(1) Chinese Remainder Theorem

Let \( m_i \) be \( K \) positive integers greater than 1 and relatively prime in pairs.

The set of linear congruencies

\[
X \equiv r_i \mod m_i \quad \text{mod} \quad 1
\]

has a unique solution modulo \( M \), with

\[
M = \prod_{i=1}^{k} m_i \quad \text{mod} \quad 2
\]
The proof of this theorem is established by using the relations

\[ X = \sum_{i=1}^{k} (M / m_i) T_i r_i \mod M \]  

where

\[ (M/m_i) T_i \equiv 1 \mod m_i \]

\[ \text{Note (i) } (M/m_j) \equiv 0 \mod m_j \text{ for } j \neq i \]

\[ \text{(ii) } (M/m_i) T_i r_i \equiv r_i \mod m_i \]
\[ X \mod 3 = 2 \]
\[ X \mod 4 = 1 \implies X = ? \]
\[ X \mod 5 = 3 \]
\[ m_1 = 3, \ m_2 = 4, \ m_3 = 5 \ \text{and} \ M = 60 \]

\[ M / m_1 = 20 \equiv 0 \mod m_2 \text{ or } m_3 \quad \text{and} \quad T_1(M / m_1) \equiv 1 \mod 3 \]
\[ M / m_2 = 15 \equiv 0 \mod m_1 \text{ or } m_3 \quad \text{and} \quad T_2(M / m_2) \equiv 1 \mod 4 \]
\[ M / m_3 = 12 \equiv 0 \mod m_2 \text{ or } m_3 \quad \text{and} \quad T_3(M / m_3) \equiv 1 \mod 5 \]
\[ \implies 20T_1 \equiv 15T_2 \equiv 12T_3 \equiv 1 \implies T_1 = 2, \ T_2 = 3, \text{ and } T_3 = 3 \]
Therefore,

\[ \frac{M}{m_1} \ T_1 \ r_1 \ \frac{M}{m_2} \ T_2 \ r_2 \ \frac{M}{m_3} \ T_3 \ r_3 \]

\[ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \]

\[ X = (20 \times 2 \times 2) + (15 \times 3 \times 1) + (12 \times 3 \times 3) \mod 60 \]

\[ = 53 \]

\[ = \sum_{i=1}^{3} \left( \frac{M}{m_i} \right) T_i r_i \ mod \ M \]
Chinese Remainder Theorem (CRT) can be used to define Residue Number System (RNS) which allow us to perform high-speed arithmetic operations without carry propagation from digit to digit.

\[ a = (a_1, a_2, \cdots a_k) \text{, where } a_i \equiv a \mod m_i \]

\[ a \odot b = (a_i \odot b_i)_{i=1}^{k} = (r_1, r_2, \cdots, r_k) = \sum_{i=1}^{K} (\frac{M}{m_i}) T_i r_i \mod M \]

\[ \text{no carry propagation!!} \]
(ii) Permutation

consider the set of $M$ integers $n$, with $n = 0, 1, \ldots, M - 1$

If we multiply modulo $M$ each element $n_i$ of $n$ by an integer $a$, we obtain a set of $M$ numbers $b_i$ defined by

$$b_i \equiv a \cdot n_i \mod M$$

in which $n_i$ are all distinct.
We would like the $b_i$ to be also all distinct in such a way that when the $n_i$'s span the $M$ values $0, 1, \ldots, M - 1$, the $b_i$'s span the same values, although in a different order. \( \rightarrow \) permutation!! It can be proved by basic number theory that the solution of (5) is unique if

\[
(a, M) = 1, \quad (6)
\]
i.e., $a$ and $M$ co-prime to each other!
Ex: consider the permutation defined by

\[ b \equiv 3 \cdot n \mod 7 , \quad (3,7) = 1 \]

\[ n = 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \]

\[ b = 0 \ 3 \ 6 \ 2 \ 5 \ 1 \ 4 \]

Remark:

Permutations are often used in DSP to reorder a set of data samples for certain purposes.
Ex: Simplify the mapping of CRT

\[ n = \sum_{i=1}^{k} \left( \frac{M}{m_i} \right) T_i n_i \mod M, \text{ where } n_i = n \mod m_i \]

for \( K = 2 \), we have \( n = m_2 \cdot T_1 \cdot n_1 + m_1 \cdot T_2 \cdot n_2 \mod M \)

