MATHEMATICS OF COMPUTATION
VOLUME 52, NUMBER 185
JANUARY 1989, PAGES 189-200

Parameter Determination for Complex Number-Theoretic Transforms Using Cyclotomic Polynomials

By R. Creutzburg and M. Tasche

Abstract. Some new results for finding all convenient moduli m for a complex number-theoretic transform with given transform length n and given primitive nth root of unity modulo m are presented. The main result is based on the prime factorization for values of cyclotomic polynomials in the ring of Gaussian integers.

1. Introduction. With the rapid advances in large-scale integration, a growing number of digital signal processing applications becomes attractive. The number-theoretic transform (NTT) was introduced as a generalization of the discrete Fourier transform (DFT) over residue class rings of integers in order to perform fast cyclic convolutions without roundoff errors [7, pp. 158–167], [10, pp. 211–216], [3]. The main drawback of the NTT is the rigid relationship between obtainable transform length and possible computer word length. In a recent paper [4], the authors have discussed this important problem of parameter determination for NTT's in the ring of integers by studying cyclotomic polynomials.

The advantage of the later introduced (see [7, pp. 210–216], [9], [10, pp. 236–239], [5]) complex number-theoretic transforms (CNT) over the corresponding rational transforms is that the transform length is larger for the same modulus. In this note, we consider the problem of parameter determination for CNT, and we extend the results of [4] to the ring of Gaussian integers.

2. Primitive Roots of Unity Modulo m. By $\mathbb{Z}$ and $\mathbb{Z}[i]$ we denote the ring of integers and the ring of Gaussian integers, respectively. We denote the conjugate complex number of $z \in \mathbb{Z}[i]$ by $\bar{z}$. The norm $\mathrm{N}(z)$ of $z = x + yi \in \mathbb{Z}[i]$ is defined as $\mathrm{N}(z) = x^2 + y^2$. If $\mathrm{N}(z)$ is odd, then we say that $z \in \mathbb{Z}[i]$ is odd. Note that $\mathbb{Z}[i]$ is a Euclidean ring (see, for instance, [6, pp. 178–187]).

In $\mathbb{Z}[i]$ there are the following primes: The number $1 + i$ and its associates; the rational primes $\equiv 3 \bmod 4$ and their associates; the Gaussian integers whose norms are rational primes $\equiv 1 \bmod 4$ (see [6, pp. 218–219]).

Let $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, be an odd Gaussian integer which possesses the complex prime factorization

$$m = i^{\gamma} p_1^{\alpha_1} \cdots p_s^{\alpha_s} c_1^{\beta_1} \cdots c_t^{\beta_t}, \tag{1}$$

Received June 23, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 94A11, 65E05, 11R04, 11R09.

Key words and phrases. Complex number-theoretic transform, complex pseudo Fermat number transform, complex pseudo Mersenne number transform, primitive root of unity modulo m, cyclotomic polynomial.

where $\gamma \in \{0,1,2,3\}$, $\alpha_j \geq 1$, $\beta_k \geq 1$, p_j are distinct rational primes $\equiv 3 \bmod 4$ and $c_k \in \mathbb{Z}[i]$ are distinct primes whose norms are rational primes $\equiv 1 \bmod 4$ ($j = 1, \ldots, s$; $k = 1, \ldots, t$). Further let $n \geq 2$. A number $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 1$, is called a *primitive nth root of unity modulo m* [3], if

$$\begin{aligned} &e^n \equiv 1 \bmod m, \\ &\mathrm{GCD}(e^k - 1, m) = 1, \qquad k = 1, \ldots, n-1. \end{aligned}$$

By definition, $e = 1$ is a primitive first root of unity modulo m. The condition

$$n | \mathrm{GCD}(p_j^2 - 1, \mathrm{N}(c_k) - 1;\ j = 1, \ldots, s;\ k = 1, \ldots, t) \tag{2}$$

is necessary and sufficient for the existence of primitive nth roots of unity modulo m in $\mathbb{Z}[i]$ (see [10, p. 237], [3]).

Note that for $n > 2$ and $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, a Gaussian integer m, $\mathrm{N}(m) \geq 5$, with the properties

$$\begin{aligned} &m | e^n - 1, \\ &\mathrm{GCD}(e^k - 1, m) = 1, \qquad k = 1, \ldots, n-1, \end{aligned}$$

is called a *primitive divisor of* $e^n - 1$. Obviously, these conditions are equivalent to

$$\begin{aligned} &m | e^n - 1, \\ &\mathrm{GCD}(N(e^k - 1), \mathrm{N}(m)) = 1, \qquad k = 1, \ldots, n-1. \end{aligned}$$

The following theorem gives criteria for a Gaussian integer to be a primitive nth root of unity modulo m. We denote the nth cyclotomic polynomial by Φ_n.

