MATHEMATICS OF COMPUTATION
VOLUME 47, NUMBER 176
OCTOBER 1986, PAGES 693–701

Number-Theoretic Transforms of Prescribed Length

By R. Creutzburg and M. Tasche

Abstract. A new constructive method for finding all convenient moduli m for a number-theoretic transform with given length N and given primitive Nth root of unity modulo m is presented. This method is based on the prime factorization of cyclotomic polynomials with integer-valued argument or on the primitive divisors of integers. Many known results can be obtained as simple corollaries.

1. Introduction. 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 round-off errors [8], [11]. A large number of transform methods were developed to remove some of the length limitations of conventional Fermat number and Mersenne number transforms [6], [10, pp. 216–219 and 222–224]. These NTT's, which under certain conditions can be computed via fast transform algorithms, allow the implementation of digital signal processing operations with better efficiency and accuracy than the fast Fourier transform. However, it is always difficult to find moduli m that are large enough to avoid overflow, and to find primitive Nth roots of unity modulo m with minimal binary weight for transform lengths N that are highly factorizable and large enough for practical applications. In this note, a useful way is shown to solve this problem by studying cyclotomic polynomials and primitive divisors of integers.

2. Primitive Roots of Unity Modulo m. Let $\mathbb{Z}$ be the ring of integers and $m > 1$ an odd integer with prime factorization

$$m = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}. \tag{1}$$

Then $\alpha \in \mathbb{Z}$ is called a primitive Nth root of unity modulo m if

$$\begin{aligned} &\alpha^N \equiv 1 \bmod m, \\ &\mathrm{GCD}(\alpha^n - 1, m) = 1, \qquad n = 1, \ldots, N-1. \end{aligned} \tag{2}$$

By definition, $\alpha = 1$ is a primitive first root of unity modulo m. If $\alpha \in \mathbb{Z}$ is a primitive Nth root of unity modulo m, then α belongs to the exponent N modulo m, but, in general, the converse is not true.

Note that by (2) the integer $m > 1$ is a primitive divisor of $\alpha^N - 1$ (i.e., m is a divisor of $\alpha^N - 1$ with the property $\mathrm{GCD}(\alpha^n - 1, m) = 1$ for $n = 1, \ldots, N-1$).

Received June 20, 1985; revised November 12, 1985.
1980 *Mathematics Subject Classification.* Primary 94A11, 10A10.
Key words and phrases. Number-theoretic transform, primitive root of unity modulo m, primitive divisor, cyclotomic polynomial.

0025-5718/86 $1.00 + $.25 per page

Remark. The definition and properties of primitive roots of unity in a finite field can be found in [7, pp. 63–66]. For a detailed discussion of primitive roots of unity in a finite commutative ring R with unity, the reader is referred to [4]. Here we consider the important special case $R = \mathbb{Z}/m\mathbb{Z}$, where $m > 1$ is an odd integer.

The following theorem gives criteria for an integer to be a primitive Nth root of unity modulo m. We denote the Nth cyclotomic polynomial by Φ_N.

THEOREM 1 ([3], [4]). *Let $m > 1$ be an odd integer. A number $\alpha \in \mathbb{Z}$, $|\alpha| \geqslant 2$, is a primitive Nth root of unity modulo m if and only if one of the following conditions holds*:

(1) $\Phi_N(\alpha) \equiv 0 \bmod m$, $\mathrm{GCD}(N, m) = 1$;

(2) $\alpha^N \equiv 1 \bmod m$, $\mathrm{GCD}(N, m) = 1$, $\sum_{k=0}^{(N/d)-1} \alpha^{dk} \equiv 0 \bmod m$ *for every divisor* $d \geqslant 1$ *of* N, *such that* N/d *is prime*;

(3) $\alpha^N \equiv 1 \bmod m$, $\mathrm{GCD}(\alpha^d - 1, m) = 1$ *for every divisor* $d \geqslant 1$ *of* N, *such that* N/d *is prime*;

(4) $\alpha^N \equiv 1 \bmod p_i^{r_i}$, $i = 1, \ldots, s$, $\alpha^d \not\equiv 1 \bmod p_i$, $i = 1, \ldots, s$, *for every divisor* $d \geqslant 1$ *of* N, *such that* N/d *is prime*;

(5) m *is a primitive divisor of* $\alpha^N - 1$.

