

Fast Complex Convolution Using Number Theoretic Transforms

EMANUEL VEGH AND LAWRENCE M. LEIBOWITZ

*Special Projects Organization
Office of the Director of Research*

November 17, 1975



NAVAL RESEARCH LABORATORY
Washington, D.C.

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NRL Report 7935	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) FAST COMPLEX CONVOLUTION USING NUMBER THEORETIC TRANSFORMS		5. TYPE OF REPORT & PERIOD COVERED Interim report on a continuing NRL Problem.
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Emanuel Vegh and Lawrence M. Leibowitz		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Research Laboratory Washington, D.C. 20375		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS NRL Problem K08-03
11. CONTROLLING OFFICE NAME AND ADDRESS Not applicable		12. REPORT DATE November 17, 1975
		13. NUMBER OF PAGES 17
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Number theoretic transform (NTT) Fermat number transform (FNT) Fast Fourier transform (FFT) Complex number theoretic (CNT) transform Convolution Finite field Circular convolution Finite ring Mersenne number transform (MNT) Complex (Gaussian) integers (Continued)		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) It is shown that discrete circular convolution of complex number sequences may be carried out without arithmetic roundoff error using a family of number theoretic transforms defined in a finite ring. In certain cases the arithmetic of this transform may involve only additions, subtractions, and circular bit shifts and may be implemented with an FFT type procedure. As an application it is shown that the discrete Fourier transform may be computed with these transforms.		

19. KEY WORDS (Continued)

Discrete Fourier transform (DFT)

Chirp z transform (CZT)

CONTENTS

1. INTRODUCTION.....	1
2. THE FINITE RING	1
3. THE TRANSFORMS DEFINED.....	2
4. THE CONVOLUTION THEOREM.....	3
5. COMPLEX-MERSENNE TRANSFORM	5
6. COMPLEX-FERMAT TRANSFORM.....	6
7. COMPUTING THE DFT.....	7
8. SUMMARY	8
9. ACKNOWLEDGMENTS.....	9
10. REFERENCES.....	9
APPENDIX A – Proof of (4) for the Entries $\alpha = 2j$ and $\alpha = 1 + j$ in Table 1.....	10
APPENDIX B – Proof of (4) for $\alpha = 1 + j$, $N = 2^{n+2}$, and $m = F_k$	13



FAST COMPLEX CONVOLUTION USING NUMBER THEORETIC TRANSFORMS

1. INTRODUCTION

Pollard [1] has recently given results for the circular convolution of sequences of elements from finite fields or from rings of integers modulo an integer. Rader [2,3] and Agarwal and Burrus [4] describe number theoretic transforms which can be used for convolution of real integer sequences and which are most suitable for implementation by digital computer. These transforms, named the Mersenne and Fermat transforms, can be implemented by a sequence of additions (or subtractions) and cyclic shifts of bits within a binary word. When these methods are used, all results are exact and thus there are no errors due to arithmetic roundoff.

Reed and Truong [5] and Agarwal and Burrus [6] define complex number theoretic (CNT) transforms in a finite field to permit the circular convolution of complex number sequences. In this report a unified theory of CNT transforms is presented by defining such transforms in a finite ring. The advantages inherent in the former number theoretic methods are equally valid here.

In section 2 a finite ring (perhaps with divisors of 0) with unit is defined that simulates the complex (Gaussian) integers. In section 3 families of CNT transforms are described, and in section 4 the convolution theorem is proved. In sections 5 and 6 special CNT transforms are dealt with that herein are called the complex-Mersenne and complex-Fermat transforms. Finally in section 7 implementation of the discrete Fourier transform (DFT) using CNT transforms is discussed.

2. THE FINITE RING

Let $m > 0$ be an integer and I_m be the set of integers

$$I_m = -\left(\frac{m}{2} - \frac{1}{2}\right), \dots, -1, 0, 1, \dots, \left(\frac{m}{2} - \frac{1}{2}\right), \quad m \text{ odd,}$$
$$= -\left(\frac{m}{2} - 1\right), \dots, -1, 0, 1, \dots, \frac{m}{2}, \quad m \text{ even.}$$

I_m is a complete system of residues modulo m ; i.e., if a is an integer, then a is congruent modulo m to exactly one of the integers in I_m , which integer will be denoted by $((a))$.