THEOREM 1 ([3]). *Let $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, be an odd Gaussian integer. Further let $n > 4$. An element $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, is a primitive nth root of unity modulo m if and only if one of the following conditions holds*:

(1) $\Phi_n(e) \equiv 0 \bmod m$, $\mathrm{GCD}(n, m) = 1$;

(2) $e^n \equiv 1 \bmod m$, $\mathrm{GCD}(e^d - 1, m) = 1$
for every divisor $d \geq 1$ of n such that n/d is a rational prime;

(3) $e^n \equiv 1 \bmod m$, $\mathrm{GCD}(N(e^d - 1), \mathrm{N}(m)) = 1$
for every divisor $d \geq 1$ of n such that n/d is a rational prime;

(4) *m is a primitive divisor of $e^n - 1$.*

The concept of the primitive nth root of unity modulo m is essential in the following context. Let $\mathbf{x} = [x_0, \ldots, x_{n-1}]$ and $\mathbf{y} = [y_0, \ldots, y_{n-1}]$ be two n-dimensional vectors with Gaussian integers as components. Note that the equality of such vectors $\mathbf{x}$ and $\mathbf{y}$ is defined by $x_k \equiv y_k \bmod m$, $k = 0, \ldots, n-1$. The *complex number-theoretic transform* (CNT) of *length* n with $e \in \mathbb{Z}[i]$ as a primitive nth root of unity modulo m, and its *inverse*, are defined to be the following mappings between n-dimensional vectors $\mathbf{x} = [x_0, \ldots, x_{n-1}]$ and $\mathbf{X} = [X_0, \ldots, X_{n-1}]$:

$$\begin{aligned} X_j &\equiv \sum_{k=0}^{n-1} x_k e^{jk} \bmod m, \qquad j = 0, \ldots, n-1, \\ x_k &\equiv n' \sum_{j=0}^{n-1} X_j e^{-jk} \bmod m, \qquad k = 0, \ldots, n-1, \end{aligned}$$

where $n'n \equiv 1 \bmod m$ (see [7, p. 211], [10, p. 238], [3]). Note that there exists such an integer n' because of $\mathrm{GCD}(n,m) = 1$ (see Theorem 1, (1)). The CNT possesses properties resembling those of the DFT, particularly the cyclic convolution property ([7, pp. 211–212], [3]).

For given transform length n and given $e \in \mathbb{Z}[i]$, one has to choose the modulus m by Theorem 1 as a divisor of $\Phi_n(e)$ which is relatively prime to n, or as a primitive divisor of $e^n - 1$. In practical applications, the following lemmas are helpful.

LEMMA 1. *Let $n, r \in \mathbb{Z}$, $n > 2$, $1 \le r < n$. Assume that $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \ge 5$, is an odd Gaussian integer.*

(1) *Let $\mathrm{GCD}(r,n) = 1$. If $e \in \mathbb{Z}[i]$ is a primitive nth root of unity modulo m, then e^r is a primitive nth root of unity modulo m.*

(2) *In the case $r|n$, the element $e \in \mathbb{Z}[i]$ is a primitive (rn)th root of unity modulo m if and only if e^r is a primitive nth root of unity modulo m.*

Proof. (1) By

$$\Phi_n(x) \equiv \prod_{\substack{\nu=1 \\ \mathrm{GCD}(n,\nu)=1}}^{n} (x - e^\nu) \bmod m$$

(see [2]), we obtain

$$\Phi_n(e^r) \equiv 0 \bmod m.$$

Since e is a primitive nth root of unity modulo m, it follows from Theorem 1, (1) that $\mathrm{GCD}(m,n) = 1$. Using Theorem 1,(1) again, the element e^r is a primitive nth root of unity modulo m.

(2) In the case $r|n$, we have

$$\Phi_{rn}(x) = \Phi_n(x^r).$$

Further, $\mathrm{GCD}(n,m) = 1$ is equivalent to $\mathrm{GCD}(rn,m) = 1$. Applying Theorem 1,(1), we obtain the second assertion of Lemma 1. □

LEMMA 2. *Let $n, r \in \mathbb{Z}$, $n \ge 2$, $r \ge 2$, and let $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \ge 5$, be an odd Gaussian integer. Let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \ge 2$, be a primitive nth root of unity modulo m. Further, let $f \in \mathbb{Z}[i]$ be a primitive rth root of unity modulo m. If $\mathrm{GCD}(n,r) = 1$, then ef is a primitive (nr)th root of unity modulo m.*

Proof. Under the above assumptions, the following congruence is valid (see [2]),

$$\Phi_{nr}(x) \equiv \prod_{\substack{\rho=1 \\ \mathrm{GCD}(\rho,r)=1}}^{r-1} \Phi_n(f^\rho x) \bmod m.$$

Hence it follows that

$$\Phi_{nr}(ef) \equiv \prod_{\substack{\rho=1 \\ \mathrm{GCD}(\rho,r)=1}}^{r-1} \Phi_n(f^{\rho+1} e) \bmod m.$$

For $\rho = r - 1$, the above product contains the factor

$$\Phi_n(f^r e) \equiv \Phi_n(e) \equiv 0 \bmod m,$$

so that

$$\Phi_{nr}(ef) \equiv 0 \bmod m.$$

By our assumptions, and by Theorem 1,(1), we have $\mathrm{GCD}(m,n) = \mathrm{GCD}(m,r) = 1$ and hence $\mathrm{GCD}(m,nr) = 1$. Applying Theorem 1,(1) again, we obtain that ef is a primitive (nr)th root of unity modulo m. □

Remark. If the given odd Gaussian integer m possesses the prime factorization (1), then we have

$$4|\mathrm{GCD}(p_j^2 - 1, \mathrm{N}(c_k) - 1;\ j = 1,\dots,s;\ k = 1,\dots,t),$$

and hence we can choose $f = -1$ or $f = i$ for an odd integer n.

