ON SOME RESULTS OF NUMBER THEORETIC TRANSFORM (NTT) - PERIODIC SIGNALS

M.TOUBA*, A. BENNIA, S. TOUBA***

*University of Biskra , B.O Box 145 RP, 07000 Biskra, Algeria
**University of Constantine 25000 , Constantine, Algeria

ABSTRACT

The interest given to the application of Number Theoretic Transforms (NTT's) to digital signal processing has not ceased to grow. These transformations are used to improve convolutions, where arithmetic operations give a modulo an integer results. In order to understand the domain of the NTT, we have to show their powerful properties and exploit them in different applications such as in signal processing.

KEY WORDS: Number Theoretic transforms, NTT, Fermat numbers, Mersenne's numbers.

1 INTRODUCTION

In the last few years, techniques of digital signal processing were used in many applications, and that grace, mainly, to transformations of signals that made easy the task.

When the computers became famous, the information given was the subject of multiple improvements to decrease the execution time, especially, which allowed the appearance, for example, of the ***Fast Fourier transform (*FFT)** [1].

However, the FFT, in spite of its many advantages, was criticized for two particular problems: errors rounding and truncation, which had with the nature of the numbers that it uses, and the generation or the storage of complicated basic functions (*cosine* and *sine*), used in the development of its algorithm.

For these reasons, the Number Theoretic Transforms (NTT), made their appearance and were studied with an aim of replacing the FFT as a tool of signal processing.

These transformations, based on rules of the number theory, were introduced by **AGARWAL *et al.*** [2,3,4] at the beginning of the seventies. They use the operations of congruencies modulo a prime number, thus eliminating the problem of error rounding or truncation.

However, in spite of the advantages of this transformation (exactness of the results), the NTT did not know a success similar to that of the FFT because of the interpretation problem of the field that it create, which is not the case for the frequency field, created by the FFT

2 NUMBER THEORETIC TRANSFORM

This theory introduced by AGARWAL et al., is used as well to improve convolutions where arithmetic operations give modulo M results [5, 11]. Many advantages are presented by the use of modulo M arithmetic, such as to avoid introducing roundness errors and to build very effective algorithms for the calculation of convolutions.

2.1 Definition

This transformation bases on the modulo-M properties. Hence, the good choice of M may gives properties similar to those of the Discrete Fourier Transform (DFT).

Choice of the Modulus: The choice of the modulus has to respond the following conditions:

2.1.1 Simplicity of calculations

Because a division is coarse for $M=2^N$, and it is very simple when $M=2^N+1$ (a carry is added or subtracted to obtain the result).

2.1.2 The modulus must be big enough

So that the result of the convolution is represented well in these modulo M arithmetic.

2.1.3 Existence of suitable algebraic properties

In order to have a transformation similar to the DFT, the complete residu system should contain periodic elements to elaborate fast algorithms. So, it is necessary to have an element such as

$$a^N \equiv 1 \bmod M \qquad ,(a,N) \in \mathbf{N}^2$$

And $a^t \equiv 1 \bmod M$, *for* $t < N$, $t \in \mathbf{N}$

Hence, the NTT of a signal *x(n)* can be defined as follows:

$$NTT\left[x(n)\right] = X(k) = \sum_{n=0}^{N-1} x(n)\alpha^{nk} \mod M, \quad k = 0,1,\ldots\ldots,N-1 \tag{1}$$

Its inverse can be given by :

$$NTT^{-1}\left[X(k)\right] = x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)\alpha^{-nk} \mod M, \quad n = 0,1,\ldots\ldots,N-1 \tag{2}$$

A set of conditions must be verified:

It is necessary, at first, that *N* and the powers of *α* have inverses. But *N* admits an inverse if *(N,M)=1*. (*N,M*) is the greatest common divisor of *N* and *M*

We must have *(α, M) = 1* and $ord_M(\alpha) = N$, where $ord_M(\alpha)$ is the order of *α* mod(*M*).