Let

$$L_m = \{a + bj \mid a, b \in I_m\}$$

and, if $x = a_1 + b_1j$ and $y = a_2 + b_2j$ are members of L_m , define their sum and product as

$$\begin{aligned} x \oplus y &= ((a_1 + a_2)) + ((b_1 + b_2))j, \\ x \odot y &= ((a_1a_2 - b_1b_2)) + ((a_1b_2 + a_2b_1))j. \end{aligned}$$

It may be shown that (L_m, \oplus, \odot) is a finite ring with unit.

Let Λ denote the ring of Gaussian integers:

$$\Lambda = \{a + bj \mid a \text{ and } b \text{ integers}\}.$$

The mapping

$$[[\dots]]: \Lambda \rightarrow L_m$$

defined by

$$[[z]] = ((\text{Re } z)) + ((\text{Im } z))j$$

may be shown to satisfy

$$[[z_1 + z_2]] = [[z_1]] \oplus [[z_2]] \tag{1}$$

and

$$[[z_1 z_2]] = [[z_1]] \odot [[z_2]]. \tag{2}$$

It is important to note that if $z \in \Lambda$ and $-m/2 < \text{Re } z, \text{Im } z < m/2$, then

$$[[z]] = z. \tag{3}$$

Thus, in this case, if z is the result of a computation involving additions, subtractions, and multiplications of Gaussian integers, then (1), (2), and (3) indicate that z may be obtained by the corresponding sequence of operations in L_m . If z is real, then $[[z]] = ((z))$.

3. THE TRANSFORMS DEFINED

Let N be a positive integer for which there exists an integer M such that $((NM)) = 1$. Let $\alpha \in \Lambda$ such that for each positive integer $t < N$ there is an element $\beta_t \in \Lambda$ for which

$$[[(1 - \alpha^t) \beta_t]] = 1 \tag{4}$$

and such that

$$[[\alpha]]^N = 1. \tag{5}$$

Let

$$L_m^N = \{(z_0, z_1, \dots, z_{N-1}) \mid z_0, z_1, \dots, z_{N-1} \in L_m\}$$

and

$$\Lambda^N = \{(z_0, z_1, \dots, z_{N-1}) \mid z_0, z_1, \dots, z_{N-1} \in \Lambda\},$$

let T_α be the transformation from Λ^N to L_m^N defined by

$$T_\alpha(z_0, z_1, \dots, z_{N-1}) = (Z_0, Z_1, \dots, Z_{N-1}),$$

where for each integer k , $0 \leq k < N$,

$$Z_k = \left[\left[\sum_{n=0}^{N-1} z_n \alpha^{nk} \right] \right], \quad (6)$$

and let T_α^{-1} be the *inverse* transformation from L_m^N to L_m^N defined by

$$T_\alpha^{-1}(V_0, V_1, \dots, V_{N-1}) = (v_0, v_1, \dots, v_{N-1}),$$

where for each integer k , $0 \leq k < N$,

$$v_k = \left[\left[M \sum_{n=0}^{N-1} V_n \alpha^{\langle -nk \rangle} \right] \right]. \quad (7)$$

(Here $\langle \dots \rangle$ is used to denote the least nonnegative integer modulo N .)

