explain how to implement the MD-CRT for integer vectors step by step. Since this example involves a family of $2 \times 2$ integer circulant matrices, let us first introduce integer circulant matrices.

An integer matrix is said to be circulant if each row can be obtained from the preceding row by a right circular shift, e.g., a $2 \times 2$ integer circulant matrix $P = \begin{pmatrix} p & q \\ q & p \end{pmatrix}$. It is readily verified that integer circulant matrices are commutative with each other, and it has been proved in (55), (56) that any two $2 \times 2$ integer circulant matrices $P_1 = \begin{pmatrix} p_1 & q_1 \\ q_1 & p_1 \end{pmatrix}$ and $P_2 = \begin{pmatrix} p_2 & q_2 \\ q_2 & p_2 \end{pmatrix}$ are coprime, if and only if $p_1 + q_1$ is coprime with $p_2 + q_2$, and $p_1 - q_1$ is coprime with $p_2 - q_2$. Note that a trivial subclass of $2 \times 2$ integer circulant matrices with all equal elements is excluded from consideration in (55), (56) and this paper. We then prove that a $2 \times 2$ integer circulant matrix $P = \begin{pmatrix} p & q \\ q & p \end{pmatrix}$ with $q \neq 0$ cannot be diagonalized as in (72).

**Lemma 4:** A $2 \times 2$ integer circulant matrix $P = \begin{pmatrix} p & q \\ q & p \end{pmatrix}$ with $q \neq 0$ cannot be diagonalized as $P = UAU^{-1}$, where $U$ is a $2 \times 2$ unimodular matrix and $A$ is a diagonal integer matrix.

**Proof:** Let $\alpha_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\alpha_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$. It is readily checked that $\alpha_1$ and $\alpha_2$ are two eigenvectors of $P$ with the corresponding eigenvalues $p + q$ and $p - q$. Any integer vector in $\mathbb{R}^2$ can be represented by a linear combination of $\alpha_1$ and $\alpha_2$. Assume that $P$ can be diagonalized as $P = UAU^{-1}$, where $U$ is a $2 \times 2$ unimodular matrix and $A$ is a diagonal integer matrix. This means that $U$ is an eigenvector of $P$. Let $u$ be any column vector of $U$ and it can be represented by $u = a\alpha_1 + b\alpha_2$ with $a, b \in \mathbb{R}$. Then, we get

$$Pu = pu + q(a\alpha_1 - b\alpha_2).$$  \hspace{1cm} (73)

Since $U$ is unimodular, it is nonsingular, and its column vectors cannot be the all-zero vectors. Since $u$ is a non-zero eigenvector of $P$ and $q \neq 0$, we know that one and only one of $a$ and $b$ must be 0. Thus, $U$ has to be the form of

$$\begin{pmatrix} a_1 & a_2 \\ -b_1 & -b_2 \end{pmatrix}, \begin{pmatrix} a_1 & -a_2 \\ b_1 & b_2 \end{pmatrix}, \text{ or } \begin{pmatrix} a_1 & a_2 \\ -b_1 & -b_2 \end{pmatrix}.$$  \hspace{1cm} (74)

Obviously, the determinants of

$$\begin{pmatrix} a_1 & a_2 \\ a_1 & -a_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a_1 & a_2 \\ -b_1 & -b_2 \end{pmatrix}$$  \hspace{1cm} (75)

are zero, which indicates that the first two forms of matrices are not possible to be unimodular. The determinants of

$$\begin{pmatrix} a_1 & a_2 \\ a_1 & -a_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b_1 & b_2 \\ b_1 & -b_2 \end{pmatrix}$$  \hspace{1cm} (76)

are $-a_1a_2$ and $2b_1b_2$, respectively, which are not equal to $\pm 1$ for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. This indicates that the last two forms of matrices are also not possible to be unimodular. Therefore, $U$ cannot be unimodular. That is to say, $P$ cannot be diagonalized as $P = UAU^{-1}$, where $U$ is a $2 \times 2$ unimodular matrix and $A$ is a diagonal integer matrix.

**Example 1:** Let $L = 3$ moduli be $M_i = M\Gamma_i$ for $1 \leq i \leq 3$, where $\Gamma_i$’s are pairwise coprime integer circulant matrices, i.e.,

$$\Gamma_1 = \begin{pmatrix} 4 & -1 \\ -1 & 4 \end{pmatrix}, \Gamma_2 = \begin{pmatrix} 7 & 4 \\ 4 & 7 \end{pmatrix}, \text{ and } \Gamma_3 = \begin{pmatrix} 6 & -2 \\ -2 & 6 \end{pmatrix}.$$  \hspace{1cm} (77)

We then consider the following two cases that are not covered by (47) or Corollary 5 in this paper.
\( M \) is commutative and coprime with each \( \Gamma_i \), for 1 \( \leq \) \( i \) \( \leq \) 3. This case corresponds to the moduli given in Corollary 1.

Without loss of generality, we take \( M = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} \), which is also an integer circulant matrix. One can see that \( M \) for 1 \( \leq \) \( i \) \( \leq \) 3 in this case are \( 2 \times 2 \) integer circulant matrices and their nondiagonal elements are non-zero. Therefore, from Lemma 4, the moduli \( M_i \)'s cannot be diagonalized as in (72). Let

\[
R = M\Gamma_1\Gamma_2\Gamma_3 = \begin{pmatrix} 402 & 522 \\ 522 & 402 \end{pmatrix}
\]

and \( m = \begin{pmatrix} 402 \\ 522 \end{pmatrix} \). Conversely, we can reconstruct \( m \) from its remainders \( r \), for 1 \( \leq \) \( i \) \( \leq \) 3 via the MD-CRT for integer vectors. Before presenting that, we first review the robust CR \( T \).