LEMMA 3. *Let $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, be an odd Gaussian integer, and let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$.*

(1) *If $n > 2$ is an odd integer, then the following conditions are equivalent:*

(i) *$\pm e$ and $\pm ie$ are primitive $(8n)$th roots of unity modulo m.*

(ii) *$\pm e^2$ are primitive $(4n)$th roots of unity modulo m.*

(iii) *e^4 is a primitive $(2n)$th root of unity modulo m.*

(iv) *$-e^4$ is a primitive nth root of unity modulo m.*

(2) *If $n \geq 2$ is an even integer, then the following conditions are equivalent:*

(v) *$\pm e$ and $\pm ie$ are primitive $(8n)$th roots of unity modulo m.*

(vi) *$\pm e^2$ and $\pm ie^2$ are primitive $(4n)$th roots of unity modulo m.*

(vii) *$\pm e^4$ are primitive $(2n)$th roots of unity modulo m.*

(viii) *e^8 is a primitive nth root of unity modulo m.*

Proof. The modulus $m \in \mathbb{Z}[i]$ is always odd. Therefore, $\mathrm{GCD}(n,m) = 1$ if and only if $\mathrm{GCD}(2n,m) = 1$.

(1) Let $n > 2$ be odd. By

$$\Phi_{8n}(\pm x) = \Phi_{8n}(\pm ix) = \Phi_{4n}(\pm x^2) = \Phi_{2n}(x^4) = \Phi_n(-x^4),$$

the first part of the lemma follows immediately from Theorem 1,(1).

(2) Let $n \geq 2$ be even. By

$$\begin{aligned}\Phi_{8n}(\pm x) &= \Phi_{8n}(\pm ix) = \Phi_{4n}(\pm x^2) = \Phi_{4n}(\pm ix^2)\\ &= \Phi_{2n}(\pm x^4) = \Phi_n(x^8),\end{aligned}$$

we obtain the second part of the lemma by Theorem 1,(1). □

Remark. Lemma 3 improves recent results of [5], [7, pp. 211–214] and [2]. Only the special cases $e = (1+i)^k$ and $e = 2^k(1+i)$, $k \geq 1$, were considered in the literature.

The following Lemma 4 gives a detailed overview in the case $e = 1 + i$ of Lemma 3. Such a case is important for practical applications, because the arithmetic in a digital computer is easy to perform for primitive nth roots of unity modulo m with a simple binary representation.

LEMMA 4. *Let $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, be an odd Gaussian integer.*

(1) *If $n > 2$ is odd, then the following conditions are equivalent:*

(i) *$\pm 1 \pm i$ are primitive $(8n)$th roots of unity modulo m.*

(ii) *$\pm 2i$ are primitive $(4n)$th roots of unity modulo m.*

(iii) -4 *is a primitive* $(2n)$*th root of unity modulo* m.

(iv) 4 *is a primitive* n*th root of unity modulo* m.

(2) *If* $n \geq 2$ *is even, then the following conditions are equivalent*:

(v) $\pm 1 \pm i$ *are primitive* $(8n)$*th roots of unity modulo* m.

(vi) $\pm 2i$ *and* ± 2 *are primitive* $(4n)$*th roots of unity modulo* m.

(vii) ± 4 *are primitive* $(2n)$*th roots of unity modulo* m.

(viii) 16 *is a primitive* n*th root of unity modulo* m.

Remark. For $e \in \mathbb{Z}[i]$, the value $\Phi_n(e)$ of the cyclotomic polynomial is a Gaussian integer, in general. But in some cases we have $\Phi_n(e) \in \mathbb{Z}$, for example,

$$\Phi_{8n}(1+i) = \Phi_{2n}(-4) \in \mathbb{Z}, \qquad n \geq 2.$$

Then Theorem 1,(1) implies that only divisors of $\Phi_{2n}(-4)$ which are relatively prime to $2n$ are possible moduli m, such that $e = 1 + i$ is a primitive $(8n)$th root of unity modulo m. In this case, the possible moduli can be obtained from the rational prime factorization of $\Phi_{2n}(-4)$. Another way is to determine the primitive divisors of $(1+i)^{8n} - 1$, where

$$(1+i)^{8n} - 1 = (2i)^{4n} - 1 = 2^{4n} - 1.$$

The rational prime factorizations of $b^n \pm 1$ for $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers of n are tabulated in [1].

Table 1 lists some important special cases for practical applications in digital signal processing. We present explicitly all possible rational moduli for some CNT's with mixed-radix length and $e = 1 + i$. These results are new (compare with [7, p. 214]) and are obtained by application of Theorem 1,(1) and rational prime factorizations of $2^n \pm 1$ (see [1, pp. ix–xvii]).

TABLE 1

Parameters for various CNT's with $e = 1 + i$ as primitive nth root of unity modulo m, where the length n is of mixed-radix form with $8|n$, and where the rational modulus $m > 1$ is an arbitrary divisor of $\Phi_n(1+i) = \Phi_{n/4}(-4)$ with $\mathrm{GCD}(m, n) = 1$. Prime divisors of $\Phi_{n/4}(-4)$ which divide n are indicated by an asterisk.