4. THE CONVOLUTION THEOREM

Theorem: If

$$T_\alpha(z_0, z_1, \dots, z_{N-1}) = (Z_0, Z_1, \dots, Z_{N-1}),$$

$$T_\alpha(w_0, w_1, \dots, w_{N-1}) = (W_0, W_1, \dots, W_{N-1}),$$

and

$$C_k = Z_k \odot W_k, \quad 0 \leq k < N,$$

then

$$T_\alpha^{-1}(C_0, C_1, \dots, C_{N-1}) = (c_0, c_1, \dots, c_{N-1})$$

where

$$c_k = \left[\left[\sum_{n=0}^{N-1} z_n w_{\langle k-n \rangle} \right] \right]. \quad (8)$$

Proof: If

$$c_n = \left[\left[M \sum_{k=0}^{N-1} C_k \alpha^{\langle -kn \rangle} \right] \right]$$

then

$$\begin{aligned}
 c_n &= \left[\left[M \sum_{k=0}^{N-1} z_k w_k \alpha^{\langle -kn \rangle} \right] \right] \\
 &= \left[\left[M \sum_{k=0}^{N-1} \left(\sum_{p=0}^{N-1} z_p \alpha^{pk} \right) \left(\sum_{l=0}^{N-1} w_l \alpha^{lk} \right) \alpha^{\langle -nk \rangle} \right] \right] \\
 &= \left[\left[\sum_{p=0}^{N-1} \sum_{l=0}^{N-1} z_p w_l M \sum_{k=0}^{N-1} \alpha^{\langle p+l-n \rangle k} \right] \right] \\
 &= \left[\left[\sum_{p=0}^{N-1} \sum_{l=0}^{N-1} z_p w_l \right] \right] \odot \left[\left[\left(M \sum_{k=0}^{N-1} \alpha^{\langle p+l-n \rangle k} \right) \right] \right]. \tag{9}
 \end{aligned}$$

Consider the sum

$$S_{\langle t \rangle} = \left[\left[\sum_{k=0}^{N-1} \alpha^{\langle t \rangle k} \right] \right].$$

If $\langle t \rangle = 0$, then $S_0 = ((N))$. If $\langle t \rangle \neq 0$, then using (3) and the fact that

$$[[1 - \alpha^{N\langle t \rangle}]] = 0,$$

we obtain

$$\begin{aligned}
 S_{\langle t \rangle} &= [[\beta_{\langle t \rangle} (1 - \alpha^{\langle t \rangle})]] \odot [[S_{\langle t \rangle}]] \\
 &= [[\beta_{\langle t \rangle}]] \odot [[(1 - \alpha^{\langle t \rangle}) S_{\langle t \rangle}]] \\
 &= [[\beta_{\langle t \rangle}]] \odot [[1 - \alpha^{N\langle t \rangle}]] = 0.
 \end{aligned}$$

Hence

$$\begin{aligned}
 \left[\left[M \sum_{k=0}^{N-1} \alpha^{\langle p+l-n \rangle k} \right] \right] &= ((MN)) = 1, & \text{if } \langle p+l-n \rangle = 0, \\
 &= 0, & \text{if } \langle p+l-n \rangle \neq 0,
 \end{aligned}$$

and, using (9),

$$c_n = \left[\left[\sum_{p=0}^{N-1} z_p w_{\langle n-p \rangle} \right] \right].$$

This completes the proof.

Let $(z_0, z_1, \dots, z_{N-1})$ and $(w_0, w_1, \dots, w_{N-1})$ be periodic Gaussian integer sequences with period N , $\max_{0 \leq i < N} |z_i| = \tau$, and $\max_{0 \leq i < N} |w_i| = \delta$. If $\tau\delta N < m/2$, then

$$-m/2 < \operatorname{Re} \sum_{p=0}^{N-1} z_p w_{\langle n-p \rangle}, \operatorname{Im} \sum_{p=0}^{N-1} z_p w_{\langle n-p \rangle} < m/2$$

and, as in Eq. (3), for $0 \leq n < N$,

$$c_n = \left[\left[\sum_{p=0}^{N-1} z_p w_{\langle n-p \rangle} \right] \right] = \sum_{p=0}^{N-1} z_p w_{n-p}; \quad (10)$$

hence the result of the computation given by the theorem is the circular convolution of the two sequences. To obtain (10) it is sufficient to have

$$m > 2\tau\delta N. \quad (11)$$

5. COMPLEX-MERSENNE TRANSFORM

Let m be the Mersenne number $M_p = 2^p - 1$, p prime, and let $N = p$. Then with $M = (2 - 2^p)/p$,

$$((NM)) = \left(\left(p \left(\frac{2 - 2^p}{p} \right) \right) \right) = ((2 - 2^p)) = ((1 - M_p)) = 1.$$