In practice, signals of interest are usually subject to noise, and accordingly the detected remainders may be erroneous in many signal processing applications of the CRT. To this end, the robust CRT for integers has been proposed in [12–14] and further dedicatedly studied in [20–24]. It basically says that even though every remainder has a small error, a large nonnegative integer can be robustly reconstructed in the sense that the reconstruction error is upper bounded by the remainder error bound. In this section, motivated by the applications in MD signal processing, we want to extend the robust CRT for integers to the MD case, the robust MD-CRT for integer vectors.

Before presenting that, we first review the robust CRT for integers in [14], for comparison purposes.

**Proposition 8 (Robust CRT for integers [24]):** Let \( L \) moduli be \( M_i = M_i \), for 1 \( \leq \) \( i \) \( \leq \) \( L \), where \( \Gamma_i \)'s are pairwise coprime positive integers, and \( M > 1 \) is an arbitrary positive integer. Let \( R = M\Gamma_1\Gamma_2\cdots\Gamma_L \) be their lcm. For an integer \( m \in N(R) \) (i.e., 0 \( \leq \) \( m \) \( < \) \( R \)), let \( r \)'s be its remainders, i.e., \( r_i = \langle m \rangle_{M_i} \) or

\[
m = M_i r_i + r_i \quad \text{for} \quad 1 \leq i \leq L,
\]

\( \text{proof of Theorem}[1] \). It is readily verified that \( M \) and \( R_1 = M\Gamma_1\Gamma_2 \) are a gcd and an lcrm of \( M_1 \) and \( M_2 \), respectively. Based on the Bezout's theorem in Proposition 5 we follow the procedure (11)–(22) to get \( P_1 = \begin{pmatrix} 3 & 11 \\ 1 & 4 \end{pmatrix} \) and \( P_2 = \begin{pmatrix} -2 & -8 \\ 1 & 4 \end{pmatrix} \) such that \( M_1 P_1 + M_2 P_2 = M \). So, from (31), we get

\[
m_1 = M_2 P_2 M^{-1} r_1 + M_1 P_1 M^{-1} r_2 = \begin{pmatrix} 510 \\ 994 \end{pmatrix},
\]

which satisfies

\[
\begin{aligned}
m_1 & \equiv r_1 \mod M_1 \\
m_1 & \equiv r_2 \mod M_2.
\end{aligned}
\]

We calculate the remainder \( \nu_1 \) of \( m_1 \), modulo \( R_1 \), i.e.,

\[
\nu_1 = \langle m_1 \rangle_{R_1} = \begin{pmatrix} 30 \\ 52 \end{pmatrix}.
\]

Following the above procedure, we calculate a solution of a system of congruences:

\[
\begin{align*}
m & \equiv \nu_1 \mod R_1 \\
m & \equiv r_3 \mod M_3.
\end{align*}
\]

It is also readily verified that \( M \) and \( R_2 = R = M\Gamma_1\Gamma_2\Gamma_3 \) are a gcd and an lcrm of \( R_1 \) and \( M_3 \), respectively. Based on the Bezout's theorem in Proposition 5 we follow the procedure (11)–(22) to get \( Q_1 = \begin{pmatrix} 4 & -21 \\ -7 & 18 \end{pmatrix} \) and \( Q_2 = \begin{pmatrix} 10 & -24 \\ -18 & 49 \end{pmatrix} \) such that \( R_1 Q_1 + M_3 Q_2 = M \). So, from (31), we get

\[
m_2 = M_1 Q_2 M^{-1} \nu_1 + R_1 Q_1 M^{-1} r_3 = \begin{pmatrix} -375 \\ 1429 \end{pmatrix}.
\]

Therefore, we get

\[
m = \langle m_2 \rangle = \begin{pmatrix} 285 \\ 505 \end{pmatrix}.
\]
where \(n_i\)'s are its folding integers. Let \(\tilde{r}_i = r_i + \Delta r_i\), \(1 \leq i \leq L\), denote the erroneous remainders, where \(\Delta r_i\)'s are the remainder errors. From the erroneous remainders \(\tilde{r}_i\)'s, we can accurately determine the folding integers \(n_i\)'s, if and only if
\[
-\frac{M}{2} \leq \Delta r_i - \Delta r_1 < \frac{M}{2} \quad \text{for } 2 \leq i \leq L.
\]
(75)

In addition, let \(\tau\) be the remainder error bound, i.e., \(|\Delta r_i| \leq \tau\) for \(1 \leq i \leq L\), and a simple sufficient condition for accurately determining the folding integers \(n_i\)'s is derived as
\[
\tau < \frac{M}{4}.
\]
(76)

Once the folding integers \(n_i\)'s are accurately obtained, a robust reconstruction of \(m\) can be calculated by
\[
\hat{m} = \left\lfloor \frac{1}{L} \sum_{i=1}^{L} (Mn_i + \tilde{r}_i) \right\rfloor,
\]
(77)
where \(\lfloor \cdot \rfloor\) denotes the rounding operation. Obviously, the reconstruction error is upper bounded by \(\tau\), i.e.,
\[
|\hat{m} - m| \leq \tau.
\]
(78)

In [14], a closed-form algorithm for determining the folding integers \(n_i\)'s in Proposition 8 was proposed as well. For more information on the robust CRT for integers, we refer the reader to a thorough review in [35].

Motivated by Proposition 8 or [14], we propose the robust MD-CRT for integer vectors through accurately determining the folding vectors in the following. Before that, let us first introduce two significant definitions related to lattices.