Furthermore, the existence of the NTT inverse is conditioned by the equation:

$$\sum_{k=0}^{N-1} \alpha^{ik} = N\,\delta(i) \quad where \quad \begin{cases} \delta(i) = 1 & if \ \ i \equiv 0 \bmod M \\ \delta(i) = 0 & if \ \ i \not\equiv 0 \bmod M \end{cases} \tag{3}$$

But, these conditions are satisfied for any prime number

P (*N\(P-1)* , and if *M* is prime, *N* has to divide *(M-1)*).

2.2 Parameters quality

The first examined moduli were the *MERSENNE's* numbers of the form: $M = 2^t - 1$ where *t* is a prime number.

The most used factors (α) are:

α =2, *α=-2*, for *N=t*, and *N=2t* respectively.

Other moduli, which have attracted attention, are *FERMAT* numbers of the form:

$$M = F_t = 2^{2^t} + 1$$

With : *α=2* and $\alpha = \sqrt{2}$, for, $N=2^{t+1}$ et $N=2^{t+2}$ respectively.

DUBOIS et *al.* [6] proposed the use of moduli of the form: $2^{2t} - 2^t + 1$ for *t=8*, In that case, the most interesting factors are: *12,16,18,24,* and *32*.

In what follows, we take the modulus, *M*, one of the *FERMAT* numbers with *t=4*, so that *M=65537,*

$\alpha^N \equiv 1 \bmod F_4$; if $\alpha = 2$, then, $N = 2^{t+1} = 2^5 = 32$

Calculation of N^{-1} :

$$N \times N^{-1} \equiv 1 \bmod F_4$$

$$\text{SO, } \alpha^N \times N \times N^{-1} \equiv 1 \bmod F_4 \Rightarrow \quad N^{-1} \equiv \alpha^N \times N^{-1} \bmod F_4$$

$$N^{-1} \equiv 2^{-t-1} \times 2^{2^{t+1}} \bmod F_4 \Rightarrow \quad N^{-1} = 2^{2^{t+1}-t-1}$$

Development for 2-dimensional applications can also be found in the literature [7, 8]. The investigated of image and video Filtering based on Fermat Number Transform (FNT) have been given by [9]. They have proposed two methods to overcome the limitation of choosing the word length, the first method is based on the use of the Generalized FNT, and the second uses a Residue Number System RNS.

A linear predictive coding procedure is developed in [10], where the Fermat Number Transform to reduce the computational complexity of a speech codec has been used.

Example 1

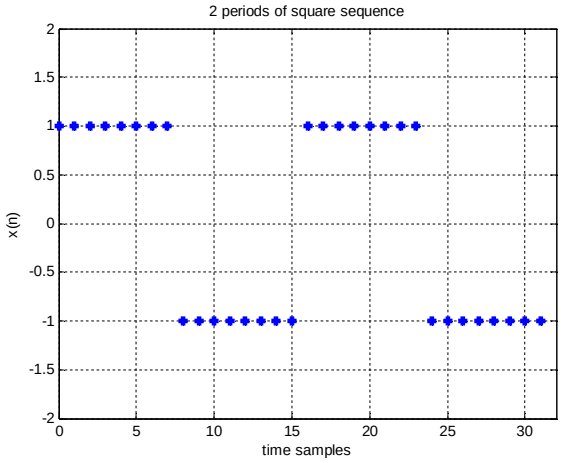
Consider the square sequences $x_i(n)$ with different periods, where '*i*' is the number of periods in the sequence:

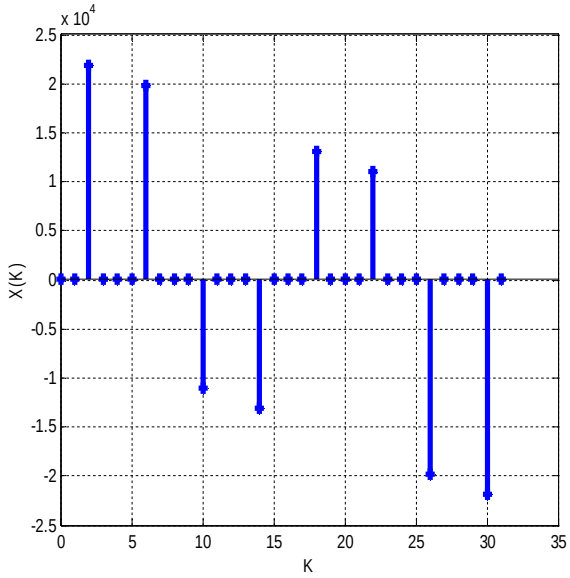
$x_4(n)$ = {1 1 1 1 -1 -1 -1 -1 1 1 1 1 -1 -1 -1 -1 1 1 1 1 -1 -1 -1 -1 1 1 1 1 -1 -1 -1 -1 }.

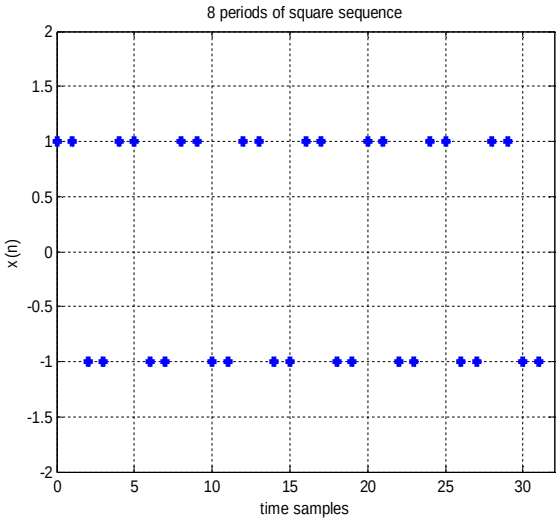
We have:

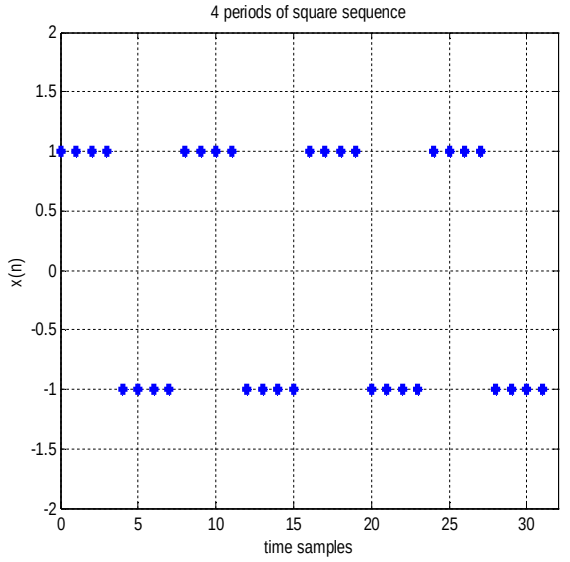
$$X(k) = \sum_{n=0}^{N-1} x(n)\,2^{nk} \bmod F_4 \qquad \text{k= 0, 1, 2, …, 31.}$$

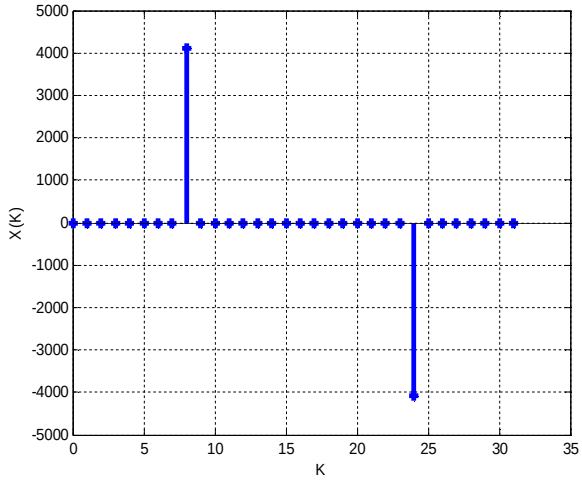
Figure 1 shows the sequences $x_i\ (n)$ for 2, 4, and 8 periods with their NTT's spectral representations.