For $\alpha = 2$ it can be shown that for each integer t , $0 < t < N$, the $\operatorname{gcd}((1 - 2^t), M_p) = 1$; hence there is an integer β_t such that

$$(((1 - 2^t)\beta_t)) = 1.$$

Furthermore

$$((2^N)) = ((2^p)) = ((M_p + 1)) = 1.$$

The conditions of section 3 are now satisfied by m , N , and α , and the transforms T_2 and T_2^{-1} as given in (6) and (7) take the following forms respectively: If $z_n = a_n + b_n j$, $0 \leq n < N$, then for $0 \leq k < N$

$$Z_k = \left[\left[\sum_{n=0}^{N-1} z_n 2^{nk} \right] \right] = \left(\left(\sum_{n=0}^{N-1} a_n 2^{nk} \right) \right) + \left(\left(\sum_{n=0}^{N-1} b_n 2^{nk} \right) \right) j. \quad (12)$$

If $V_n = A_n + B_n j$, $0 \leq n < N$, then for $0 \leq k < N$

$$v_k = \left[\left[M \sum_{n=0}^{N-1} V_n 2^{\langle -nk \rangle} \right] \right] = \left(\left(M \sum_{n=0}^{N-1} A_n 2^{\langle -nk \rangle} \right) \right) + \left(\left(M \sum_{n=0}^{N-1} B_n 2^{\langle -nk \rangle} \right) \right) j. \quad (13)$$

Here $((...))$ means modulo M_p .

The implementation of (12) and (13) requires only additions and cyclic shifts of bits within the binary words a_n , b_n , A_n , and B_n . The real and imaginary parts of Z_k and v_k may also be

computed concurrently. There is no roundoff error in these computations, since all quantities are represented modulo M_p .

Similarly, longer sequences may be convolved with the complex-Mersenne transform by using the values of α and N in Table 1. Each of the pairs $\{\alpha, N\}$ in Table 1 may be shown to satisfy (4) and (5). The table entries for $\alpha = 2$ and $\alpha = -2$ were covered by Rader [2] for the real-Mersenne transform. The entries for $\alpha = 2j$ and $\alpha = 1 + j$ are discussed in Appendix A. Transforms with these values of α are straightforward even with $\alpha = 1 + j$, since powers of α , expressed as α^t , are of the form $2^s a + 2^s b j$, a and b taking on values of 0 and ± 1 and s being the integer part of $t/2$. In addition, since the values of N can be somewhat composite, some advantage may be obtained by using a fast Fourier transform (FFT) procedure.

TABLE 1 — Multipliers α
and sequence lengths N
for $m = M_p$

α	N
2	p
-2	$2p$
$2j$	$4p$
$1 + j$	$8p$

6. COMPLEX-FERMAT TRANSFORM

Let n be a positive integer, let $m = F_n = 2^{2^n} + 1$, $N = 2^{n+1}$, and let $M = 2^{2^{n+1} - (n+1)}$. We see that

$$((NM)) = ((2^{2^n})) = ((2^N)) = (((F_n - 1)^2)) = 1.$$

For $0 < t < N$, it can be shown that $\gcd(1 - 2^t, F_n) = 1$. Thus, with $\alpha = 2$, there is for each integer t , $0 < t < N$, an integer β_t such that

$$(((1 - 2^t)\beta_t)) = 1.$$

The conditions of section 3 are now satisfied by m , N , and α , and the transformations T_2 and T_2^{-1} are given by (12) and (13) with $((...))$ now meaning modulo F_n .