**Definition 1 (The shortest vector problem (SVP) on lattices):** For a lattice \(\text{LAT}(M)\) that is generated by a nonsingular matrix \(M\), the minimum distance of \(\text{LAT}(M)\) is the smallest distance between any two lattice points:
\[
\lambda_{\text{LAT}(M)} = \min_{w,v \in \text{LAT}(M), w \neq v} \|w - v\|.
\]
(79)

It is obvious that lattices are closed under addition and subtraction operations. Therefore, the minimum distance of \(\text{LAT}(M)\) is equivalently defined as the length (magnitude) of the shortest non-zero lattice point:
\[
\lambda_{\text{LAT}(M)} = \min_{v \in \text{LAT}(M) \setminus \{0\}} |v|.
\]
(80)

**Definition 2 (The closest vector problem (CVP) on lattices):** For a lattice \(\text{LAT}(M)\) that is generated by a nonsingular matrix \(M \in \mathbb{R}^{D \times D}\), given an arbitrary point \(w \in \mathbb{R}^D\), we find a closest lattice point of \(\text{LAT}(M)\) to \(w\) by
\[
\text{dist}(\text{LAT}(M), w) = \min_{v \in \text{LAT}(M)} |v - w|.
\]
(81)

The SVP and CVP are the two most important computational problems on lattices. The algorithms for solving these problems either exactly or approximately have been extensively studied [57], [58]. Note that the distance above can be measured by any norm of vectors, e.g., the Euclidean norm \(\|v\|_2 = \sqrt{\sum_i |v(i)|^2}\), the \(\ell_1\) norm \(\|v\|_1 = \sum_i |v(i)|\), and the \(\ell_\infty\) norm \(\|v\|_\infty = \max_i |v(i)|\).

Let \(L\) nonsingular moduli \(M_i \in \mathbb{Z}^{D \times D}\) for \(1 \leq i \leq L\) be given by
\[
M_i = \Gamma_i M,
\]
(82)
where \(\Gamma_i \in \mathbb{Z}^{D \times D}\) for \(1 \leq i \leq L\) are pairwise commutative and coprime, and \(M \in \mathbb{Z}^{D \times D}\). Define
\[
\mathcal{A}_i = \{m \in \mathbb{Z}^D | [M_i^{-1} m] \in \mathcal{N}(\Gamma_1 \cdots \Gamma_{i-1} \Gamma_{i+1} \cdots \Gamma_L U_i)\}
\]
(83)
for \(1 \leq i \leq L\), where \(U_i \in \mathbb{Z}^{D \times D}\) is any unimodular matrix. Let \(\tilde{r}_i = r_i + \Delta r_i \in \mathbb{Z}^D\) for \(1 \leq i \leq L\) be the erroneous remainders of an integer vector \(m\) with respect to the moduli \(M_i\)'s, where \(r_i\)'s and \(\Delta r_i\)'s are the remainders and remainder errors, respectively.

Since \(r_i\)'s are the remainders of \(m\) with respect to the moduli \(M_i\)'s in (82), we have
\[
m = M_1 n_1 + r_1
\]
\[
m = M_2 n_2 + r_2
\]
\[
\vdots
\]
\[
m = M_L n_L + r_L.
\]
(84)

Without loss of generality, we assume that \(m \in \mathcal{A}_1\). Therefore, we treat the first equation in (82) as a reference to be subtracted from the other \(L - 1\) equations, and we get
\[
\begin{align*}
\Gamma_1 n_1 - \Gamma_2 n_2 &= r_2 - r_1 \\
\Gamma_1 n_1 - \Gamma_3 n_3 &= r_3 - r_1 \\
&\vdots \\
\Gamma_1 n_1 - \Gamma_L n_L &= r_L - r_1.
\end{align*}
\]
(85)

Left-multiplying \(M^{-1}\) on both sides of all the equations in (85), we obtain
\[
\begin{align*}
\Gamma_1 n_1 - \Gamma_2 n_2 &= M^{-1}(r_2 - r_1) \\
\Gamma_1 n_1 - \Gamma_3 n_3 &= M^{-1}(r_3 - r_1) \\
&\vdots \\
\Gamma_1 n_1 - \Gamma_L n_L &= M^{-1}(r_L - r_1).
\end{align*}
\]
(86)

From (86), we know that \(M^{-1}(r_i - r_1)\) for \(2 \leq i \leq L\) are integer vectors, i.e.,
\[
r_i - r_1 \in \text{LAT}(M).
\]
(87)

We then perform the modulo-\(\Gamma_i\) operation on both sides of the corresponding \((i-1)\)-th equation in (85) for \(2 \leq i \leq L\) to get
\[
\begin{align*}
\Gamma_1 n_1 &\equiv 0 \pmod{\Gamma_1} \\
\Gamma_1 n_1 &\equiv M^{-1}(r_2 - r_1) \pmod{\Gamma_2} \\
\Gamma_1 n_1 &\equiv M^{-1}(r_3 - r_1) \pmod{\Gamma_3} \\
&\vdots \\
\Gamma_1 n_1 &\equiv M^{-1}(r_L - r_1) \pmod{\Gamma_L},
\end{align*}
\]
(88)

where the first equation is always available.

Since we know the erroneous remainders \(\tilde{r}_i\)'s rather than the remainders \(r_i\)'s, we estimate \(r_i - r_1\) for each \(2 \leq i \leq L\) by using a closest lattice point \(v_i\) of \(\text{LAT}(M)\) to \(\tilde{r}_i - r_1\), i.e.,
\[
v_i \doteq \arg \min_{v \in \text{LAT}(M)} |v - (\tilde{r}_i - r_1)|.
\]
(89)

Let \(\tilde{n}_i\) for \(1 \leq i \leq L\) be a set of solutions of (85) when \(r_i - r_1\) for \(2 \leq i \leq L\) are replaced with \(v_i\). In summary, we have the following Algorithm 1 for obtaining \(\tilde{n}_i\)'s.