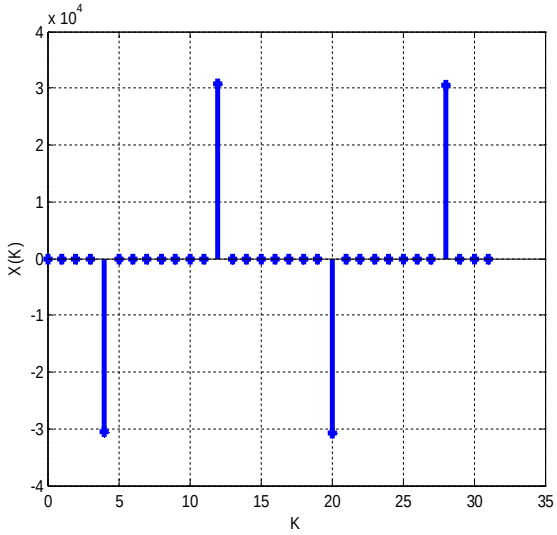


Figure 1: Square sequences for 2, 4, and 8 periods with their NTT's representations

3 DOMAIN OF NUMBERS

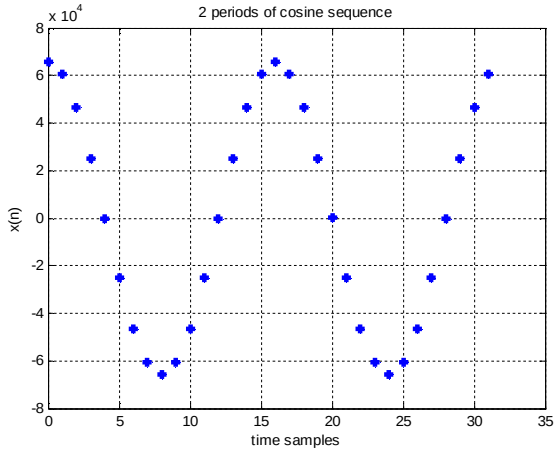
It is clear that a sample of NTT spectrum of a signal does not present any useful information. But, information can be extracted from the whole number of samples constituting the spectrum. By calculating the NTT of a periodic signal, is clear to distinguish that the number of non zero samples, gives the frequency of the signal. More exactly, the number of non zero samples in the NTT spectrum is equal to the half-period for signals of the form: $x\left(n+\frac{T}{2}\right)=\pm x(n)$

