associated in a one-to-one fashion to the d-tuple $(\ell_1, \ell_2, \ldots, \ell_d)$ of its residue classes in $\mathbb{Z}/N_1\mathbb{Z}, \mathbb{Z}/N_2\mathbb{Z}, \ldots, \mathbb{Z}/N_d\mathbb{Z}$.

The proof of the CRT goes as follows. Let

$$Q_j = \frac{N}{N_j} = \prod_{i \neq j} N_i.$$

Since g.c.d. $(N_j, Q_j) = 1$ there exist integers n_j and q_j such that

$$n_j N_j + q_j Q_j = 1, \qquad j = 1, \ldots, d,$$

then the integer

$$\ell = \sum_{i=1}^{d} \ell_i q_i Q_i \bmod N$$

is the solution. Indeed,

$$\ell \equiv \ell_j q_j Q_j \bmod N_j$$

because all terms with $i \neq j$ contain N_j as a factor; and

$$q_j Q_j \equiv 1 \bmod N_j$$

by the defining relation for q_j.

It may be noted that

$$(q_i Q_i)(q_j Q_j) \equiv 0 \qquad \bmod N \text{ for } i \neq j,$$
$$(q_j Q_j)^2 \equiv q_j Q_j \qquad \bmod N, \quad j = 1, \ldots, d,$$

so that the $q_j Q_j$ are mutually orthogonal *idempotents* in the ring $\mathbb{Z}/N\mathbb{Z}$, with properties formally similar to those of mutually orthogonal *projectors onto subspaces* in linear algebra. The analogy is exact, since by virtue of the CRT the ring $\mathbb{Z}/N\mathbb{Z}$ may be considered as the direct product

$$\mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \ldots \times \mathbb{Z}/N_d\mathbb{Z}$$

via the two mutually inverse mappings:

(i) $\ell \longmapsto (\ell_1, \ell_2, \ldots, \ell_d)$ by $\ell \equiv \ell_j \bmod N_j$ for each j;

(ii) $(\ell_1, \ell_2, \ldots, \ell_d) \longmapsto \ell$ by $\ell = \sum_{i=1}^{d} \ell_i q_i Q_i \bmod N$.

The mapping defined by (ii) is sometimes called the 'CRT reconstruction' of ℓ from the ℓ_j.

These two mappings have the property of sending sums to sums and products to products, *i.e*:

(i) $\ell + \ell' \longmapsto (\ell_1 + \ell'_1, \ell_2 + \ell'_2, \ldots, \ell_d + \ell'_d)$
$\ell\ell' \longmapsto (\ell_1\ell'_1, \ell_2\ell'_2, \ldots, \ell_d\ell'_d)$

(ii) $(\ell_1 + \ell'_1, \ell_2 + \ell'_2, \ldots, \ell_d + \ell'_d) \longmapsto \ell + \ell'$
$(\ell_1\ell'_1, \ell_2\ell'_2, \ldots, \ell_d\ell'_d) \longmapsto \ell\ell'$

(the last proof requires using the properties of the idempotents $q_j Q_j$). This may be described formally by stating that the CRT establishes a *ring isomorphism*:

$$\mathbb{Z}/N\mathbb{Z} \cong (\mathbb{Z}/N_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/N_d\mathbb{Z}).$$

1.3.3.2.2.3. *The prime factor algorithm*

The CRT will now be used to factor the N-point DFT into a tensor product of d transforms, the jth of length N_j.

Let the indices k and k^* be subjected to the following mappings:

(i) $k \longmapsto (k_1, k_2, \ldots, k_d), k_j \in \mathbb{Z}/N_j\mathbb{Z}$, by $k_j \equiv k \bmod N_j$ for each j, with reconstruction formula

$$k = \sum_{i=1}^{d} k_i q_i Q_i \bmod N;$$

(ii) $k^* \longmapsto (k_1^*, k_2^*, \ldots, k_d^*), k_j^* \in \mathbb{Z}/N_j\mathbb{Z}$, by $k_j^* \equiv q_j k^* \bmod N_j$ for each j, with reconstruction formula

$$k^* = \sum_{i=1}^{d} k_i^* Q_i \bmod N.$$

Then

$$k^* k = \left(\sum_{i=1}^{d} k_i^* Q_i\right)\left(\sum_{j=1}^{d} k_j q_j Q_j\right) \bmod N$$
$$= \sum_{i,j=1}^{d} k_i^* k_j Q_i q_j Q_j \bmod N.$$

Cross terms with $i \neq j$ vanish since they contain all the factors of N, hence

$$k^* k = \sum_{j=1}^{d} q_j Q_j^2 k_j^* k_j \bmod N$$
$$= \sum_{j=1}^{d} (1 - n_j N_j) Q_j k_j^* k_j \bmod N.$$

Dividing by N, which may be written as $N_j Q_j$ for each j, yields

$$\frac{k^* k}{N} = \sum_{j=1}^{d} (1 - n_j N_j) \frac{Q_j}{N_j Q_j} k_j^* k_j \bmod 1$$
$$= \sum_{j=1}^{d} \left(\frac{1}{N_j} - n_j\right) k_j^* k_j \bmod 1,$$

and hence

$$\frac{k^* k}{N} \equiv \sum_{j=1}^{d} \frac{k_j^* k_j}{N_j} \bmod 1.$$

Therefore, by the multiplicative property of $e(.)$,

$$e\left(\frac{k^* k}{N}\right) \equiv \bigotimes_{j=1}^{d} e\left(\frac{k_j^* k_j}{N_j}\right).$$

Let $\mathbf{X} \in L(\mathbb{Z}/N\mathbb{Z})$ be described by a one-dimensional array $X(k)$ indexed by k. The index mapping (i) turns $\mathbf{X}$ into an element of $L(\mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_d\mathbb{Z})$ described by a d-dimensional array $X(k_1, \ldots, k_d)$; the latter may be transformed by $\bar{F}(N_1) \bigotimes \ldots \bigotimes \bar{F}(N_d)$ into a new array $X^*(k_1^*, k_2^*, \ldots, k_d^*)$. Finally, the one-dimensional array of results $X^*(k^*)$ will be obtained by reconstructing k^* according to (ii).

The prime factor algorithm, like the Cooley–Tukey algorithm, reindexes a 1D transform to turn it into d separate transforms, but the use of coprime factors and CRT index mapping leads to the further gain that *no twiddle factors* need to be applied between the successive transforms (see Good, 1971). This makes up for the cost of the added complexity of the CRT index mapping.

The natural factorization of N for the prime factor algorithm is thus its factorization into prime powers: $\bar{F}(N)$ is then the tensor product of separate transforms (one for each prime power factor $N_j = p_j^{\nu_j}$) whose results can be reassembled without twiddle factors. The separate factors p_j within each N_j must then be dealt with by another algorithm (*e.g.* Cooley–Tukey, which does require twiddle factors). Thus, the DFT on a prime number of points remains undecomposable.

1.3.3.2.3. *The Rader algorithm*

The previous two algorithms essentially reduce the calculation of the DFT on N points for N composite to the calculation of smaller DFTs on prime numbers of points, the latter remaining irreducible. However, Rader (1968) showed that the p-point DFT for p an odd

references