Since \( T_1 \) and \( T_2 \) are mutually prime with \( m_1 \) and \( m_2 \), respectively, \( m_2 \cdot n_1 T_1 \) and \( m_1 \cdot n_2 T_2 \) can be viewed as 2 permutations \( n_1 T_1 \mod m_1 \) and \( n_2 T_2 \mod m_2 \) of 2 sets of \( m_1 \) points and \( m_2 \) points, respectively.
Hence the mapping defined by \( n = m_2 \cdot T_1 \cdot n_1 + m_1 \cdot T_2 \cdot n_2 \mod M \) can be replaced by the simpler mapping
\[
n = m_2 (n_1 T_1) + m_1 (n_2 T_2) \mod M
\]
\[
= m_2 n'_1 + m_1 n'_2 \mod M
\]
\[
= m_2 n_1 + m_1 n_2 \mod M
\]
since \( n'_i \)'s span the same values of \( n_i \)'s.
And, in the case of more than two factors,
\[
n = \sum_{i=1}^{K} \left( \frac{M}{m_i} \right) n_i \mod M
\]
\( \Rightarrow \) The computation of the inverses \( T_i \) is no longer required!!
Ex: $M = 2 \times 3 = m_1 \times m_2$

The sequence $n$ is given by $\{0,1,2,3,4,5,\}$

Since $T_1 = 1$ and $T_2 = 2$,

Eqn. (7) yields $n = 3 \times 1 \times n_1 + 2 \times 2 \times n_2 = 3n_1 + 4n_2 \mod 6$

while Eqn. (8) gives $3n_1 + 2n_2 \mod 6$
When the pair \((n_1, n_2)\) takes successively the values
\((0,0), (1,0), (0,1), (1,1), (0,2),\) and \((1,2)\)
the sequence becomes

(i) \[ n = 3n_1 + 4n_2 \mod 6 \rightarrow \{0,3,4,1,2,5\} \]
(ii) \[ n = 3n_1 + 2n_2 \mod 6 \rightarrow \{0,3,2,5,4,1\} \]

thus, both approaches span the complete set of values of \(n\),
although in a different order.
(3) Primitive Roots

Definition. \( \phi(M) \): Euler's Totient Function

The number of integers smaller than \( M \) and relatively prime to \( M \)

\[
\begin{align*}
\phi(1) &= 1 \\
\phi(P) &= P - 1, \ P: \text{a prime} \\
\phi(P^r) &= P^{r-1} (p - 1) = P^r (1 - \frac{1}{p})
\end{align*}
\]

If \( a \) and \( b \) are two mutually prime integers, then

\[
\phi(a, b) = \phi(a) \cdot \phi(b)
\]
In general, for \( N = P_1^{r_1} \cdot P_2^{r_2} \cdots P_k^{r_k} \), then

\[
\phi(N) = N \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)
\]

properties of \( \phi(N) \):

\[
\sum_{d \mid N} \phi(d) = \sum_{d \mid N} \phi\left(\frac{N}{d}\right) = N
\]
Euler's Theorem

If \((a, M) = 1\), then \(a^{\phi(M)} \equiv 1 \mod M\)

If \(P\) is a prime, then for every integer \(a\)
\(a^{P-1} \equiv 1 \mod P\)
An interesting application of Euler's theorem can be found for the CRT reconstruction:

one of the difficulties in using CRT consists in evaluating the $K$ inverses $T_i$ modulo $m_i$. 
By using Euler's theorem, the CRT reconstruction defined by

$$X = \sum_{i=1}^{k} \frac{M}{m_i} T_i r_i \mod M \text{ and } (\frac{M}{m_i}) T_i \equiv 1 \mod m_i$$

Can be replaced by a much simpler formulation which does not require the computation of inverses $T_i$, that is

$$X = \sum_{i=1}^{K} \left(\frac{M}{m_i}\right)^{\phi(m_i)} r_i \mod M$$
Egn. 16 is established by noting that
\[
\left( \frac{M}{m_i} \right)^{\phi(m_u)} \equiv 0 \mod m_u \quad \text{for } i \neq u
\]
and that
\[
\left( \frac{M}{m_u} \right)^{\phi(m_u)} \equiv 1 \mod m_u , \quad \text{by Euler's theorem.}
\]
Definition. The order of an integer $a$.

If $r$ is the smallest positive integer such that $a^r \equiv 1 \mod M$,
the sequence of integers $a^n \mod M$ will be periodic with period $r$.
$r$ is called the order of the integer $a$. 
From Euler's theorem that if \((a, M) = 1\), \(r = \phi(M)\)

Now if \((a, M) = d \neq 1\), we have \((\frac{a}{d}, \frac{M}{d}) = 1\) and \(r_1 = \phi(\frac{M}{d})\)

Since \(\phi(\frac{M}{d}) < \phi(M)\), the period is maximum for \((a, M) = 1\).