Transform length n	Rational prime factorization of $\Phi_{n/4}(-4)$
$48 = 2^4 \times 3$	241
$56 = 2^3 \times 7$	43×127
$72 = 2^3 \times 3^2$	$3^* \times 19 \times 73$
$96 = 2^5 \times 3$	97×673
$120 = 2^3 \times 3 \times 5$	151×331
$144 = 2^4 \times 3^2$	$433 \times 38\,737$
$168 = 2^3 \times 3 \times 7$	$7^* \times 337 \times 5\,419$
$200 = 2^3 \times 5^2$	$251 \times 601 \times 1\,801 \times 4\,051$
$216 = 2^3 \times 3^3$	$3^* \times 87\,211 \times 262\,657$
$280 = 2^3 \times 5 \times 7$	$71 \times 281 \times 86\,171 \times 122\,921$
$360 = 2^3 \times 3^2 \times 5$	$631 \times 23\,311 \times 18\,837\,001$
$400 = 2^4 \times 5^2$	$401 \times 340\,801 \times 2\,787\,601 \times 3\,173\,389\,601$
$504 = 2^3 \times 3^2 \times 7$	$92\,737 \times 649\,657 \times 77\,158\,673\,929$

It is sometimes desirable to compute cyclic convolutions with improved dynamic range. In this case, the same cyclic convolution can be computed modulo several relatively prime integers $m_1, \ldots, m_r$, and the final result can be obtained modulo

$(m_1 \dots m_r)$ via the Chinese remainder theorem. For this application, the availability of CNT's having the same length and defined modulo relatively prime integers is particularly interesting. For instance, a 200-dimensional cyclic convolution could be computed via the complex pseudo Mersenne number transform (with $e = 1 + i$) modulo $(2^{25} - 1)/31 = 601 \times 1\ 801$ and via the complex pseudo Fermat number transform (with $e = 1 + i$) modulo $(2^{25} + 1)/33 = 251 \times 4\ 051$ (see Table 1).

3. Construction of Convenient Moduli. From the numerical point of view, the following three essential conditions on CNT's are required:

- The transform length n has to be large enough and highly factorizable in order to implement fast algorithms.
- The primitive nth root e of unity modulo m should have a simple binary representation, so that the arithmetic modulo m is easy to perform.
- The modulus m has to be large enough to avoid overflow, but on the other hand small enough so that the machine word length is not exceeded. Furthermore, m should have a simple binary representation.

Therefore, we determine *all possible* moduli m for given length $n > 4$ and given $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, such that e is a primitive nth root of unity modulo m. We solve this question by studying cyclotomic polynomials.

Let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, be given. Further, let $c \in \mathbb{Z}[i]$ be an odd prime. If e belongs to the exponent k modulo c, then we write for short $\mathrm{ord}_c(e) = k$.

The following theorem on the prime factorization of $\Phi_n(e)$ for $e \in \mathbb{Z}[i]$ is a generalization of a known result of Kronecker (see [8, pp. 164–168]) and is proved in [12]. We see that the prime divisors of $\Phi_n(e)$ can be characterized by certain congruence conditions.

THEOREM 2 ([12]). *Let $n > 4$, and let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, be given. Further, let p be the greatest rational prime factor of n with $p^t | n$ and $p^{t+1} \nmid n$, $t \geq 1$. The number $q \in \mathbb{Z}[i]$ is defined as follows*:

$$q = \begin{cases} 2 & \text{if } n = 2^t,\ t > 2, \text{ and } e \text{ is odd}, \\ p & \text{if } p \equiv 3 \bmod 4 \text{ and } \mathrm{ord}_p(e) = n/p^t, \\ c & \text{if } p \equiv 1 \bmod 4,\ \mathrm{N}(c) = p \text{ and } \mathrm{ord}_c(e) = n/p^t \neq \mathrm{ord}_{\bar{c}}(e), \\ p & \text{if } p \equiv 1 \bmod 4,\ \mathrm{N}(c) = p \text{ and } \mathrm{ord}_c(e) = n/p^t = \mathrm{ord}_{\bar{c}}(e), \\ 1 & \text{otherwise}. \end{cases}$$

Then the value $\Phi_n(e)$ of the nth cyclotomic polynomial Φ_n possesses a prime factorization of the following type

$$\Phi_n(e) = i^h q \prod z^{s(z)}, \tag{3}$$

where $h \in \{0, 1, 2, 3\}$ and $\prod$ is defined as the product of all those primes $z \in \mathbb{Z}[i]$, $\mathrm{N}(z) > 2$, with $\mathrm{ord}_z(e) = n$. Further, $s(z)$ denotes that positive integer s with $z^s | e^n - 1$ and $z^{s+1} \nmid e^n - 1$. Except for

$$(n, e) = (5, -1 \pm i), (6, 1 \pm i), (6, 2), (10, 1 \pm i), \tag{4}$$

there exists at least one prime $z \in \mathbb{Z}[i]$, $\mathrm{N}(z) > 2$, with $\mathrm{ord}_z(e) = n$.

From the above result and Theorem 1, the following construction of suitable moduli is obtained.

THEOREM 3. *Let $n > 4$, and let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, be given, where the cases (4) are omitted. Under these assumptions, e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) > 1$, is a divisor of $\Phi_n(e)/q$.*

Remark. By Theorem 1,(4) and Theorem 3, it follows that under the above assumptions, m is a primitive divisor of $e^n - 1$ if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) > 1$, is a divisor of $\Phi_n(e)/q$.