**Algorithm 1:**

1. Set \(i \leftarrow 2\).
2. Update \(n_i \leftarrow v_i\).
3. For \(i \leftarrow 3, \ldots, L\), set \(n_i \leftarrow \text{round}(v_i + n_{i-1})\).
4. Set \(i \leftarrow i + 1\).
5. If \(i \leq L\), go to Step 2; else, stop.

**Theorem 3 (Robust MD-CRT for integer vectors–I):** Let \(L\) nonsingular moduli be given by (82). For an integer vector \(m \in \bigcup_{i=1}^L \mathcal{A}_i\) (assuming without loss of generality that \(m \in \mathcal{A}_1\)), we can accurately determine the folding vectors \(n_i\)'s of
Besides, we present two simple sufficient conditions for accurately determining the folding vectors \( m \)'s with respect to the moduli \( \Gamma_i \)'s. Due to \( m \in A \) and \( n_1 = [M_1^{-1}m] \), we obtain \( n_1 \in N(\Gamma_1 \Gamma_2 \cdots \Gamma_{\ell-1}U_1) \), where \( U_1 \) is any unimodular matrix, and thus \( \Gamma_1n_1 \in N(\Gamma_1 \Gamma_2 \cdots \Gamma_{\ell-1}U_1) \). From (91), \( \Gamma_1n_1 \) can be accurately determined by the CC MD-CRT for integer vectors in Theorem 2 and so can be \( n_1 \), i.e., \( \bar{n}_1 = n_1 \). After obtaining \( n_1 \), we can accurately determine the other folding vectors \( n_i \) for \( 2 \leq i \leq L \) by substituting \( n_1 \) into (88). Therefore, we get \( \bar{n}_1 = n_1 \) for \( 1 \leq i \leq L \) in (91).

We next prove the necessity. Assume that there exists at least one remainder error that does not satisfy (93). For example, the \( k \)-th remainder error \( \Delta r_k \) with \( 2 \leq k \leq L \) satisfies

\[
\theta_k \neq 0. \tag{100}
\]

Therefore, \( v_k \) in (89) does not equal \( r_k - r_1 \). We then have the following cases.

**Case A:** There exists one \( j \) with \( 2 \leq j \leq L \) such that

\[
\theta_j \notin \text{LAT}(\Gamma_j). \tag{101}
\]

i.e., \( \theta_j = \text{MG}_j q \) for any integer vector \( q \). We then prove that the remainders of \( M_1^{-1}v_j \) and \( M_1^{-1}(r_j - r_1) \) modulo \( \Gamma_j \) are different. Assume that \( M_1^{-1}v_j \) and \( M_1^{-1}(r_j - r_1) \) have the same remainder modulo \( \Gamma_j \), i.e.,

\[
M_1^{-1}v_j - M_1^{-1}(r_j - r_1) = \Gamma_j q \tag{102}
\]

for some integer vector \( q \). Left-multiplying \( M \) on both sides of (102), we get

\[
v_j - (r_j - r_1) = \text{MG}_j q. \tag{103}
\]

i.e., \( \theta_j = \text{MG}_j q \), which contradicts with (101). Therefore, the remainders of \( M_1^{-1}v_j \) and \( M_1^{-1}(r_j - r_1) \) modulo \( \Gamma_j \) are different. As a consequence, \( \chi_1 = \Gamma_1 \bar{n}_1 \) obtained from the system of congruences in (91) does not equal \( \Gamma_1 n_1 \) as in (88), and hence \( \bar{n}_1 \neq n_1 \).

**Case B:** For each \( 2 \leq i \leq L \), \( \theta_i \in \text{LAT}(\Gamma_i) \) but there exists at least one \( j \) with \( 2 \leq j \leq L \) such that \( \theta_j \neq 0 \); see, for example, that the \( k \)-th remainder error makes \( \theta_k \neq 0 \) according to (100), i.e., \( v_k \neq r_k - r_1 \). Since \( v_i = \theta_i + (r_i - r_1) \) and \( \theta_i \in \text{LAT}(\Gamma_i) \) for \( 2 \leq i \leq L \), we have

\[
M_1^{-1}v_i = M_1^{-1}(r_i - r_1) \mod \Gamma_i. \tag{104}
\]

So, \( \Gamma_1 n_1 \) and \( \Gamma_1 \bar{n}_1 \) have the same remainders \( \zeta_i \)'s with respect to the moduli \( \Gamma_i \)'s, and \( n_1 \) can be accurately determined, i.e., \( \bar{n}_1 = n_1 \). However, due to \( v_k \neq r_k - r_1 \), we have \( \bar{n}_k \neq n_k \) from (92). This proves the necessity.

We finally prove the two simple sufficient conditions in (95) and (96) for accurately determining the folding vectors \( n_i \)'s, respectively.