We call the element \(g\) which generates a sequence of length \(\phi(M)\) a primitive root. An element \(g'\) generating a shorter cyclic sequence of length \(r < \phi(M)\) will be simply called a root of order \(r\).
Theorem 1: 1. If $g$ is a root of order $r \mod M$, the $r$ integers 
$g^0, g^1, \ldots, g^{r-1}$ are incongruent (i.e., distinct) modulo $M$.

2. If $(g, M) = 1$ and $g^b \equiv 1 \mod M$, the order $r$ of the integer $g$ must divide $b$.

3. If $(g, M) = 1$, the order $r$ of the integer $g$ must divide $\phi(M)$.

4. If $r \mid (p-1)$, with $P$ an odd prime, there are $\phi(r)$ incongruent integers which have order $r$ modulo $P$.

once a primitive root $g$ has been found, any root of order $r_i$, where $r_i \mid r$, can easily be found by raising $g$ to the power $r/r_i$. 
Mersenne and Fermat Numbers

Mersenne numbers are defined by

\[ M_p = 2^p - 1, \text{ with } p \text{ an odd prime.} \]

Fermat numbers are defined by

\[ F_t = 2^{2^t} + 1, \text{ with } t \text{ a positive integer.} \]
These numbers are important in DSP because arithmetic operation modulo Mersenne and Fermat numbers can be implemented relatively simple in digital hardware.

\[
a = \sum_{i=0}^{B-1} a_i 2^i, \quad a_i \in \{0,1\}
\]

then

\[
a \mod M_p = \sum_{i=0}^{P-1} \left( \sum_{K} a_{i+KP} \right) 2^i, \quad \text{when } P < B
\]
When two integers $a$ and $b$, defined modulo $M_P$, are added together, this generates a $(P + 1)$ – bit result, which is reduced by modulo $M_P$ by simply adding the most significant carry to the least significant bit position.

⇒ operations modulo $M_P$ are equivalent to the familiar one's complement arithmetic.

**Question**: How about the operations modulo $F_t$?

**Theorems**: (i) All Mersenne numbers are relatively prime. (ii) All Fermat numbers are mutually prime.
Number Theoretic Transform:
DFT defined in a finite field.

Example.

Since \( 2^{2^t} \equiv -1 \mod F_t \)
we have \( 2^{2^{t+1}} \equiv 1 \mod F_t \)
which means 2 is the \( 2^{t+1} \) – th root of unity mod \( F_t \)
Thus we can define a length - $2^{t+1}$ DFT in the field mod $F_t$ for $t = 0,1,2,3,4$. like

$$\overline{X}_K = \sum_{n=0}^{2^{t+1}} x_n 2^{nK} \mod F_t, \quad t = 0,1,2,3,4$$

for integer sequence $x_n$ defined over modulo $F_t$.
The convolution of two integer sequences $x_n$ and $y_n$ of length $2^{t+1}$ can now be computed by

$$C_n = \frac{1}{2^{t+1}} \sum_{K=0}^{2^{t+1}-1} X_K \cdot \overline{Y_K} \cdot 2^{-nK} \mod F_t$$

under the condition that $|C_n| < \frac{1}{2} F_t$.
In general, if $g$ is an $N$-th root of $GF(P)$, a DFT can be defined in $GF(P)$ as

$$X_K = \sum_{n=0}^{N-1} x_n \cdot g^{nK} \mod P$$

Prime-Factor Fast Fourier Transform Algorithms

\[ N = N_1 \cdot N_2, \text{ where } N_1 \text{ and } N_2 \text{ are co-prime to each other, i.e., } \gcd(N_1, N_2) = 1. \]

\[ \begin{align*}
  n \rightarrow (n_1, n_2) & \quad \text{where} \quad n_i = n \mod N_i \\
  K \rightarrow (K_1, K_2) & \quad \text{where} \quad K_i = K \mod N_i
\end{align*} \]

Based on the Chinese Remainder Theorem (CRT), we have
\begin{equation}
\begin{aligned}
n &= N_1 n_2 + N_2 n_1 \mod N, \quad n_1, K_1 = 0, \cdots, N_1 - 1 \\
K &= N_1 K_2 + N_2 K_1 \mod N, \quad n_2, K_2 = 0, \cdots, N_2 - 2 \\
\overline{X}_{N_1 K_2 + N_2 K_1} &= \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{N_1 n_2 + N_2 n_1} w_N^{(N_1 n_2 + N_2 n_1)(N_1 K_2 + N_2 K_1)} \\
\end{aligned}
\end{equation}

\begin{equation}
\begin{aligned}
&= w_{N_2}^{N_1 n_2 K_2} \cdot w_{N_1}^{N_2 n_1 K_1} \\
\end{aligned}
\end{equation}
\[
\overline{X}_{N_1K_2+N_2K_1} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{N_1n_2+N_2n_1} W_{N_2}^{N_1n_2K_2} \cdot W_{N_1}^{N_2n_1K_1}
\]