Proof of Theorem 3. (1) Let $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) > 1$, be a divisor of $\Phi_n(e)/q$. By (3), it follows that m is odd and hence $\mathrm{N}(m) \geq 5$, and that $\Phi_n(e) \equiv 0 \bmod m$ and $\mathrm{GCD}(m, n) = 1$. Using Theorem 1,(1), e is a primitive nth root of unity modulo m.

(2) If e is a primitive nth root of unity modulo m, then $m | \Phi_n(e)$ and $\mathrm{GCD}(m, n) = 1$ by Theorem 1,(1). Then Theorem 2 implies $m | \Phi_n(e)/q$. □

If we compare Theorem 1,(1) and Theorem 3, then we see that Theorem 3 is more precise than Theorem 1,(1). Note that there exists only a finite number of moduli m for given transform length $n > 4$ and given Gaussian integer e, $\mathrm{N}(e) \geq 2$, such that e is a primitive nth root of unity modulo m. Further, we remark that m is always an odd Gaussian integer with $\mathrm{N}(m) \geq 5$. Many interesting results can be obtained as simple corollaries of Theorem 3.

COROLLARY 1. *Let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, and let $n = 2^{d+1}$, $d > 1$. Further, let*

$$q = \begin{cases} 2 & \textit{if } e \textit{ is odd}, \\ 1 & \textit{otherwise}. \end{cases}$$

Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of $\Phi_n(e)/q$, where

$$\Phi_n(x) = x^{2^d} + 1.$$

Examples. In the case $e = 2i$ and $n = 2^{d+1}$, $d > 1$, we have $q = 1$. Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of the Fermat number

$$\Phi_n(2i) = 2^{2^d} + 1.$$

In the case $e = 1 + i$ and $n = 2^{d+2}$, $d > 1$, we obtain $q = 1$. Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of the Fermat number

$$\Phi_n(1 + i) = 2^{2^d} + 1.$$

COROLLARY 2. *Let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$, and let $n = 2^{d+1}p^t$, $d \geq 1$, $t \geq 1$, where $p > 2$ is a rational prime. In the case $p \equiv 3 \bmod 4$, we set*

$$q = \begin{cases} p & \textit{if } \mathrm{ord}_p(e) = 2^{d+1}, \\ 1 & \textit{otherwise}. \end{cases}$$

In the case $p \equiv 1 \bmod 4$ with $a^2 + b^2 = p$, $a, b \in \mathbb{Z}$, we set $c = a + bi$ and

$$q = \begin{cases} c & \textit{if } \mathrm{ord}_c(e) = 2^{d+1} \neq \mathrm{ord}_{\bar{c}}(e), \\ p & \textit{if } \mathrm{ord}_c(e) = 2^{d+1} = \mathrm{ord}_{\bar{c}}(e), \\ 1 & \textit{otherwise}. \end{cases}$$

Under these assumptions, e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, *is a divisor of* $\Phi_n(e)/q$, *where*

$$\Phi_n(x) = (x^{n/2}+1)(x^{n/(2p)}+1)^{-1}.$$

Examples. In the case $e = 2i$ and $n = 4p$, where $p > 3$ is a rational prime, we obtain $q = 1$. Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of

$$\Phi_n(2i) = \frac{2^p+1}{3}(2^p-1).$$

Note that the corresponding CNT's are called *complex pseudo Fermat number transform* and *complex pseudo Mersenne number transform*, respectively [7, pp. 210–216], [9], [10, p. 238].

In the case $e = 2i$ and $n = 4 \times 3^t$, $t \geq 1$, we have $q = 3$. Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of

$$\Phi_n(2i)/3 = \frac{2^{2\cdot 3^{t-1}} - 2^{3^{t-1}} + 1}{3}(2^{2\cdot 3^{t-1}} + 2^{3^{t-1}} + 1).$$

In the case $e = 1+i$ and $n = 8p$, where $p > 3$ is a rational prime, we obtain $q = 1$. Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of

$$\Phi_n(1+i) = \frac{2^p+1}{3}(2^p-1).$$

Note that the corresponding CNT's are called complex pseudo Fermat number transform and complex pseudo Mersenne number transform, respectively [7, pp. 210–216], [9], [10, p. 238].

In the case $e = 1+i$ and $n = 8 \times 3^t$, $t \geq 1$, we get $q = 3$. Then e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is a divisor of

$$\Phi_n(1+i)/3 = \frac{2^{2\cdot 3^{t-1}} - 2^{3^{t-1}} + 1}{3}(2^{2\cdot 3^{t-1}} + 2^{3^{t-1}} + 1).$$

COROLLARY 3. *Let* p_1 *and* p *be rational primes with* $2 < p_1 < p$, *and let* $n = 2^{d+1}p_1^s p^t$, $d \geq 0$, $s \geq 1$, $t \geq 1$. *Let* $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$. *In the case* $p \equiv 3 \bmod 4$, *we set*

$$q = \begin{cases} p & \textit{if } \mathrm{ord}_p(e) = n/p^t, \\ 1 & \textit{otherwise.} \end{cases}$$