Agarwal and Burrus [4] give other values $\{\alpha, N\}$ for the real-Fermat transform. These pairs are also valid for the complex-Fermat transform. In particular

$$\{\alpha = 2^{2^{n-2}}(2^{2^{n-1}} - 1), N = 2^{n+2}\}$$

gives a transform whose length N is twice that given when $\alpha = 2$. Another pair

$$\{\alpha = 1 + j, N = 2^{n+2}\}$$

may be shown to satisfy (4) and (5) (Appendix B); furthermore using these values for $\{\alpha, N\}$ the transforms may be implemented with a cyclic shift of bits within a binary word together with additions (or subtractions). Since N is a power of 2, the complex-Fermat transform may be implemented with an FFT type algorithm. To convolve long complex sequences, the multi-dimensional methods described by Agarwal and Burrus [7] may be applied.

7. COMPUTING THE DFT

The discrete Fourier transform may be implemented using the CNT transform via the method of Bluestein [8]. Let N be an even integer, let $z = (z_0, \dots, z_{N-1})$ be a sequence of complex numbers of period N , let $W = e^{-2\pi j/N}$, and let T be the discrete Fourier transform. Then $Tz = (Z_0, Z_1, \dots, Z_{N-1})$, where

$$\begin{aligned} Z_k &= \sum_{n=0}^{N-1} z_n W^{nk} \\ &= \sum_{n=0}^{N-1} z_n (W^{1/2})^{2nk} \\ &= (W^{1/2})^{k^2} \sum_{n=0}^{N-1} (z_n W^{n^2/2}) W^{(k-n)^2/2} \\ &= (W^{1/2})^{k^2} \sum_{n=0}^{N-1} d_n g_{k-n}, \end{aligned}$$

where

$$d_n = z_n (W^{1/2})^{n^2} \text{ and } g_n = (W^{-1/2})^{n^2}. \quad (14)$$

Since N is even,

$$d_{n+N} = d_n \text{ and } g_{n+N} = g_n.$$

Finally, if $W^{1/2}$, d_n , and g_n are scaled so that they are members of Λ and if m is chosen subject to (11), then the computations may be carried out using the transforms of section 4 or 5 and the theorem of section 3.

Example: Consider the DFT of $(z_0, z_1, z_2, z_3) = (1, 1, 1, 1)$. Let $m = F_4 = 2^{16} + 1$, $N = 2^2$, $M = 2^{30}$, $\alpha = 2^8$ ($\alpha^2 = -1$, $\alpha^3 = -2^8$, $\alpha^4 = 1$), and $W^{1/2} = 0.7-0.7j$ (quantized to one significant decimal digit).

Each of the terms in (14) are multiplied by 10 for scaling purposes, and we obtain

$$(d_0, d_1, d_2, d_3) = (10, 7 - 7j, -10, 7 - 7j)$$

and

$$(g_0, g_1, g_2, g_3) = (10, 7 + 7j, -10, 7 + 7j)$$

for the sequences to be convolved. If we use (12), the transforms of these sequences are respectively

$$(D_0, D_1, D_2, D_3) = (14 - 14j, 20, -14 + 14j, 20)$$

and

$$(G_0, G_1, G_2, G_3) = (14 + 14j, 20, -14 - 14j, 20).$$

(Naturally all computations are modulo $2^{16} + 1$.) Taking the product of these transforms, we have

$$(V_0, V_1, V_2, V_3) = (392, 400, 392, 400),$$

and, using (13) for the inverse transform, we obtain

$$(v_0, v_1, v_2, v_3) = (398, 0, -4, 0). \quad (15)$$

Multiplying each member of (15) by the appropriate term, $(W^{1/2})^{k^2}$, and rescaling, we obtain the DFT

$$(Z_0, Z_1, Z_2, Z_3) = (3.98, 0, 0.04, 0) \approx (4, 0, 0, 0).$$

8. SUMMARY

A family of transforms were defined that generalized the recently given number theoretic transforms (NTT) of Rader, Agarwal, and Burrus. These new transforms were used for circular convolution of finite sequences of complex numbers. The computation of the DFT was given as an example.

Several multipliers α were defined that can be used even with real number sequences to allow for the convolution of sequences longer than those previously considered.

As with a real NTT, the principal advantages of these transforms are that they may be implemented with an FFT procedure, without computational roundoff, employing only circular bit shifts within words and additions (or subtractions).