Eqn. 30 is a 2-D DFT of size \(N_1 \times N_2\) but with the exponents \(n_1K_1\) and \(n_2K_2\) permutated respectively, by \(N_1\) and \(N_2\)
In order to obtain the 2-D DFT in the conventional lexicographic order, it is convenient to replace $K_1$ and $K_2$ by their permuted values $t_2K_1$ and $t_2K_2$ such that $N_2t_2 \equiv 1 \mod N_1$ and $N_1t_1 \equiv 1 \mod N_2$. This is equivalent to replacing the mapping of $K = N_1K_2 + N_2K_1 \mod N$ with its Chinese Remainder equivalent

$$K = N_1t_1K_2 + N_2t_2K_1 \mod N$$
Then \(30\) can be converted to

\[
\bar{X}_{N_1 t_1 K_2 + N_2 t_2 K_1} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{N_1 n_2 + N_2 n_1} w_{N_2}^{n_2 K_2} w_{N_1}^{n_1 K_1}
\]

which is the usual representation of a DFT of size \(N_1 \times N_2\)
Thus, for $N = N_1 \cdot N_2$, $(N_1, N_2) = 1$, by using for $n$ the permutation defined by

$$n = N_1 n_2 + N_2 n_1 \mod N,$$

and for $K$ the Chinese Remainder correspondence defined by

$$K = N_1 t_1 K_2 + N_2 t_2 K_1 \mod N$$

(or vice versa), we are able to map a 1-D DFT (convolution) of length $N_1 \cdot N_2$ into a 2-D DFT (convolution) of size $N_1 \times N_2$.
The same method can be used recursively to define a one-to-many multi-dimensional mapping. More precisely, if $N$ is the product of $d$ mutually prime factors $N_i$, with

$$N = \prod_{i=1}^{d} N_i$$

then the 1-D DFT of length $N$ is converted into a $d$-D DFT of size $N_1 \times N_2 \times \cdots \times N_d$ by the change of indices.

\[ n = \sum_{i=1}^{d} Nn_i / N_i \mod N, \quad n_i = 0,1, \ldots, N_i - 1 \]  
\[ K = \sum_{i=1}^{d} Nt_i K_i / N_i \mod N, \quad K_i = 0,1, \ldots, N_i - 1 \]

where \( t_i \) is given by
\[ Nt_i / N_i \equiv 1 \mod N_i \]

It can be verified easily that, in the product of \( n \cdot K \mod N \), with
\( n \) and \( K \) defined by (33) and (34), all cross-products \( n_i K_u \) for \( i \neq u \) cancel, so that
\[ nK \equiv \sum_{i=1}^{d} N n_i K_i / N_i \mod N \]

Therefore, a 1-D to d-D mapping can be established.
We now consider a 2-D DFT \( \bar{X}_{K_1, K_2} \) of size \( N_1 \times N_2 \), with \( (N_1, N_2) = 1 \)

\[
\bar{X}_{K_1, K_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} X_{n_1, n_2} W_{N_2}^{n_2 K_2} \cdot W_{N_1}^{n_1 K_1} 
\]

\[
= \sum_{n_2=0}^{N_2-1} W_{N_2}^{n_2 K_2} \left\{ \sum_{n_1=0}^{N_1-1} X_{n_1, n_2} W_{N_1}^{n_1 K_1} \right\} 
\]

\[
\bar{X}_{n_2, K_1} 
\]
This illustrates that $\overline{X}_{\kappa_1,\kappa_2}$ can be evaluated by first computing one DFT of $N_1$ terms for each value of $n_2$. This gives $N_1$ sets of $N_2$ points $\overline{X}_{n_2,\kappa_1}$ which are the input sequences to $N_1$ DFTs of $N_2$ points.

$\Rightarrow \overline{X}_{\kappa_1,\kappa_2}$ is calculated with $N_2$ DFTs of length $N_1$ plus $N_1$ DFTs of length $N_2$
Assume that $M_1, M_2$ and $A_1, A_2$ are the numbers of multiplications and additions required for the calculation of DFTs of lengths $N_1$ and $N_2$, respectively. Then, we have

\[ M = N_1 M_2 + N_2 M_1 \]
\[ A = N_1 A_2 + N_2 A_1 \]

In general, for $N = \prod_{i=1}^{d} N_i$, $(N_i, N_l) = 1$ for $i \neq l$