In the case $p \equiv 1 \bmod 4$ *with* $a^2 + b^2 = p$, $a, b \in \mathbb{Z}$, *we set* $c = a + bi$ *and*

$$q = \begin{cases} c & \textit{if } \mathrm{ord}_c(e) = n/p^t \neq \mathrm{ord}_{\bar{c}}(e), \\ p & \textit{if } \mathrm{ord}_c(e) = n/p^t = \mathrm{ord}_{\bar{c}}(e), \\ 1 & \textit{otherwise.} \end{cases}$$

Under these assumptions, e is a primitive nth root of unity modulo m if and only if $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, *is a divisor of* $\Phi_n(e)/q$, *where*

$$\Phi_n(x) = (x^{n/2}+1)(x^{n/(2p_1p)}+1)(x^{n/(2p_1)}+1)^{-1}(x^{n/(2p)}+1)^{-1}.$$

The advantage of the CNT over the corresponding rational transform is that the transform length is larger for the same modulus (see Table 2).

TABLE 2

Parameters e, n and m for CNT's, where $m \in \mathbb{Z}[i]$, $\mathrm{N}(m) \geq 5$, is an arbitrary divisor of $\Phi_n(e)/q$, such that e is a primitive nth root of unity modulo m. Here the integer q is explained in Theorem 2.

e	n	q	$\Phi_n(e)$
2	2^{d+1} $d \geq 1$	1	$2^{2^d}+1$
$2i$	2^{d+1} $d \geq 2$	1	$2^{2^d}+1$
$1+i$	2^{d+2} $d \geq 2$	1	$2^{2^d}+1$
2	3^t $t \geq 1$	1	$(2^{3^t}-1)(2^{3^{t-1}}-1)^{-1}$
$2i$	4×3^t $t \geq 1$	3	$(2^{3^t}-1)(2^{3^t}+1)(2^{3^{t-1}}-1)^{-1}(2^{3^{t-1}}+1)^{-1}$
$1+i$	8×3^t $t \geq 1$	3	$(2^{3^t}-1)(2^{3^t}+1)(2^{3^{t-1}}-1)^{-1}(2^{3^{t-1}}+1)^{-1}$
2	p^t p prime, $t \geq 1$	1	$(2^{p^t}-1)(2^{p^{t-1}}-1)^{-1}$
$2i$	$4p^t$ $p > 3$ prime, $t \geq 1$	1	$(2^{p^t}-1)(2^{p^t}+1)(2^{p^{t-1}}-1)^{-1}(2^{p^{t-1}}+1)^{-1}$
$1+i$	$8p^t$ $p > 3$ prime, $t \geq 1$	1	$(2^{p^t}-1)(2^{p^t}+1)(2^{p^{t-1}}-1)^{-1}(2^{p^{t-1}}+1)^{-1}$
2	$2^{d+1} \times 3^t$ $d \geq 2,\ t \geq 1$	1	$(2^{2^d 3^t}+1)(2^{2^d 3^{t-1}}+1)^{-1}$
$2i$	$2^{d+1} \times 3^t$ $d \geq 2,\ t \geq 1$	1	$(2^{2^d 3^t}+1)(2^{2^d 3^{t-1}}+1)^{-1}$
$1+i$	$2^{d+2} \times 3^t$ $d \geq 2,\ t \geq 1$	1	$(2^{2^d 3^t}+1)(2^{2^d 3^{t-1}}+1)^{-1}$

4. Connection Between Complex and Rational Moduli. Theorem 3 yields the result that in general the suitable moduli m are Gaussian integers. However, for practical applications usually rational integers (instead of Gaussian integers) are more convenient as moduli of CNT's. Therefore we consider now a complex modulus $m = s + ti \in \mathbb{Z}[i]$ with $st \neq 0$ and $\mathrm{GCD}(s,t) = 1$, and we ask which properties does a primitive nth root $e \in \mathbb{Z}[i]$ of unity modulo m possess.

LEMMA 5. *Let $m = s + ti \in \mathbb{Z}[i]$ with $st \neq 0$ and $\mathrm{GCD}(s,t) = 1$ be given. Then we have*

$$\mathbb{Z}[i]/m\mathbb{Z}[i] \cong \mathbb{Z}/\mathrm{N}(m)\mathbb{Z} \tag{5}$$

with the correspondence for arbitrary $x + yi \in \mathbb{Z}[i]$

$$(x + yi) + m\mathbb{Z}[i] \leftrightarrow (x + (t\lambda - s\mu)y) + \mathrm{N}(m)\mathbb{Z},$$

where $\lambda, \mu \in \mathbb{Z}$ are determined by $s\lambda + t\mu = 1$.

Proof. (1) We define a mapping of the ring $\mathbb{Z}$ into the residue class ring $\mathbb{Z}[i]/m\mathbb{Z}[i]$ by

$$x \to x + m\mathbb{Z}[i] \tag{6}$$

for arbitrary $x \in \mathbb{Z}$. From the properties of the ideal $m\mathbb{Z}[i]$, it follows that

$$x + w \to (x+w) + m\mathbb{Z}[i],$$
$$x \cdot w \to (x \cdot w) + m\mathbb{Z}[i]$$

for all $x, w \in \mathbb{Z}$.