It was shown that a characteristic of these methods, when used for circular convolution, was that the computation word size linearly depends on the sequence length.

9. ACKNOWLEDGMENTS

The authors express appreciation to R. E. Ellis, Head of the Special Projects Organization, NRL, for his continued support and encouragement. The labors of Mrs. Anita Latham with respect to the typing and other preparation of the report manuscript are greatly appreciated.

10. REFERENCES

1. J.M. Pollard, "The fast Fourier transform in a finite field," *Math. Comput.* **25**, 365-374 (Apr. 1971).
2. C.M. Rader, "Discrete convolutions via Mersenne transforms," *IEEE Trans. on Computer*, **C-21** (No. 12), 1269-1273 (Dec. 1972).
3. L.R. Rabiner and B. Gold, *Theory and Applications of Digital Signal Processing*, Englewood Cliffs, N.J., Prentice-Hall, 1975, pp. 419-434.
4. R.C. Agarwal and C.S. Burrus, "Fast convolution using Fermat number transforms with applications to digital filtering," *IEEE Trans. on Acoustics, Speech and Signal Processing ASSP-22* (No. 2), 87-97 (Apr. 1974).
5. I.S. Reed and T.K. Truong, "The Use of Finite Fields to Compute Convolutions," *IEEE Transactions on Information Theory IT-21*, 208-213 (Mar. 1975).
6. R.C. Agarwal and C.S. Burrus, "Number Theoretic Transforms to Implement Fast Digital Convolution," *Proc. IEEE* **63**, 550-560 (Apr. 1975).
7. R.C. Agarwal and C.S. Burrus, "Fast one-dimensional digital convolution by multidimensional techniques," *IEEE Trans. on Acoustics, Speech and Signal Processing ASSP-22* (No. 1), 1-10 (Feb. 1974).
8. L.I. Bluestein, "A linear filtering approach to the computation of the discrete Fourier transform," *Northeast Electronics Research and Engineering Meeting Record* **10**, 218-219 (1968).

Appendix A
PROOF OF (4) FOR THE ENTRIES $\alpha = 2j$ AND $\alpha = 1 + j$ IN TABLE 1

The purpose of this appendix is to prove (4) for $\alpha = 1 + j$ and $\alpha = 2j$ with modulus M_p . Let m and N be positive integers and t be an integer $0 < t < N$. Let

$$\lambda_t \triangleq (1 - (1 + j)^t)(1 - (1 - j)^t).$$

The following tabulation allows one to compute with λ_t :

$$\lambda_t = \left\{ \begin{array}{lll} \text{(i):} & (1 - 2^{4n})^2, & t = 8n, \\ \text{(ii):} & (1 - 2^{4n})^2 + (2^{4n})^2, & t = 8n + 1 \\ \text{(iii):} & 1 + (2^{4n+1})^2, & t = 8n + 2 \\ \text{(iv):} & (1 + 2^{4n+1})^2 + (2^{4n+1})^2, & t = 8n + 3 \\ \text{(v):} & (1 + 2^{4n+2})^2, & t = 8n + 4 \\ \text{(vi):} & (1 + 2^{4n+2})^2 + (2^{4n+2})^2, & t = 8n + 5 \\ \text{(vii):} & 1 + (2^{4n+3})^2, & t = 8n + 6 \\ \text{(viii):} & (1 - 2^{4n+3})^2 + (2^{4n+3})^2, & t = 8n + 7 \end{array} \right\}, \quad 0 \leq n < N/8.$$

If $\gcd(\lambda_t, m) = 1$ (so that λ_t^{-1} exists modulo m), then, by defining

$$\beta_t \triangleq \lambda_t^{-1}(1 - (1 - j)^t),$$

we see that

$$(1 - (1 + j)^t)\beta_t = \lambda_t^{-1}\lambda_t = 1.$$

This is (4) for $\alpha = 1 + j$ and modulus m .

Definition: We say that a belongs to the integer t modulo m (we write $a \rightarrow t \pmod{m}$) if and only if t is the smallest positive integer s such that $a^s \equiv 1 \pmod{m}$.