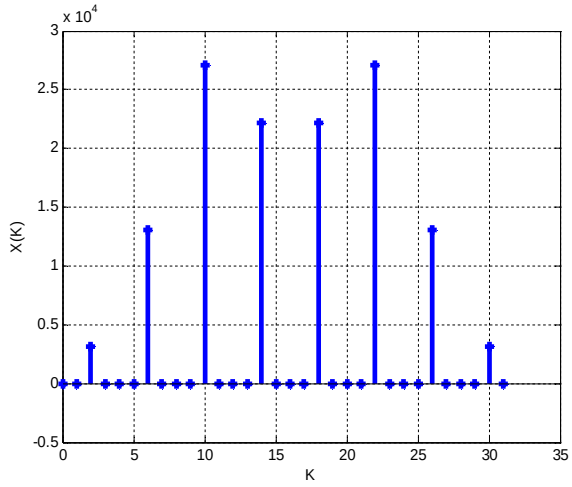
Example 2

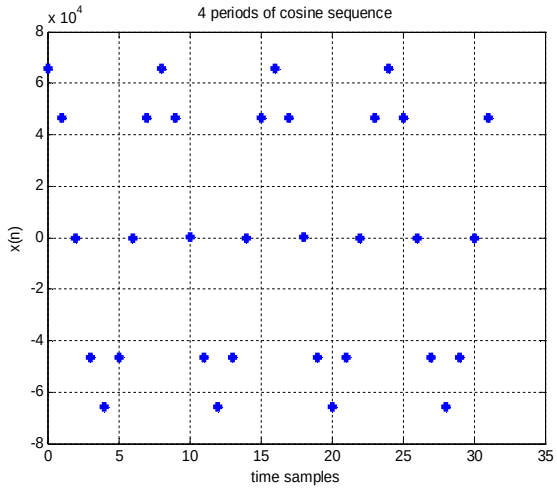
Let's consider the cosine signal: $x_i(n)=(M-1)\cos\left(2\pi\frac{n}{N}i\right)$ *n=0, 1, …, N-1*

The NTT spectra of Periodic sequences generate symmetric signal in the same period, also, symmetry between the samples $X(k)$ *and* $X(n-k)$, as shown in figure (2).

i=2, for 2 periods (T = 16)







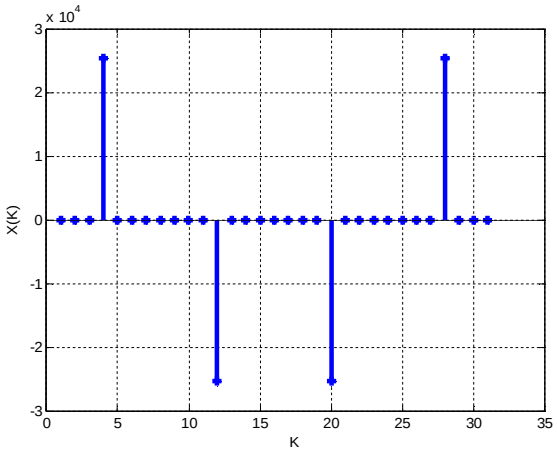


Figure 2: cosine sequences for 2, and 4 periods with their NTT's representations

3.1 FLOW DIAGRAM

Note by $X_i(k)$ the NTT of a periodic sequence with ***i*** periods.

For the example of the cosine sequence we have:

$$X_2(k)=\begin{cases}3150 & k=2\\ 13052 & k=6\\ 27125 & k=10\\ 22194 & k=14\\ 22194 & k=18\\ 27125 & k=22\\ 13052 & k=26\\ 3150 & k=30\\ 0 & other\end{cases}$$

and

$$X_4(k)=\begin{cases}25344 & k=4\\ -25360 & k=12\\ -25360 & k=20\\ 25344 & k=28\\ 0 & other\end{cases}$$

We can observe that :

$$\begin{cases}X_2(2)+X_2(18)\equiv 25344 \quad Mod\ F_4=X_4(4)\\ X_2(6)+X_2(22)\equiv -25360 \quad Mod\ F_4=X_4(12)\\ X_2(10)+X_2(26)\equiv -25360 \quad Mod\ F_4=X_4(20)\\ X_2(14)+X_2(30)\equiv 25344 \quad Mod\ F_4=X_4(28)\end{cases}$$

and

$$\begin{cases}X_4(4)+X_4(20)\equiv X_8(8) \quad Mod\ F_4\\ X_4(12)+X_4(28)\equiv X_8(24) \quad Mod\ F_4\end{cases}$$

3.1.1 Flow diagram

Let *x(n)* be a periodic sequence with period *T samples*. Samples of *x(n)* verify the expression :

$x\left(n+\frac{T}{2}\right)=\pm x(n)$. So,

$X_1(k) \longrightarrow X_2(k) \longrightarrow X_4(k) \longrightarrow X_8(k)$

as shown in the diagram below. Hence, we can write:

$$X_i(k) \oplus X_i\left(k+\frac{N}{2}\right) = X_{2i}(2k) \tag{4}$$

Where $\oplus$ is *modulo M* addition.