(2) Now we show that an arbitrary residue class $(x+yi) + m\mathbb{Z}[i]$, $x, y \in \mathbb{Z}$, of $\mathbb{Z}[i]/m\mathbb{Z}[i]$ can be represented in the form $w + m\mathbb{Z}[i]$ with some $w \in \mathbb{Z}$. Since $\mathrm{GCD}(s,t) = 1$, there exist $\lambda, \mu \in \mathbb{Z}$ with $s\lambda + t\mu = 1$. Then by $m(\mu + \lambda i) = (s\mu - t\lambda) + i$, it follows that

$$(x+yi) + m\mathbb{Z}[i] = (x + (t\lambda - s\mu)y) + m\mathbb{Z}[i].$$

Consequently, a homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}[i]/m\mathbb{Z}[i]$ is defined by (6).

(3) Let $k\mathbb{Z}$, $k \in \mathbb{Z}$, be the kernel of this homomorphism (6). Obviously, we have $k\mathbb{Z} = \mathbb{Z} \cap m\mathbb{Z}[i]$. Since $m|k$ and $\bar{m}|k$, we can choose $k = m\bar{m} = \mathrm{N}(m)$. Using the homomorphism theorem for rings, we obtain the isomorphism (5). □

By Lemma 5, we obtain immediately the following result on the connection between complex and rational moduli.

THEOREM 4. *Let $m = s + ti \in \mathbb{Z}[i]$ with $st \neq 0$ and* $\mathrm{GCD}(s,t) = 1$ *be given. Let $\lambda, \mu \in \mathbb{Z}$ be determined by $s\lambda + t\mu = 1$.*

The Gaussian integer $e = a + bi$ is a primitive nth root of unity modulo m if and only if the rational integer $e' = a + (t\lambda - s\mu)b$ is a primitive nth root of unity modulo $\mathrm{N}(m)$.

Example. By

$$\Phi_5(2i) = ((2i)^5 - 1)/(2i - 1) = (2+i)(4-5i)$$

and $\mathrm{GCD}(4-5i, 5) = 1$, we conclude from Theorem 1,(1) or Theorem 3 that $e = 2i$ is a primitive 5th root of unity modulo $m = 4 - 5i$. Then we have $\lambda = \mu = -1$. By Lemma 5, we obtain the isomorphism

$$\mathbb{Z}[i]/(4-5i)\mathbb{Z}[i] \cong \mathbb{Z}/41\,\mathbb{Z},$$

such that especially

$$2i + (4-5i)\mathbb{Z}[i] \leftrightarrow 18 + 41\,\mathbb{Z}.$$

Hence, $e' = 18$ is a primitive 5th root of unity modulo 41. In order to perform a simple binary arithmetic for an NTT with $e' = 18$ as primitive 5th root of unity modulo 41, we can set $e' = 2j$ with $j \equiv 9 \bmod 41$ and $j^2 \equiv -1 \bmod 41$.

5. Primitive Roots of Unity Modulo a Mersenne Prime. In order to implement fast transforms in digital computers, moduli m with simple binary representation are important for practical applications. Hence prime moduli of the form $m = 2^p - 1$, where p is a rational prime, are studied very intensively (see [7, pp. 203–208], [11]). Such integers are called Mersenne primes. The corresponding CNT's are called *complex Mersenne number transforms*. Short proofs and some improvements of results in [7, pp. 205–206] and [11] follow immediately from Theorem 1.

THEOREM 5 ([11]). *Let p be a rational prime, and let $m = 2^p - 1$ be a Mersenne prime. Further let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$. Under these assumptions, e is a primitive (m^2-1)th root of unity modulo m if and only if* $\mathrm{N}(e)$ *is a primitive $(m-1)$th root of unity modulo m, i.e.,* $\mathrm{N}(e)$ *is a primitive root modulo m.*

Proof. (1) Let $e = a + bi \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$. Since m is a rational prime $\equiv 3 \bmod 4$, the binomial formula and Fermat's theorem in $\mathbb{Z}$ imply

$$(a+bi)^m \equiv a^m + b^m i^m \equiv a - bi \bmod m$$

and hence

$$(a+bi)^{2^p} = (a+bi)^{m+1} \equiv a^2 + b^2 \equiv \mathrm{N}(e) \bmod m. \tag{7}$$

(2) By

$$m^2 - 1 = 2^{p+1}(2^{p-1} - 1), \qquad m - 1 = 2(2^{p-1} - 1),$$

the integers m^2-1 and $m-1$ have the same rational prime divisors $p_1 = 2, p_2, \dots, p_s$. From (7) it follows that the condition

$$e^{m^2-1} \equiv 1 \bmod m$$

is equivalent to $\mathrm{N}(e)^{m-1} \equiv 1 \bmod m$. Further, by (7),

$$e^{(m^2-1)/p_k} \not\equiv 1 \bmod m, \qquad k = 1, \dots, s,$$

is equivalent to

$$\mathrm{N}(e)^{(m-1)/p_k} \not\equiv 1 \bmod m, \qquad k = 1, \dots, s.$$

Since m is also a prime in $\mathbb{Z}[i]$, the assertion follows from Theorem 1,(2). □

COROLLARY 4 ([11]). *Let p be a rational prime, and let $m = 2^p - 1$ be a Mersenne prime. Further let $a = 2^{(p-1)/2} + 1$ and $b = 2^{(p-1)/2} - 1$. Then $e = a + bi \in \mathbb{Z}[i]$ is a primitive (m^2-1)th root of unity modulo m if and only if 3 is a primitive $(m-1)$th root of unity modulo m, i.e., 3 is a primitive root modulo m.*