1) **Condition 1:** Assume that there exists \( \theta_i \in \text{LAT}(M) \) with \( \theta_i \neq 0 \) satisfying

\[
\theta_i = \arg \min_{\theta \in \text{LAT}(M)} \| \theta - (\Delta r_i - \Delta r_1) \| \tag{105}
\]

for each \( 2 \leq i \leq L \). Then, we have

\[
\| \theta_i \| = \| \theta_i - (\Delta r_i - \Delta r_1) - (0 - (\Delta r_i - \Delta r_1)) \| \leq \| \theta_i - (\Delta r_i - \Delta r_1) \| + \| \Delta r_i - \Delta r_1 \| \leq 2\| \Delta r_i - \Delta r_1 \| < \lambda \text{LAT}(M), \tag{106}
\]

Therefore, we have

\[
\begin{align*}
\theta_i = \arg \min_{\theta \in \text{LAT}(M)} & \| \theta - (\Delta r_i - \Delta r_1) \| \\
& < \lambda \text{LAT}(M),
\end{align*}
\]

for \( 2 \leq i \leq L \). If the condition in (93), i.e., \( \theta_i = 0 \) for \( 2 \leq i \leq L \), holds, we obtain \( v_i = r_i - r_1 \) for \( 2 \leq i \leq L \). Then, from (88) and (91), \( \Gamma_1 n_1 \) and \( \Gamma_1 \bar{n}_1 \) have the same remainders \( \zeta_i \)'s with respect to the moduli \( \Gamma_i \)'s. Therefore, we get \( \bar{n}_1 = n_1 \) for \( 1 \leq i \leq L \).
which contradicts with $\|\boldsymbol{\theta}\| \geq \frac{\lambda_{\text{LAT}(M)}}{2}$. Thus, we obtain $\boldsymbol{\theta}_i = \mathbf{0}$ for each $2 \leq i \leq L$.

2) Condition 2: When $\|\mathbf{A}_i r_i\| \leq r$ for $1 \leq i \leq L$, we have

$$\|\mathbf{A}_1 r_1 - \mathbf{A}_2 r_2 \| \leq \|\mathbf{A}_1 r_1\| + \|\mathbf{A}_2 r_2\| \leq 2r < \frac{\lambda_{\text{LAT}(M)}}{2}$$

(107)

for $2 \leq l \leq L$, which implies Condition 1.

This completes the proof of the theorem. ■

Remark 3: In the 1-dimensional case when $M$ is an arbitrary positive integer and $\mathcal{A}_i$ are pairwise coprime positive integers, we can readily verify that i) $\mathcal{A}_1 = \mathcal{A}_2 = \cdots = \mathcal{A}_L = \bigcup_{k=1}^L \mathcal{A}_k = \mathcal{N}(M\Gamma_1 \Gamma_2 \cdots \Gamma_L)$, and ii) the conditions in (103) and (104) imply each other, whereas i) and ii) are generally not observed in the MD case. Therefore, in the 1-dimensional case, from Theorem 5 it turns out that $\|\mathbf{A}_1 r_1 - \mathbf{A}_2 r_2\| < \frac{\lambda_{\text{LAT}(M)}}{2}$ for $2 \leq i \leq L$ is a necessary and sufficient condition for accurately determining the folding integers $n_i$ for $1 \leq i \leq L$, which is very similar to the robust CRT for integers in Proposition 8. The only difference is that there is one more equality sign in the left side of (75), which is due to the fact that the rounding operation instead of a norm on $\mathbb{R}$ is used in (13).

Interestingly, we observe that the result of the robust MD-CRT for integer vectors is dependent upon its reconstruction algorithm. Different reconstruction algorithms might bring about different results of the robust MD-CRT for integer vectors. In the following, we propose another reconstruction algorithm, by which a different result of the robust MD-CRT for integer vectors is derived.

By Proposition 2 we first calculate the Smith normal form of $\mathbf{M}$ in (82) as

$$\mathbf{M} = \Lambda_{\text{LAT}(\mathbf{M})} \mathbf{U},$$

(108)

where $\mathbf{U}$ and $\mathbf{V}$ are unimodular matrices, and $\Lambda$ is a diagonal integer matrix. So, we have $\mathbf{M}^{-1} = \mathbf{V}^{-1} \Lambda^{-1} \mathbf{U}$. From (86), we get

$$\begin{bmatrix}
\Gamma_1 n_1 - \Gamma_2 n_2 = \mathbf{V}^{-1} \mathbf{U}(r_2 - r_1) \\
\Gamma_1 n_1 - \Gamma_3 n_3 = \mathbf{V}^{-1} \mathbf{U}(r_3 - r_1) \\
\vdots \\
\Gamma_1 n_1 - \Gamma_L n_L = \mathbf{V}^{-1} \mathbf{U}(r_L - r_1)
\end{bmatrix}$$

(109)

Left-multiplying $\mathbf{V}^{-1}$ on both sides of all the equations in (109), we obtain

$$\begin{bmatrix}
\mathbf{V}^{-1} \Gamma_1 n_1 - \mathbf{V}^{-1} \Gamma_2 n_2 = \Lambda^{-1} \mathbf{U}(r_2 - r_1) \\
\mathbf{V}^{-1} \Gamma_1 n_1 - \mathbf{V}^{-1} \Gamma_3 n_3 = \Lambda^{-1} \mathbf{U}(r_3 - r_1) \\
\vdots \\
\mathbf{V}^{-1} \Gamma_1 n_1 - \mathbf{V}^{-1} \Gamma_L n_L = \Lambda^{-1} \mathbf{U}(r_L - r_1)
\end{bmatrix}$$

(110)

We then perform the modulo-$\mathbf{V}^{-1} \Gamma_1$ operation on both sides of the corresponding $(i - 1)$-th equation in (110) for $2 \leq i \leq L$ to get

$$\begin{bmatrix}
\mathbf{V}^{-1} \Gamma_1 n_1 \equiv 0 \mod \mathbf{V}^{-1} \Gamma_1 \\
\mathbf{V}^{-1} \Gamma_1 n_1 \equiv \Lambda^{-1} \mathbf{U}(r_2 - r_1) \mod \mathbf{V}^{-1} \Gamma_2 \\
\mathbf{V}^{-1} \Gamma_1 n_1 \equiv \Lambda^{-1} \mathbf{U}(r_3 - r_1) \mod \mathbf{V}^{-1} \Gamma_3 \\
\vdots \\
\mathbf{V}^{-1} \Gamma_1 n_1 \equiv \Lambda^{-1} \mathbf{U}(r_L - r_1) \mod \mathbf{V}^{-1} \Gamma_L
\end{bmatrix}$$