3.1.2 Demonstration

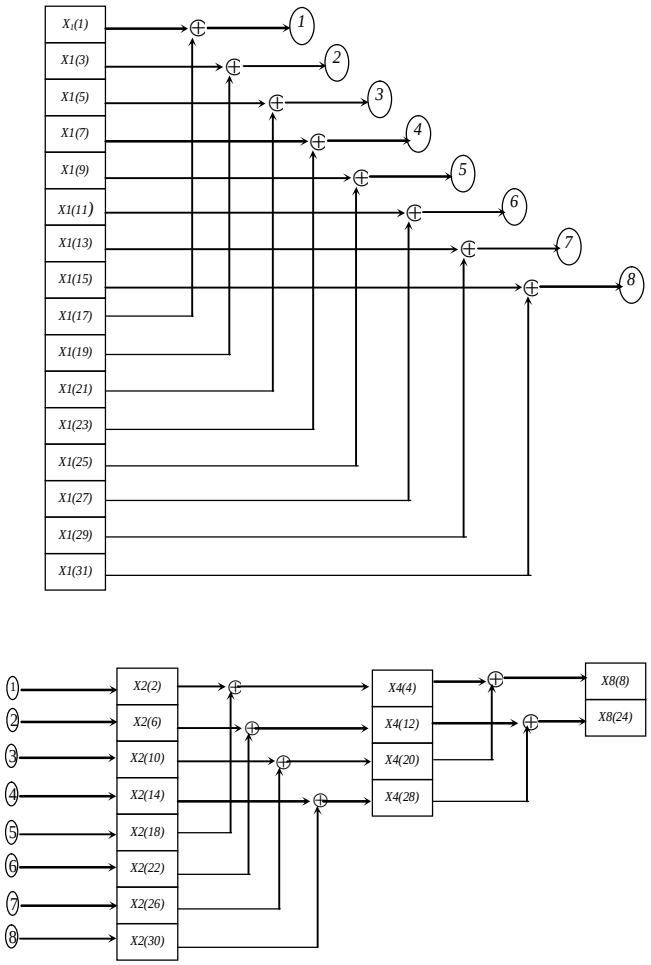


Figure 3: Flow diagram scheme.

If *x(n)* is a periodic sequence, and *X(k)* its NTT. Then,

$$X(k) = \sum_{n=0}^{N-1} x(n)\, 2^{nk} \bmod F_4 \tag{5}$$

$$X\left(k+\frac{N}{2}\right) = \sum_{n=0}^{N-1} x(n)\, 2^{n\left(k+\frac{N}{2}\right)} \bmod F_4$$

$$= \sum_{n=0}^{N-1} x(n)\, 2^{nk}\, 2^{n\frac{N}{2}} \bmod F_4$$

$$= \begin{cases} \sum_{n=0}^{N-1} x(n)\, 2^{nk} \bmod F_4 & n \text{ even} \\ -\sum_{n=0}^{N-1} x(n)\, 2^{nk} \bmod F_4 & n \text{ odd} \end{cases} \tag{6}$$

then,

$$X(k) + X\left(k+\frac{N}{2}\right) = \begin{cases} 2\sum_{n=0}^{N-1} x(n)\, 2^{nk} \bmod F_4 & \text{n even} \\ 0 & \text{n odd} \end{cases} \tag{3.4}$$

$$= 2\left\{x(0) + x(2)2^{2k} + x(4)2^{4k} + \ldots + x(N-2)2^{(N-2)k}\right\} \quad mod\ F_4$$

$$= \sum_{n=0}^{\frac{N}{2}-1} x(2n)\, 2^{2nk} \bmod F_4$$

4 SQUARE SIGNAL

A square signal, *x(n),* with zero mean value has the expression:

$$\begin{cases} x(n+T) = a = x(n) \\ x\left(n+\frac{T}{2}\right) = -a = -x(n) \end{cases} \tag{7}$$

Where T: the period a: a positive constant for *a=1* and T=16 (2 periods), we have:

$$X_2(k) = \begin{cases} 21843 & k=2 \\ 19765 & k=6 \\ -11083 & k=10 \\ -13101 & k=14 \\ 13109 & k=18 \\ 11091 & k=22 \\ -19757 & k=26 \\ -21835 & k=30 \\ 0 & other \end{cases}$$

We can observe that all non zero samples, $x(k)$ and $|X(N-k)|$ are different by a constant value, called *absolute difference*.