A necessary and sufficient condition for the existence of a primitive Nth root of unity modulo m [1], [10, p. 215] is

$$N \mid \mathrm{GCD}(p_1 - 1, \ldots, p_s - 1). \tag{3}$$

Condition (3) implies the existence of $\varphi(N)^s$ incongruent primitive Nth roots of unity modulo m [3]. Here φ denotes Euler's totient function.

Remark. The order N and the number $\varphi(N)^s$ of primitive Nth roots of unity modulo m depend only on the prime divisors of the modulus m, and do not depend on the exponents of the prime divisors in (1).

The concept of the primitive Nth root of unity modulo m is fundamental 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-point integer vectors, and let $m > 1$ be a fixed odd integer. Note that 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 *number-theoretic transform* (NTT) of length N with α as a primitive Nth root of unity modulo m, and its *inverse*, are defined to be the following mappings between N-point integer vectors $\mathbf{x} = [x_0, \ldots, x_{N-1}]$ and $\mathbf{X} = [X_0, \ldots, X_{N-1}]$,

$$X_n \equiv \sum_{k=0}^{N-1} x_k \alpha^{nk} \bmod m, \qquad n = 0, \ldots, N - 1,$$

$$x_k \equiv N' \sum_{n=0}^{N-1} X_n \alpha^{-nk} \bmod m, \qquad k = 0, \ldots, N - 1,$$

where $N'N \equiv 1 \bmod m$. Note that there exists such an integer N' by $\mathrm{GCD}(N, m) = 1$ (see Theorem 1, (1)). We denote this correspondence by

$$\mathbf{x} \overset{\mathrm{NTT}}{\Leftrightarrow} \mathbf{X}.$$

The NTT has a structure and properties resembling those of the DFT [4], [10, pp. 211–216], particularly the cyclic convolution property:

$$\mathbf{x} * \mathbf{y} \overset{\mathrm{NTT}}{\Leftrightarrow} \mathbf{X} \circ \mathbf{Y} = [X_0 Y_0, \ldots, X_{N-1} Y_{N-1}],$$

where $*$ denotes the cyclic convolution and $\circ$ signifies the Hadamard product.

3. Construction of Primitive Roots of Unity Modulo m. The following algorithm allows us to calculate all $\varphi(N)^s$ primitive Nth roots of unity modulo m for a given odd modulus $m > 1$ (with (1)) and for a suitably chosen order $N > 2$ satisfying condition (3). Let n_i $(i = 1, \ldots, s)$ be arbitrary integers with $1 \leqslant n_i \leqslant N - 1$ and $\mathrm{GCD}(n_i, N) = 1$. Further, let g_i be a primitive root modulo p_i $(i = 1, \ldots, s)$.

Step 1. Calculate $\varphi(N)$ primitive Nth roots of unity modulo $p_i^{r_i}$ by

$$\alpha_{i,n_i} \equiv g_i^{\varphi(p_i^{r_i})n_i/N} \bmod p_i^{r_i}, \qquad i = 1, \ldots, s.$$

Step 2. Calculate $\varphi(N)^s$ primitive Nth roots of unity modulo m by the Chinese Remainder Theorem

$$\alpha \equiv \sum_{i=1}^{s} \left(mp_i^{-r_i}\right)\alpha_{i,n_i}t_i \bmod m,$$

with

$$\left(mp_i^{-r_i}\right)t_i \equiv 1 \bmod p_i^{r_i}.$$

For a proof of this algorithm, the reader is referred, e.g., to [3].

If a primitive Nth root of unity modulo m is known, then in some cases it is possible to obtain a primitive $(2N)$th root of unity modulo m.

THEOREM 2. *Let $m > 1$ be an odd integer.*

(1) *Let $N > 2$ be odd. The integer α $(|\alpha| \geqslant 2)$ is a primitive Nth root of unity modulo m if and only if $-\alpha$ is a primitive $(2N)$th root of unity modulo m.*

(2) *Let $N = 2^{n-1}N'$ with $n \geqslant 4$ and an odd $N' \geqslant 1$ be given. If 2 is a primitive Nth root of unity modulo m, then $\beta = 2^{N/8}(2^{N/4} - 1)$ is a primitive $(2N)$th root of unity modulo m with $\beta^2 \equiv 2 \bmod m$.*

Proof. (1) Let $N > 2$ be odd. By Theorem 1, (1), the integer α is a primitive Nth root of unity modulo m if and only if $\Phi_N(\alpha) \equiv 0 \bmod m$ and $\mathrm{GCD}(N, m) = 1$. By $\Phi_N(x) = \Phi_{2N}(-x)$, this condition is equivalent to $\Phi_{2N}(-\alpha) \equiv 0 \bmod m$ and $\mathrm{GCD}(2N, m) = 1$, i.e., $-\alpha$ is a primitive $(2N)$th root of unity modulo m by Theorem 1, (1).