The following results may easily be proved:

Lemma 1: If $a \rightarrow t \pmod{m}$ and $a^n \equiv 1 \pmod{m}$, then $t|n$.

Lemma 2: If $a \not\equiv 1 \pmod{m}$, $a^t \equiv 1 \pmod{m}$, and t is a prime number, then $a \rightarrow t \pmod{m}$.

Lemma 3: If $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

Lemma 4: If $a|b$ and $\gcd(b, m) = 1$, then $\gcd(a, m) = 1$.

Lemma 5: $\gcd(x, m) = 1$ if and only if $\gcd(x^2, m) = 1$.

For each t we shall show

$$\gcd(\lambda_t, m) = 1. \quad (\text{A1})$$

In all cases except (i) and (v), λ_t is of the form

$$2^k + 1 \quad (\text{A2})$$

or, by virtue of the identity

$$(2^{2s+1} + 2^{s+1} + 1)(2^{2s+1} - 2^{s+1} + 1) = 2^{4s+2} + 1, \quad (\text{A3})$$

λ_t divides an integer of the form (A2). Using Lemma 4 in cases (ii) through (viii) and Lemma 5 in case (v), we shall prove (A1) by showing that

$$\gcd(2^k + 1, m) = 1 \text{ for all values of } k. \quad (\text{A4})$$

We will show case (i) independently.

Let $m = M_p = 2^p - 1$, let $p > 2$ be a prime, and let $N = 8p$. Then $2^p \equiv 1 \pmod{M_p}$, and, using Lemma 3, it will be sufficient to prove (A4) for k , $0 \leq k < p$.

Assume $\gcd(2^k + 1, M_p) = qd > 1$, where q is prime. Then

$$2^p \equiv 1 \pmod{q} \text{ and } 2^{2k} \equiv 1 \pmod{q}.$$

Using Lemma 2, $2 \rightarrow p \pmod{q}$. Using Lemma 1, $p|2k$. Since p is odd, then $p|k$ and hence $k \geq p$, which is a contradiction. Thus we have proved (A4) for all cases except (i). In this case, we need only show via Lemma 5 that

$$\gcd(1 - 2^{4n}, M_p) = 1, \quad 0 < n < p. \quad (\text{A5})$$

Once again if we assume that $\gcd(1 - 2^{4n}, M_p) = qd > 1$, q a prime, then

$$2^{4n} \equiv 1 \pmod{q} \text{ and } 2^p \equiv 1 \pmod{q}.$$

Using Lemma 2, $2 \rightarrow p \pmod{q}$. Using Lemma 1, $p|4n$. Since p is odd, then $p|n$; hence $n \geq p$, which is a contradiction. Thus we have (A5) and have proved (A1) for each t , $0 < t < N$. Therefore $\alpha = 1 + j$ has property (4) mod M_p .

Let $m = M_p$, $N = 4p$, $\alpha = 2j$, and

$$\sigma_t \triangleq (1 - (2j)^t)(1 - (-2j)^t), \quad 0 < t < N.$$

Then

$$\sigma_t = \left\{ \begin{array}{ll} \textcircled{a}: (1 - 2^{4n})^2, & t = 4n, \\ \textcircled{b}: 1 + 2^{8n+2}, & t = 4n + 1 \\ \textcircled{c}: (1 + 2^{4n+2})^2, & t = 4n + 2 \\ \textcircled{d}: 1 + 2^{8n+6}, & t = 4n + 3 \end{array} \right\}, 0 \leq n < p.$$

We see using (A4), and also Lemma 5 in case \textcircled{c} , that

$$\gcd(\sigma_t, M_p) = 1$$

in cases \textcircled{b} , \textcircled{c} , and \textcircled{d} . By Lemma 5 and (A5) we have \textcircled{a} . Thus $\sigma_t^{-1} \bmod M_p$ exists. Now defining

$$\bar{\beta}_t = \sigma_t^{-1}(1 - (-2j)^t),$$

we have

$$(1 - (2j)^t)\bar{\beta}_t = \sigma_t \sigma_t^{-1} = 1, \quad 0 < t < N.$$

Thus $\alpha = 2j$ has property (4) mod M_p .