(111)

where the first equation is always available. From Lemma 3, we know that $\mathbf{V}^{-1} \Gamma_1 \Gamma_2 \cdots \Gamma_L$ is an lcm of the moduli $\mathbf{V}^{-1} \Gamma_i$ in (111). Because of $\mathbf{m} \in \mathcal{A}_i$ and $n_i = \lfloor M_i^{-1} \mathbf{m} \rfloor$, we obtain

Algorithm 2

Input: the moduli $M_i$'s and the nonzero remainders $\mathbf{r}_i$'s;
Output: the folding vectors $\mathbf{n}_i$'s.

1. Calculate $\mathbf{p}_i$ for $2 \leq i \leq L$ in (112) from $\mathbf{r}_i$ for $1 \leq i \leq L$.
2. Calculate the remainder $\mathbf{v}_i$ of $\Lambda^{-1} \mathbf{p}_i$ modulo $\mathbf{V}^{-1} \Gamma_i$ for each $2 \leq i \leq L$, i.e.,

$$\Lambda^{-1} \mathbf{p}_i \equiv \mathbf{v}_i \mod \mathbf{V}^{-1} \Gamma_i,$$

(114)

where $\mathbf{v}_i \in \mathcal{N}(\mathbf{V}^{-1} \Gamma_i)$.
3. Calculate $\mathbf{v}_1 \equiv \mathbf{V}^{-1} \Gamma_1 \mathbf{n}_1 \in \mathcal{N}(\mathbf{V}^{-1} \Gamma_1 \Gamma_2 \cdots \Gamma_L U_1)$ via the MD-CRT for integer vectors in Corollary 3 from the following system of congruences

$$\begin{aligned}
\mathbf{V}^{-1} \Gamma_1 \mathbf{n}_1 &\equiv 0 \mod \mathbf{V}^{-1} \Gamma_1 \\
\mathbf{V}^{-1} \Gamma_1 \mathbf{n}_1 &\equiv \mathbf{v}_2 \mod \mathbf{V}^{-1} \Gamma_2 \\
\mathbf{V}^{-1} \Gamma_1 \mathbf{n}_1 &\equiv \mathbf{v}_3 \mod \mathbf{V}^{-1} \Gamma_3 \\
&\vdots \\
\mathbf{V}^{-1} \Gamma_1 \mathbf{n}_1 &\equiv \mathbf{v}_L \mod \mathbf{V}^{-1} \Gamma_L
\end{aligned}$$

(115)

4. Calculate $\mathbf{n}_i = \Gamma_1^{-1} \mathbf{V} \mathbf{v}_i \in \mathcal{N}(\Gamma_1 \Gamma_2 \cdots \Gamma_L U_1)$, and then

$$\mathbf{n}_i = \Gamma_1^{-1} \mathbf{V} (\mathbf{v}_i - \Lambda^{-1} \mathbf{p}_i) \text{ for } 2 \leq i \leq L.$$
2) Condition 2: Let \( \tau \) be the remainder error bound, i.e., \( ||\Delta r_i|| \leq \tau \) for \( 1 \leq i \leq L \), and then a much simpler sufficient condition is given by
\[
\tau < \frac{\lambda_{\text{LAT}(A)}}{4}\|U\|_2.
\] (119)

where \( \|U\|_2 \) stands for the subordinate matrix norm of \( U \) based on the vector norm \( ||\cdot|| \), i.e., \( \|U\|_2 = \sup \{||Ux|| \} \).

Once the folding vectors \( n_i \)'s are accurately obtained, a robust reconstruction of \( m \) can be calculated by \( \tilde{m} = M \tilde{n}_m + \tilde{r}_m \) for any \( 1 \leq h_m \leq L \). Obviously, the reconstruction error is upper bounded by \( \tau \), i.e.,
\[
||\tilde{m} - m|| \leq \tau. \quad (120)
\]

On the basis of the above analysis, the proof of Theorem 3 is similar to that of Theorem 2 and is thus omitted here. Let us take a simple example below to show a difference between Theorem 3 and Theorem 4 (between Algorithm 1 and Algorithm 2). Their difference is caused by the non-equivalence of the conditions in (93) and (117).

**Example 2:** Let \( U = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \) be a unimodular matrix, and \( M \) in (82) be \( M = U^{-1}A \), where \( A = \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} \). According to Proposition 5 we know
\[
\text{LAT}(M) = \text{LAT}(U^{-1}A) = \text{LAT}(\begin{pmatrix} 8 & -8 \\ -8 & 16 \end{pmatrix}).
\]

Without loss of generality, we consider the first two remainder errors, i.e., \( \Delta r_1 \) and \( \Delta r_2 \). Let \( \Delta r_2 - \Delta r_1 \approx \begin{pmatrix} \Delta_1 \\ \Delta_2 \end{pmatrix} \). Then,
\[
U(\Delta r_2 - \Delta r_1) = \begin{pmatrix} 2\Delta_1 + \Delta_2 \\ \Delta_1 + \Delta_2 \end{pmatrix}.
\]