(2) Now let $N = 2^{n-1}N'$ with $n \geqslant 4$ and an odd $N' \geqslant 1$ be given. If 2 is a primitive Nth root of unity modulo m, then it follows by Theorem 1, (3), that

$$2^N - 1 = (2^{N/2} - 1)(2^{N/2} + 1) \equiv 0 \bmod m$$

and $\mathrm{GCD}(2^{N/2} - 1, m) = 1$. Hence $2^{N/2} \equiv -1 \bmod m$. For $\beta = 2^{N/8}(2^{N/4} - 1)$, we obtain

$$\beta^2 = 2^{N/4}(2^{N/2} - 2 \cdot 2^{N/4} + 1) \equiv -2 \cdot 2^{N/2} \equiv 2 \bmod m.$$

Applying $\Phi_{2N}(x) = \Phi_N(x^2)$ for even N, we get by Theorem 1, (1),

$$\Phi_{2N}(\beta) = \Phi_N(\beta^2) \equiv \Phi_N(2) \equiv 0 \bmod m$$

and $\mathrm{GCD}(N, m) = 1$, since 2 is a primitive Nth root of unity modulo m. Then there also holds $\mathrm{GCD}(2N, m) = 1$. Again using Theorem 1, (1), β is a primitive $(2N)$th root of unity modulo m. □

Let α be a primitive Nth root of unity modulo m. In order to perform fast multiplication by powers of α in the NTT, it is desirable to choose an α with small binary weight. With the help of the above algorithm, it is possible to select from all

$\varphi(N)^s$ primitive Nth roots of unity modulo m that integer with minimal binary weight. The following example readily shows that the binary representation of primitive Nth roots of unity modulo m can be complicated.

Example. The integers ± 57 and ± 307 are all primitive 4th roots of unity modulo $1625 = 5^3 \cdot 13$. By $57 = 2^5 + 2^4 + 2^3 + 2^0$ and $307 = 2^8 + 2^5 + 2^4 + 2^1 + 2^0$, the minimal binary weight of the above integers is 4 (see also [6]).

From the numerical point of view, the following three essential conditions on NTT's are required:

- —The length N has to be large enough and highly factorizable in order to implement fast algorithms like prime-factor, Winograd, single-radix, or mixed-radix algorithms [10, pp. 85–94, 116–120, and 125–144];
- —The primitive Nth root α of unity modulo m should have a simple binary representation ($\alpha = 2$, for example), 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.

For instance, the Fermat number transform with $N = 2^{d+1}$ ($d > 0$), $\alpha = 2$ and $m = 2^{2^d} + 1$ is a compromise between these various conditions, but its length limitations are well known (see [5], [10, pp. 222–224], or Corollary 3). It is clear that the above algorithm does not, in general, fulfil the required conditions. Therefore, in the following section we determine, by studying cyclotomic polynomials, all possible moduli m for given $N > 2$ and given $\alpha \in \mathbb{Z}$ ($|\alpha| \geqslant 2$) such that α is a primitive Nth root of unity modulo m.

4. Construction of Convenient Moduli. An important question for practical application is the following: Is it possible to find convenient moduli m for NTT's, if a highly factorizable length N and an integer α with small binary weight are prescribed, such that α is a primitive Nth root of unity modulo m?

The following result originates with Kronecker and was developed in detail later.