Appendix B

PROOF OF (4) FOR $\alpha = 1 + j$, $N = 2^{n+2}$, AND $m = F_k$

The purpose of this appendix is to prove (4) for $\alpha = 1 + j$ with modulus $F_k = 2^{2^k} + 1$. We use the notation of Appendix A. If we use the identity (A3) and cases (i) through (viii) of Appendix A, we find that λ_t divides the following integers in these respective cases:

$$\left. \begin{array}{lll} \text{(i):} & (1 - 2^{4n})^2, & t = 8n, \\ \text{(ii):} & 2^{16n+2} + 1, & t = 8n + 1 \\ \text{(iii):} & 2^{8n+2} + 1, & t = 8n + 2 \\ \text{(iv):} & 2^{16n+6} + 1, & t = 8n + 3 \\ \text{(v):} & (2^{4n+2} + 1)^2, & t = 8n + 4 \\ \text{(vi):} & 2^{16n+10} + 1, & t = 8n + 5 \\ \text{(vii):} & 2^{8n+6} + 1, & t = 8n + 6 \\ \text{(viii):} & 2^{16n+14} + 1, & t = 8n + 7 \end{array} \right\}, 0 \leq n < N/8.$$

Let $m = F_k$, $k > 1$, and $N = 2^{k+2}$. If q is a prime divisor of F_k , then

$$2^{2^k} \equiv -1 \pmod{q} \text{ and } 2^{2^{k+1}} \equiv 1 \pmod{q}.$$

If $2 \rightarrow t \pmod{q}$, then using Lemma 7 we have

$$t | 2^{k+1}$$

or $t = 2^\ell$ for some positive integer $\ell \leq k + 1$. If $\ell < k + 1$, then

$$2^{2^\ell} \equiv 1 \pmod{q}$$

implies

$$(2^{2^\ell})^{2^{k-\ell}} \equiv 1 \pmod{q}$$

or

$$2^{2^k} \equiv 1 \pmod{q},$$

which is a contradiction. Thus $t = 2^{k+1}$ or

$$2 \rightarrow 2^{k+1} \pmod{q}. \tag{B1}$$

In case (ii) assume for some n , $0 \leq n < 2^{k-1}$, that

$$\gcd(2^{16n+2} + 1, F_k) = qd > 1, \quad q \text{ prime.}$$

Then

$$2^{16n+2} \equiv -1 \pmod{q}$$

and

$$2^{32n+4} \equiv 1 \pmod{q}.$$

Hence, by Lemma 1 and (B1), $2^{k+1} | 32n + 4$. This is possible only if $k \leq 1$, which is a contradiction. Thus

$$\gcd(2^{16n+2} + 1, F_k) = 1, \quad 0 \leq n < 2^{k-1}.$$

Each of the cases (iii) through (viii) leads to the same conclusion.

In case (i), assume for some n , $0 < n < 2^{k-1}$,

$$\gcd((1 - 2^{4n})^2, F_k) = qd > 1, \quad q \text{ prime.}$$

Then $2^{4n} \equiv 1 \pmod{q}$ and, by Lemma 1 and (B1), $2^{k+1} | 4n$; or $n \geq 2^{k-1}$, which is contradiction. Hence $\gcd((1 - 2^{4n})^2, F_k) = 1$. Thus, for $0 < t < N$, λ_t divides an integer which is relatively prime to F_k , so that, by Lemma 3,

$$\gcd(\lambda_t, F_k) = 1, \quad 0 < t < N.$$

Thus λ_t^{-1} exists modulo F_k , and, as in Appendix A, with

$$\beta_t \triangleq \lambda_t^{-1}(1 - (1 - j)^t)$$

we see that

$$(1 - (1 + j)^t)\beta_t = \lambda_t^{-1}\lambda_t = 1;$$

so $\alpha = 1 + j$ has property (4) mod F_k .