In this example, we measure the distance by the Euclidean norm of vectors in \( \mathbb{R}^2 \). On one hand, let \( \Delta_1 = 5 \) and \( \Delta_2 = -8 \). It is ready to verify that \( \theta_2 = 0 \), i.e., the condition in (117) holds for \( i = 2 \). However, \( \theta_2 \neq 0 \) in (93), since \( \Delta r_2 - \Delta r_1 \) is much closer to a non-zero lattice point, e.g., \( \begin{pmatrix} 0 \\ -8 \end{pmatrix} \), of \( \text{LAT}(M) \) than to \( 0 \). On the other hand, let \( \Delta_1 = 3 \) and \( \Delta_2 = 0 \). It is ready to verify that \( \theta_2 = 0 \), i.e., the condition in (93) holds for \( i = 2 \). However, \( \theta_2 \neq 0 \) in (117), since \( U(\Delta r_2 - \Delta r_1) \) is much closer to a non-zero lattice point, e.g., \( \begin{pmatrix} 8 \\ 0 \end{pmatrix} \), of \( \text{LAT}(A) \) than to \( 0 \).

We shall make a remark that the MD-CRT and robust MD-CRT for integer vectors studied in this paper are different from the generalized CRT and robust generalized CRT for integers in (38)–(44). In the generalized CRT and robust generalized CRT for integers, every modular is a positive integer and multiple large positive integers are reconstructed from their unordered remainder sets, where an unordered remainder set consists of the remainders of the multiple integers modulo one modular, but the correspondence between the multiple integers and their remainders in the remainder set is unknown. However, in the MD-CRT and robust MD-CRT for integer vectors, every modular is a nonsingular integer matrix and an integer vector is reconstructed from its remainders, where a remainder is an integer vector. In particular, when the moduli \( M_i \in \mathbb{Z}^{D \times D} \) for \( 1 \leq i \leq L \) are diagonal integer matrices with positive main diagonal elements, i.e., \( M_i = \text{diag}(M_i(1, 1), M_i(2, 2), \ldots, M_i(D, D)) \), with \( M_i(j, j) > 0 \) for \( 1 \leq j \leq D \) and \( 1 \leq i \leq L \), let \( R = \text{diag}(R(1, 1), R(2, 2), \ldots, R(D, D)) \) be their lcm, where \( R(j, j) \) is the lcm of \( M_i(j, j), M_j(j, j), \ldots, M_L(j, j) \) for each \( 1 \leq j \leq D \). Then, reconstruction of an integer vector \( m = (m(1), m(2), \ldots, m(D)) \) in \( \mathbb{N}(R) \) using the MD-CRT and robust MD-CRT for integer vectors is equivalent to reconstruction of all elements of the integer vector one by one using the CRT and robust CRT for integers, and is also equivalent to reconstruction of all elements of the integer vector using the generalized CRT and robust generalized CRT for integers with ordered remainder sets.

**V. Conclusion**

In this paper, the CRT and robust CRT for integers are extended to the MD case, called the MD-CRT and robust MD-CRT for integer vectors, which are expected to have numerous applications in MD signal processing. More specifically, we first derive the MD-CRT for integer vectors with respect to a general set of moduli, which allows to uniquely reconstruct an integer vector from its remainders, if the integer vector is in the fundamental cell of the lattice generated by an lcm of all the moduli. When the moduli are given in some special forms, we further present explicit reconstruction formulae. In addition, we provide some results of the robust MD-CRT for integer vectors under the assumption that the remaining integer matrices of all the moduli left divided by their gcd are pairwise commutative and coprime. Accordingly, we propose two different reconstruction algorithms, by which two different conditions on the remainder error bound for the reconstruction robustness are separately obtained and proved to be related to a quarter of the minimum distance of the lattice generated by the gcd of all the moduli or the Smith normal form of the gcd. The robust MD-CRT for integer vectors with respect to a general set of moduli is still an open problem for future research.

**References**

[1] N. S. Szabo and R. I. Tanaka, *Residue Arithmetic and its Application to Computer Technology*, New York: McGraw-Hill, 1967.

[2] H. Krishna, B. Krishna, K.-Y. Lin, and J.-D. Sun, *Computational Number Theory and Digital Signal Processing: Fast Algorithms and Error Control Techniques*, Boca Raton, FL: CRC, 1994.

[3] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, Singapore: World Scientific, 1999.

[4] H. Krishna, K.-Y. Lin, and B. Krishna, “Rings, fields, the Chinese remainder theorem and an extension—Part II: applications to digital signal processing,” *IEEE Trans. Circuits Syst. II*, vol. 41, no. 10, pp. 656-668, 1994.

[5] R. C. Agarwal and C. S. Burrus, “Number theoretic transforms to implement fast digital convolution,” *Proc. IEEE*, vol. 63, no. 4, pp. 550-560, 1975.

[6] C.-F. Hsiao, Y. Chen, and C.-Y. Lee, “A generalized mixed-radix algorithm for memory-based FFT processors,” *IEEE Trans. Circuits Syst. II*, vol. 57, no. 5, pp. 553-574, 2016.

[7] A. Christlieb, D. Lawlor, and Y. Wang, *A multiscale sub-linear time Fourier algorithm for noisy data*, *Appl. Comput. Harmon. Anal.*, vol. 40, no. 3, pp. 533-574, 2016.

[8] P. P. Vaidyanathan and P. Pal, “Sparse sensing with co-prime samplers and arrays,” *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 573-586, 2011.

[9] S. Qin, Y. D. Zhang, and M. G. Amin, “Generalized coprime array configurations for direction-of-arrival estimation,” *IEEE Trans. Signal Process.*, vol. 63, no. 6, pp. 1377-1390, 2015.
X.-G. Xia and G. Wang, “Phase wrapping and a robust Chinese remainder theorem,” IEEE Trans. Signal Process., vol. 67, no. 11, pp. 2998-3010, 2019.