Proof. From Theorem 5 it follows that $e = a + bi \in \mathbb{Z}[i]$ is a primitive (m^2-1)th root modulo m if and only if $\mathrm{N}(e) = a^2 + b^2 = m + 3$ is a primitive $(m-1)$th root of unity modulo m. This is valid if and only if 3 is a primitive root modulo m. □

THEOREM 6 ([7, p. 205]). *Let p be a rational prime, and let $m = 2^p - 1$ be a Mersenne prime. Further let $n = 2^k$, $2 < k \leq p + 1$, and let $e \in \mathbb{Z}[i]$, $\mathrm{N}(e) \geq 2$. Under these assumptions, e is a primitive nth root of unity modulo m if and only if $e^{n/2} \equiv -1 \bmod m$.*

Proof. By

$$n | m^2 - 1 = 2^{p+1}\ (2^{p-1} - 1),$$

the existence of primitive nth roots of unity modulo m is clear (see (2)). Applying Theorem 1,(1), the assertion follows from $\mathrm{GCD}(n, m) = 1$ and $\Phi_n(e) = e^{n/2} + 1 = 0 \bmod m$. □

COROLLARY 5 ([7, pp. 205–206]). *Let $p > 2$ be a rational prime, and let $m = 2^p - 1$ be a Mersenne prime. Further, let $a, b \in \mathbb{Z}$ with*

$$a \equiv \pm 2^{2^{p-2}} \bmod m, \qquad b \equiv \pm(-3)^{2^{p-2}} \bmod m$$

be given. Then $e = a + bi \in \mathbb{Z}[i]$ is a primitive (2^{p+1})th root of unity modulo m.

Proof. By Theorem 1,(1) and by $\mathrm{GCD}(2, m) = 1$, we have only to show that

$$(a + bi)^{2^p} + 1 \equiv 0 \bmod m. \tag{8}$$

(1) By the first step of the proof of Theorem 5, we have (7). By assumption, it follows that

$$a^2 \equiv 2^{2^{p-1}} \bmod m, \qquad b^2 \equiv (-3)^{2^{p-1}} \bmod m. \tag{9}$$

(2) Both 2 and -3 are quadratic residues modulo $m = 2^p - 1$ (see [8, p. 136 and p. 144]). Then by Euler's criterion, we obtain

$$1 \equiv 2^{(m-1)/2} \bmod m, \qquad 1 \equiv (-3)^{(m-1)/2} \bmod m,$$

i.e.,

$$2 \equiv 2^{(m+1)/2} \bmod m, \qquad -3 \equiv (-3)^{(m+1)/2} \bmod m \tag{10}$$

with $(m + 1)/2 = 2^{p-1}$. From (7), (9) and (10), there follows (8). □

Akademie der Wissenschaften der DDR
Zentralinstitut für Kybernetik und Informationsprozesse
Postfach 1298
DDR–1086 Berlin, German Democratic Republic

Sektion Mathematik
Wilhelm-Pieck-Universität Rostock
Universitätsplatz 1
DDR–2500 Rostock, German Democratic Republic

1. J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN & S. S. WAGSTAFF, JR., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers*, Contemp. Math., vol. 22, Amer. Math. Soc., Providence, R. I., 1983.

2. R. CREUTZBURG, *Finite Signalfaltungen und finite Signaltransformationen in endlichen kommutativen Ringen mit Einselement*, Dissertation, Wilhelm-Pieck-Universität Rostock, 1984.

3. R. CREUTZBURG & M. TASCHE, "*F*-Transformation und Faltung in kommutativen Ringen," *Elektron. Informationsverarb. Kybernet.*, v. 21, 1985, pp. 129–149.

4. R. CREUTZBURG & M. TASCHE, "Number-theoretic transforms of prescribed length," *Math. Comp.*, v. 47, 1986, pp. 693–701.

5. E. DUBOIS & A. N. VENETSANOPOULOS, "The generalized discrete Fourier transform in rings of algebraic integers," *IEEE Trans. Acoust. Speech Signal Process.*, v. 28, 1980, pp. 169–175.

6. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1954.

7. J. H. MCCLELLAN & C. M. RADER, *Number Theory in Digital Signal Processing*, Prentice-Hall, Englewood Cliffs, N. J., 1979.

8. T. NAGELL, *Introduction to Number Theory*, Wiley, New York, 1951.

9. H. J. NUSSBAUMER, "Relative evaluation of various number theoretic transforms for digital filtering applications," *IEEE Trans. Acoust. Speech Signal Process.*, v. 26, 1978, pp. 88–93.

10. H. J. NUSSBAUMER, *Fast Fourier Transform and Convolution Algorithms*, Springer-Verlag, Berlin, 1981.

11. I. S. REED, T. K. TRUONG & R. L. MILLER, "A new algorithm for computing primitive elements in the field of Gaussian complex integers modulo a Mersenne prime," *IEEE Trans. Acoust. Speech Signal Process.*, v. 27, 1979, pp. 561–563.

12. G. DRAUSCHKE & M. TASCHE, "Prime factorizations for values of cyclotomic polynomials in $\mathbb{Z}[i]$," *Arch. Math.*, v. 49, 1987, pp. 292–300.