THEOREM 3 ([13]). *Let $N > 2$ and $\alpha \in \mathbb{Z}$ ($|\alpha| \geqslant 2$) be given. Let p be the greatest prime factor of N with $p^t \mid N$ and $p^{t+1} \nmid N$ ($t \geqslant 1$), and let*

$$\tau_p = \begin{cases} 1 & \text{if } \alpha \text{ belongs to the exponent } N/p^t \text{ modulo } p, \\ 0 & \text{otherwise.} \end{cases}$$

Then the value $\Phi_N(\alpha)$ of the Nth cyclotomic polynomial Φ_N possesses the prime factorization

$$\Phi_N(\alpha) = p^{\tau_p} \prod q^{\mu_q},$$

where $\prod$ is defined as the product of all primes $q > 2$, such that α belongs to the exponent N modulo q. For these primes $q > 2$, μ_q denotes that integer $\mu \geqslant 1$ with $q^\mu \mid \alpha^N - 1$ and $q^{\mu+1} \nmid \alpha^N - 1$. If further $(N, \alpha) \neq (3, -2), (6, 2)$, then the integer

$$M = \Phi_N(\alpha)/p^{\tau_p} > 1 \tag{4}$$

possesses only prime factors $\equiv 1 \bmod N$.

With the help of Theorems 1 and 3, the following construction of suitable moduli is obtained.

THEOREM 4. *Let* $N > 2$ *and* $\alpha \in \mathbb{Z}$ $(|\alpha| \geqslant 2)$ *be given, where* $(N, \alpha) \neq (3, -2)$, $(6, 2)$. *Under these assumptions,* α *is a primitive* N*th root of unity modulo* m *if and only if* $m > 1$ *is a divisor of* M *given by* (4).

Remark. By Theorems 1,(5) and 4, it follows that under the above assumptions, m is a primitive divisor of $\alpha^N - 1$ if and only if $m > 1$ is a divisor of (4).

Proof of Theorem 4. (1) Let $m > 1$ be a divisor of M. Then one has $\Phi_N(\alpha) \equiv 0 \bmod m$ and $\mathrm{GCD}(N, m) = 1$ by Theorem 3. Using Theorem 1, (1), α is a primitive Nth root of unity modulo m.

(2) If α is a primitive Nth root of unity modulo m, then $m \mid \Phi_N(\alpha)$ and $\mathrm{GCD}(N, m) = 1$ by Theorem 1, (1). Theorem 3 implies $m \mid M$. □

Note that there exists only a finite number of moduli m for given transform length N and given integer α, such that α is a primitive Nth root of unity modulo m.

Known results of Erdelsky [10, pp. 231 and 234] and others can be obtained as simple corollaries of Theorems 2 and 4.

COROLLARY 1 ([10, pp. 231 and 234]). *Let* p *be prime,* $N = p^t > 2$ $(t \geqslant 1)$ *and* $\alpha \in \mathbb{Z}$ $(|\alpha| \geqslant 2)$ *with* $(N, \alpha) \neq (3, -2)$. *The integer* α *is a primitive* N*th root of unity modulo* m *if and only if* $m > 1$ *is a divisor of the integer*

$$M = \begin{cases} \Phi_N(\alpha)/p & \text{if } \alpha \equiv 1 \bmod p, \\ \Phi_N(\alpha) & \text{otherwise}, \end{cases} \tag{5}$$

with

$$\Phi_N(x) = (x^N - 1)(x^{N/p} - 1)^{-1}. \tag{6}$$

Furthermore, for $p > 2$, *the integer* $-\alpha$ *is a primitive* $(2N)$*th root of unity modulo* m *if and only if* $m > 1$ *is a divisor of* (5).

Proof. Using the notation of Theorem 3, we observe that

$$\tau_p = \begin{cases} 1 & \text{if } \alpha \equiv 1 \bmod p, \\ 0 & \text{otherwise.} \end{cases}$$

Hence (5) follows from (4). To complete the first part of the proof, we apply Theorem 4. For $p > 2$, we can apply the first assertion of this corollary and Theorem 2. □

Note that in Corollary 1, the discussion of the case $\alpha \equiv 1 \bmod p$ is new, so that we improve Erdelsky's result. In the special case $\alpha = 2$ and $N = p$ with prime $p > 2$, an immediate consequence of Corollary 1 is

COROLLARY 2 ([10, pp. 217–218]). *Let* $p > 2$ *be prime. The integer* 2 *is a primitive* p*th root of unity modulo* m *if and only if* $m > 1$ *is a divisor of the Mersenne number*

$$M = \Phi_p(2) = 2^p - 1. \tag{7}$$

Furthermore, -2 *is a primitive* $(2p)$*th root of unity modulo* m *if and only if* $m > 1$ *is a divisor of* (7).