C. H. Li, L. Gan, and C. Ling, “Coprime sensing via Chinese remainder theorem over quadratic fields–Part I: Array designs,” IEEE Trans. Signal Process., vol. 67, no. 11, pp. 2911-2922, 2019.

X.-G. Xia and G. Wang, “Phase wrapping and a robust Chinese remainder theorem,” IEEE Signal Process. Lett., vol. 14, no. 4, pp. 247-250, 2007.

X. W. Li, H. Liang, and X.-G. Xia, “A robust Chinese remainder theorem with its applications in frequency estimation from undersampled waveforms,” IEEE Trans. Signal Process., vol. 57, no. 11, pp. 4314-4322, 2009.

W. J. Wang and X.-G. Xia, “A closed-form robust Chinese remainder theorem and its performance analysis,” IEEE Trans. Signal Process., vol. 58, no. 11, pp. 5556-5566, 2010.

G. Li, J. I. Xu, Y.-N. Peng, and X.-G. Xia, “Location and imaging of moving targets using non-uniform linear antenna array,” IEEE Trans. Aerosp. Electron. Syst., vol. 43, no. 3, pp. 1214-1220, 2007.

Y. M. Zhang and M. Amin, “MIMO radar exploiting narrowband frequency-hopping waveforms.” In Proc. 16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, 2008.

Z. Yuan, Y. Deng, F. Li, R. Wang, G. Liu, and X. Han, “Multichannel InSAR DEM reconstruction through improved closed-form robust Chinese remainder theorem,” IEEE Geosci. Remote Sens. Lett., vol. 10, no. 6, pp. 1314-1318, 2013.

B. Silva and G. Fraidenreich, “Performance analysis of the classic and robust Chinese remainder theorems in pulsed Doppler radars,” IEEE Trans. Signal Process., vol. 66, no. 18, pp. 4898-4903, 2018.

J. Xu, Z.-Z. Huang, Z. Wang, L. Xiao, X.-G. Xia, and T. Long, “Radial velocity retrieval for multichannel SAR moving targets with time-space Doppler deambiguity,” IEEE Trans. Geosci. Remote Sens., vol. 56, no. 1, pp. 35-48, 2018.

G. Xu, “On solving a generalized Chinese remainder theorem in the presence of remainder errors.” In Conference on Geometry, Algebra. Number Theory, and their Information Technology Applications (GANITA), pp. 461-476, Springer, Cham, 2016.

B. Yang, W. J. Wang, X.-G. Xia, and Q. Yin, “Phase detection based range estimation with a dual-band robust Chinese remainder theorem,” Sci. China Inf. Sci., vol. 57, no. 2, pp. 1-9, 2014.

W. J. Wang, X. P. Li, W. Wang, and X.-G. Xia, “Maximum likelihood estimation based robust Chinese remainder theorem for real numbers and its fast algorithm,” IEEE Trans. Signal Process., vol. 63, no. 13, pp. 3317-3331, 2015.

L. Xiao, X.-G. Xia, and W. J. Wang, “Multi-stage robust Chinese remainder theorem,” IEEE Trans. Signal Process., vol. 62, no. 18, pp. 4772-4785, 2014.

L. Xiao, X.-G. Xia, and H. Y. Huo, “Towards robustness in residue number systems,” IEEE Trans. Signal Process., vol. 65, no. 6, pp. 1497-1510, 2017.

K. Falaggi, D. P. Towers, and C. E. Towers, “Method of excess fractions with application to absolute distance metrology: Analytical solution,” Appl. Optics, vol. 52, no. 23, pp. 5758-5765, 2013.

S. Tang, X. Zhang, and D. Tu, “Micro-phase measuring profilometry: Its sensitivity analysis and phase unwrapping,” Opt. Lasers Eng., vol. 72, pp. 47-57, 2015.

T. Petković, T. Pribanić, and M. Donlić, “Temporal phase unwrapping using orthographic projection,” Opt. Lasers Eng., vol. 90, pp. 34-47, 2017.

W. C. Li, X. Z. Wang, and B. Moran, “Wireless signal travel distance estimation using non-coprime wavelengths,” IEEE Signal Process. Lett., vol. 24, no. 1, pp. 27-31, 2017.

A. Ahlqvar, R. McKilliam, R. Subramanian, and A. Pollok, “Selecting wavelengths for least squares range estimation,” IEEE Trans. Signal Process., vol. 64, no. 20, pp. 5205-5216, 2016.

C. Chi, H. Vishnu, K. T. Beng, and M. Chitre, “Utilizing orthogonal co-prime signals for improving broadband acoustic Doppler current profilers,” IEEE J. Oceanic Eng., DOI: 10.1109/JOE.2019.2925912.

C. Chi, H. Vishnu, K. T. Beng, and M. Chitre, “Robust resolution of velocity ambiguity for multifrequency pulse-to-pulse coherent Doppler sonars,” IEEE J. Oceanic Eng., DOI: 10.1109/JOE.2019.2925912.

G. Campobello, A. Leonardi, and S. Palazzo, “Improving energy saving and reliability in wireless sensor networks using a simple CRF-based packet-forwarding solution,” IEEE/ACM Trans. Netw., vol. 20, no. 1, pp. 191-205, 2012.

S. Chessa and P. Maestrini, “Robust distributed storage of residue encoded data,” IEEE Trans. Inf. Theory, vol. 58, no. 12, pp. 7280-7294, 2012.

Y.-S. Su, “Topology-transparent scheduling via the Chinese remainder theorem,” IEEE/ACM Trans. Netw., vol. 3, no. 5, pp. 1416-1429, 2015.