We can, also, observe that

$$\begin{cases} 21843 \times 2^2 = \ \ 21835 = -X(30) \\ 19765 \times 2^6 = \ \ 19757 = -X(26) \\ -11083 \times 2^{10} = -11091 = -X(22) \\ -13101 \times 2^{14} = -13109 = -X(18) \\ 13109 \times 2^{18} = 13101 = -X(14) \\ 11091 \times 2^{22} = 11083 = -X(10) \\ -19757 \times 2^{26} = -19765 = -X(6) \\ -21835 \times 2^{30} = -21843 = -X(2) \end{cases}$$

In general form we have,

$$X(N-k) = -2^k X(k) \mod F_4 \tag{8}$$

5 CONCLUSION

An interesting feature of the number theory transform is that all computations are exact (integer multiplication and addition modulo a prime integer). There is no round-off

error. This feature has been used to do fast convolutions to multiply extremely large numbers, such as is required when computing to millions of digits of precision.

Unlike the DFT, the number theoretic transform does not transform to a meaningful ``frequency domain''. However, it has analogous theorems, such as the convolution theorem, enabling it to be used for fast convolutions and correlations like the various FFT algorithms.

In this paper we demonstrated that many properties of number theoretic transforms can be found in signal processing applications such as: *flow diagram* and the relationship between NTT's square signal samples.

Finally, as a future works, we are looking for exploiting the NTT properties for image compression.

BIBLIOGRAPHY

[1] E. O. BRIGHA, "The Fast Fourier Transform". Prentice Hall, 1974.

[2] C. M. RADER,: "Discrete convolutions via Mersenne transforms. IEEE Trans. Comput., Vol. C-21, pp. 1269-1273, Dec. 1972.

[3] R. C. AGARWAL and C. S. BURRUS, "Number theoretic transforms to implement fast digital convolution". Proc. IEEE, Vol. 63, pp. 550-560, Apr. 1975.

[4] R. C. AGARWAL and C. S. BURRUS, "Fast convolution using Fermat number transforms with applications to digital filtering". IEEE Trans. On Acoust. Speech. Signal Process. Vol. ASSP-22, pp. 87-97, 1974.

[5] J. B. MARTENS, "Number Theoretic Transforms for the Calculation of Convolutions". IEEE Trans. On Acoust. Speech. Signal Process. Vol. ASSP-31, No. 04, pp. 969 – 978, August 1983.

[6] E. DUBOIS, and A. N. VENETSANOPOULOS, "The generalized discrete Fourier transform in rings of algebraic integers. IEEE Trans. On Acoust. Speech Signal Process. Vol. ASSP-28, pp. 169- 175, (1980).

[7] C. M. RADER, "On the application of the number theoretic transform methods of high-speed convolution to two-dimensional filtering. IEEE Trans., pp. 575, (1977).

[8] F. MARIR, "The Application of Number Theoretic Transforms to Two-Dimensional Convolution and Adaptive Filtering". PhD Thesis, Newcastle University, UK 1986.

[9] T. Toivonen and J. Heikkilä, "Video Filtering with Fermat Number Theoretic Transforms Using Residue Number System", IEEE Trans. On circuits and systems for video technology, VOL. 16, NO. 1, January 2006.

[10] G. Madre, *et al.* "Linear predictive speech coding using Fermat number transform", the 4th EURASIP Conference on video/image processing and multimedia communications, Zagreb, Croatia, 2-5 july 2003,.

[11] T. Conway, "Modified overlap technique using Fermat and Mersenne transforms", IEEE Trans. On circuits and systems-II express briefs, VOL. 53, NO. 8, August 2006.

[12] R. M. Campello de Souza, *et al.*, "Hartley number theoretic transforms", ISIT2001, Washington, DC, June 24-29, 2001