For $\alpha = 2$ and $N = 2^{d+1}$ ($d > 0$), we obtain by Corollary 1 and Theorem 2:

COROLLARY 3 ([5], [10, pp. 223–224]). *Let $N = 2^{d+1}$ ($d > 0$). The integer 2 is a primitive Nth root of unity modulo m if and only if $m > 1$ is a divisor of the Fermat number*

$$M = \Phi_N(2) = 2^{2^d} + 1. \tag{8}$$

In the case $d \geqslant 2$, the integer $\beta = 2^{N/8}(2^{N/4} - 1)$ with $\beta^2 \equiv 2 \bmod m$ is a primitive $(2N)$th root of unity modulo m, if $m > 1$ is an arbitrary divisor of (8).

The next results are new. The proofs of Corollaries 4–6 follow directly from Theorems 2 and 4.

COROLLARY 4. *Let $p > 2$ be prime, and let $N = 2^{d+1}p^t > 6$ ($d \geqslant 0, t \geqslant 1$). The integer 2 is a primitive Nth root of unity modulo m if and only if $m > 1$ is a divisor of the pseudo-Fermat number*

$$M = \begin{cases} \Phi_N(2)/p & \text{if 2 belongs to the exponent } 2^{d+1} \text{ modulo } p, \\ \Phi_N(2) & \text{otherwise}, \end{cases} \tag{9}$$

with

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

In the case $d \geqslant 2$, the integer $\beta = 2^{N/8}(2^{N/4} - 1)$ with $\beta^2 \equiv 2 \bmod m$ is a primitive $(2N)$th root of unity modulo m, if $m > 1$ is an arbitrary divisor of (9).

COROLLARY 5. *Let p and q be primes ($2 < q < p$), and let $N = q^s p^t$ ($s \geqslant 1, t \geqslant 1$). Further, let $\alpha \in \mathbb{Z}$ ($|\alpha| \geqslant 2$). The integer α is a primitive Nth root of unity modulo m if and only if $m > 1$ is a divisor of the integer*

$$M = \begin{cases} \Phi_N(\alpha)/p & \text{if } \alpha \text{ belongs to the exponent } q^s \text{ modulo } p, \\ \Phi_N(\alpha) & \text{otherwise}, \end{cases} \tag{10}$$

with

$$\Phi_N(x) = (x^N - 1)(x^{N/(qp)} - 1)(x^{N/q} - 1)^{-1}(x^{N/p} - 1)^{-1}.$$

The integer $-\alpha$ is a primitive $(2N)$th root of unity modulo m if and only if $m > 1$ is a divisor of (10).

COROLLARY 6. *Let p and q be primes with $2 < q < p$, and let $N = 2^{d+1}q^s p^t$ ($d \geqslant 0$, $s \geqslant 1$, $t \geqslant 1$). The integer 2 is a primitive Nth root of unity modulo m if and only if $m > 1$ is a divisor of the integer*

$$M = \begin{cases} \Phi_N(2)/p & \text{if 2 belongs to the exponent } 2^{d+1}q^s \text{ modulo } p, \\ \Phi_N(2) & \text{otherwise}, \end{cases} \tag{11}$$

with

$$\Phi_N(x) = (x^{N/2} + 1)(x^{N/(2qp)} + 1)(x^{N/(2q)} + 1)^{-1}(x^{N/(2p)} + 1)^{-1}.$$

In the case $d \geqslant 2$, the integer $\beta = 2^{N/8}(2^{N/4} - 1)$ with $\beta^2 \equiv 2 \bmod m$ is a primitive $(2N)$th root of unity modulo m, if $m > 1$ is an arbitrary divisor of (11).

Finally, we demonstrate the importance of our results. The following Table 1 gives a detailed overview of interesting cases for NTT's that can be obtained from Theorems 2 and 4 or from Corollaries 1–4. In Table 1, known parameters of practicable NTT's (see [9], [10, pp. 216–219, 222–224, and 231–236]) are summarized. We show that these parameters follow in a unified and simple way from the above results.

TABLE 1

Parameters α, N and m for NTT's, where $m > 1$ is an arbitrary divisor of $M = \Phi_N(\alpha)$, such that α is a primitive Nth root of unity modulo m.

α	N	$M = \Phi_N(\alpha)$	Corresponding NTT
2	p	$2^p - 1$ p prime	Mersenne number transform
-2	$2p$	$2^p - 1$ $p > 2$ prime	Mersenne number transform
2	2^{d+1}	$2^{2^d} + 1$ $d > 0$	Fermat number transform
$2^{2^{d-2}}(2^{2^{d-1}} - 1)$	2^{d+2}	$2^{2^d} + 1$ $d \geq 2$	Fermat number transform
2	p^2	$(2^{p^2} - 1)/(2^p - 1)$ p prime	Pseudo-Mersenne number transform
-2	$2p^2$	$(2^{p^2} - 1)/(2^p - 1)$ $p > 2$ prime	Pseudo-Mersenne number transform
2^q	p	$(2^{pq} - 1)/(2^q - 1)$ p prime, $q \geq 2$ $2^q \not\equiv 1 \bmod p$	Pseudo-Mersenne number transform
-2^q	$2p$	$(2^{pq} - 1)/(2^q - 1)$ $p > 2$ prime, $q \geq 2$ $2^q \not\equiv 1 \bmod p$	Pseudo-Mersenne number transform
2^q	2^{d+1}	$2^{q2^d} + 1$ $q \geq 2$, $d > 0$	Pseudo-Fermat number transform
$2^{q2^{d-2}}(2^{q2^{d-1}} - 1)$	2^{d+2}	$2^{q2^d} + 1$ $q \geq 2$, $d \geq 2$	Pseudo-Fermat number transform
2	$2p$	$(2^p + 1)/3$ $p > 3$ prime	Pseudo-Fermat number transform
2	$2p^2$	$(2^{p^2} + 1)/(2^p + 1)$ $p > 3$ prime	Pseudo-Fermat number transform
2^q	$2p$	$(2^{pq} + 1)/(2^q + 1)$ $p > 2$ prime, $q \geq 2$ $2^q \not\equiv -1 \bmod p$	Pseudo-Fermat number transform
2	$p2^{d+1}$	$(2^{p2^d} + 1)/(2^{2^d} + 1)$ $p > 2$ prime, $d \geq 0$ $2^{2^d} \not\equiv -1 \bmod p$	Pseudo-Fermat number transform
$2^{p2^{d-2}}(2^{p2^{d-1}} - 1)$	$p2^{d+2}$	$(2^{p2^d} + 1)/(2^{2^d} + 1)$ $p > 2$ prime, $d \geq 2$ $2^{2^d} \not\equiv -1 \bmod p$	Pseudo-Fermat number transform

Table 1 is obtained by systematic application of properties of the cyclotomic polynomials. Of course, every divisor $m > 1$ of M listed in Table 1 is a possible modulus for a NTT with the same length N and the same integer α, such that α is a primitive Nth root of unity modulo m. This means, for example, that for $\alpha = 2$ and $N = 2^{d+1}$ $(d > 0)$, the only possible moduli are the Fermat number $M = 2^{2^d} + 1$ and its divisors $m > 1$ [5]. These divisors are often too large for practical applications, so that one has to look for other moduli for transform lengths that are not powers of 2.

TABLE 2

Parameters for various NTT's with $\alpha = 2$ as primitive Nth root of unity modulo m, where N is of mixed-radix form and $m > 1$ is an arbitrary divisor of $M = \Phi_N(2)$.

Transform length N	Prime factorization of $\Phi_N(2)$
$180 = 2^2 \times 3^2 \times 5$	$\dfrac{2^{60} - 2^{30} + 1}{2^{12} - 2^6 + 1} = 181 \times 54\,001 \times 29\,247\,661$
$210 = 2 \times 3 \times 5 \times 7$	$\dfrac{3(2^{70} - 2^{35} + 1)}{(2^{10} - 2^5 + 1)(2^{14} - 2^7 + 1)} = 211 \times 664\,441 \times 1\,564\,921$
$240 = 2^4 \times 3 \times 5$	$\dfrac{2^{80} - 2^{40} + 1}{2^{16} - 2^8 + 1} = 394\,783\,681 \times 46\,908\,728\,641$
$252 = 2^2 \times 3^2 \times 7$	$\dfrac{2^{84} - 2^{42} + 1}{2^{12} - 2^6 + 1} = 40\,388\,473\,189 \times 118\,750\,098\,349$
$256 = 2^8$	$2^{128} + 1 = 59\,649\,589\,127\,497\,217 \times 5\,704\,689\,200\,685\,129\,054\,721$
$336 = 2^4 \times 3 \times 7$	$\dfrac{2^{112} - 2^{56} + 1}{2^{16} - 2^8 + 1} = 2\,017 \times 25\,629\,623\,713 \times 1\,538\,595\,959\,564\,161$
$360 = 2^3 \times 3^2 \times 5$	$\dfrac{2^{120} - 2^{60} + 1}{2^{24} - 2^{12} + 1} = 168\,692\,292\,721 \times 469\,775\,495\,062\,434\,961$
$420 = 2^2 \times 3 \times 5 \times 7$	$\dfrac{13(2^{140} - 2^{70} + 1)}{(2^{20} - 2^{10} + 1)(2^{28} - 2^{14} + 1)} = 421 \times 146\,919\,792\,181 \times 1\,041\,815\,865\,690\,181$
$504 = 2^3 \times 3^2 \times 7$	$\dfrac{2^{168} - 2^{84} + 1}{2^{24} - 2^{12} + 1} = 1009 \times 21169 \times 2627857 \times 269389009 \times 1475204679190128571777$

Example. According to Theorem 4, and by the prime factorization of $\Phi_{210}(2)$ (apply the prime decomposition of $2^{105} + 1$ given in [2, p. 13]),

$$\Phi_{210}(2) = 211 \times 664\,441 \times 1\,564\,921,$$

seven moduli m_i $(i = 1, \ldots, 7)$ arise, with the result that 2 is a primitive 210th root

of unity modulo m_i, where

$$\begin{aligned} m_1 &= 211, \\ m_2 &= 664\,441, \\ m_3 &= 1\,564\,921, \\ m_4 &= 211 \times 664\,441 \approx 1.41 \times 10^8, \\ m_5 &= 211 \times 1\,564\,921 \approx 3.30 \times 10^8, \\ m_6 &= 664\,441 \times 1\,564\,921 \approx 1.04 \times 10^{12}, \\ m_7 &= 211 \times 664\,441 \times 1\,564\,921 \approx 2.19 \times 10^{14}. \end{aligned}$$

Note that m_i $(i = 1, \ldots, 7)$ are all the primitive divisors of $2^{210} - 1$.

For practical applications, mixed-radix, Winograd, or prime-factor algorithms become attractive. These algorithms are based on highly factorizable transform lengths. Mixed-radix lengths have the form $N = 2^a 3^b 5^c 7^d$. In Table 2, we give explicitly all possible moduli for some NTT's with mixed-radix lengths $\geqslant 180$ and $\alpha = 2$. These results are new (compare with [12], [10, pp. 233, 235, and 236]). Table 2 lists the complete prime factorization of $\Phi_N(2)$. Note that $\Phi_N(2)$ can, of course, be a prime number, for example: $\Phi_{56}(2) = (2^{28} + 1)/17 = 15\ 790\ 321$. The preceding discussion apparently represents an interesting application of factorization of very large numbers.

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

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

1. R. C. AGARWAL & C. S. BURRUS, "Number theoretic transforms to implement fast digital convolution," *Proc. IEEE*, v. 63, 1975, pp. 550–560.

2. 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.

3. R. CREUTZBURG & M. TASCHE, "Zahlentheoretische Transformationen und primitive Einheitswurzeln in einem Restklassenring modulo m," *Rostock. Math. Kolloq.*, v. 25, 1984, pp. 4–22.

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

5. P. DUHAMEL & H. HOLLMANN, "Number-theoretic transforms with 2 as a root of unity," *Electron. Lett.*, v. 18, 1982, pp. 978–980.

6. S. W. GOLOMB, I. S. REED & T. K. TRUONG, "Integer convolutions over the finite field GF($3 \cdot 2^n + 1$)," *SIAM J. Appl. Math.*, v. 32, 1977, pp. 356–365.

7. R. LIDL & H. NIEDERREITER, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

8. P. J. NICHOLSON, "Algebraic theory of finite Fourier transforms," *J. Comput. System Sci.*, v. 5, 1971, pp. 524–547.

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, Berlin, 1981.

11. J. M. POLLARD, "The fast Fourier transform in a finite field," *Math. Comp.*, v. 25, 1971, pp. 365–374.

12. B. RICE, "Some good fields and rings for computing number-theoretic transforms," *IEEE Trans. Acoust. Speech Signal Process.*, v. 27, 1979, pp. 432–433.

13. B. RICHTER, "Die Primzahlzerlegung der Werte der Kreisteilungspolynome," *J. Reine Angew. Math.*, v. 254, 1972, pp. 123–132.