COMPOSITION OF $\Phi_3(X)$ MODULO m

SISTER CHRISTELLE THEUSCH
Dominican College, Racine, Wisconsin

1. INTRODUCTION

In an earlier issue of this quarterly, Cohn* investigated the value of the residues modulo n of X^m when $0 \le X \le (n-1)$. The object of this paper is to study the value set modulo m of another function — the cyclotomic polynomial $\Phi_3(X) = X^2 + X + 1$, and further to consider some properties of the composition of this function with itself n times. We will denote this n-fold composition by

$$n{:}\Phi_3(X) = \Phi_3(\Phi_3(\cdots(\Phi_3(X))\cdots)) .$$

We define

$$\Psi(m,n) = \{n{:}\Phi_3(X) \pmod m \mid 0 \le X < m\} ,$$

and such that if α is in (m,n), then $0 \le \alpha < m$. Further, we let $r(m)$ be the minimum n for which $\Psi(m,n) = \Psi(m,n+1)$ and refer to $\Psi(m,r(m))$ simply as $\Psi(m)$. The cardinality of $\Psi(m,n)$ will be denoted by $N(\Psi(m,n))$.

2. PROPERTIES

Definition. We say that $f(X)$ is modulo m-symmetric if $f(X) \equiv f(-X-1) \pmod m$ and that $f(X)$ is modulo m-doubly symmetric if $f(X) \equiv f(m/2 - X - 1) \equiv f(m/2 + X) \equiv f(-X-1) \pmod m$ for $0 \le X < m$.

Property 1. $n{:}\Phi_3(X)$ is modulo m-symmetric.

Proof. We have

$$\Phi_3(X) = X^2 + X + 1 = X^2 + 2X + 1 - X - 1 + 1 = \Phi_3(-X-1)$$

and hence also

*John H. E. Cohn, "On m-tic Residues Modulo n," Fibonacci Quarterly, 5 (1967), pp. 305-318.

$$n:\Phi_3(X) = n:\Phi_3(-X - 1) .$$

We note that X and $-X - 1$ cannot simultaneously be elements of $\Psi(m)$ since $r:\Phi_3(X)$ is modulo m-symmetric.

Property 2. $n:\Phi_3(X)$ is modulo 2p-doubly symmetric.

Proof. Elementary calculations yield

$$\Phi_3(p - X - 1) \equiv \Phi_3(p + X) \equiv p^2 + p + X^2 + X + 1 \pmod{2p} .$$

Now

$$p^2 + p = 2p[(p + 1)/2] \equiv 0 \pmod{2p}$$

and hence

$$\Phi_3(X) \equiv \Phi_3(p + X) \pmod{2p} .$$

These congruences together with Property 1 yield the result.

Property 3. $N(\Psi(p,1))$ is $(p + 1)/2$.

Proof. Since $\Phi_3(X)$ is modulo p-symmetric $N(\Psi(p,1))$ is at most $(p + 1)/2$. Suppose

$$\Phi_3(X) \equiv \Phi_3(X + a) \pmod{p} ,$$

with $a \not\equiv 0 \pmod{p}$. Then, simple calculations yield

$$a(2X + a + 1) \equiv 0 \pmod{p} .$$

Since $a \not\equiv 0 \pmod{p}$, we must have $X + a \equiv -X - 1 \pmod{p}$.

Property 4. $N(\Psi(m)) \neq 1$ for $m > 2$.

Proof. Clearly a necessary condition that $N(\Psi(m)) = 1$ is that $\Phi_3(X) \equiv X \pmod{m}$ for exactly one X where $0 \leq X < m$. In order for the above congruence to hold, we need $X^2 \equiv -1 \pmod{m}$. However, for $m > 2$, this congruence has either two distinct solutions or no solutions.

Property 5. $N(\Psi(2^n)) = 2^{n-1}$; $r(2^n) = 1$.

Proof. First, we note that for any α in $\Psi(2^n, 1)$ we have $\alpha \equiv 1$ (mod 2). Thus since X and $-X - 1$ are of opposite parity modulo 2^n and $\Phi_3(X)$ is modulo 2^n-symmetric $\Psi(2^n, 1)$ is completely determined by $\Phi_3(2k$ $k = 1, \cdots, 2^{n-1}$. Suppose that

$$\Phi_3(2k_1 - 1) \equiv \Phi_3(2k_2 - 1) \pmod{2^n}$$

with $1 \leq k_1,\ k_2 \leq 2^{n-1}$. It can readily be verified that this supposition yields

$$4(k_1^2 - k_2^2) - 2(k_1 - k_2) \equiv 0 \pmod{2^n}$$

and hence

$$(k_1 - k_2)(2k_1 + 2k_2 - 1) \equiv 0 \pmod{2^{n-1}} ,$$

from which it follows immediately that $k_1 = k_2$. Hence, $N(\Psi(2^n, 1)) = 2^{n-1}$ and since $\alpha \equiv 1 \pmod 2$ we must have $r(2^n) = 1$.

Property 6. If $p \equiv 11, 13, 17, 19$ modulo 20 then $r(p) > 1$.

Proof. Let

$$\Phi_3((p - 1)/2) \equiv \beta \pmod p .$$

First we note that if

$$\Phi_3(X) \not\equiv (p - 1)/2 \pmod p$$

for all X, then properties 1 and 3 imply that β is an element of $\Psi(p, 1)$ while it is not in $\Psi(p)$ and hence $r(p) > 1$. Now from

$$X^2 + X + 1 \equiv (p - 1)/2 \pmod p ,$$

it follows that

$$2X^2 + 2X + 3 \equiv 0 \pmod p .$$

The quadratic formula indicates that -5 must be a quadratic residue modulo p if this congruence has a solution. However -5 is a quadratic non-residue for the p in the hypothesis.

Property 7. $N(\Psi(m))$ is multiplicative.

Proof. Let

$$m = p_1^{e_1} \cdots p_t^{e_t} .$$

For each γ in $\Psi(m)$ there exists an X such that

$$r:\Phi_3(X) - \gamma \equiv 0 \pmod{m} .$$

Thus

$$r:\Phi_3(X) - \gamma \equiv 0 \pmod{p_i^{e_i}}, \qquad 1 \le i \le t ,$$

and hence

$$\gamma \equiv \alpha_i \pmod{p_i^{e_i}}$$

for some α_i in $\Psi(p_i^{e_i})$. The Chinese Remainder Theorem assures a unique γ, $0 \le \gamma < m$, as a solution to this system of congruences, and hence

$$N(\Psi(m)) \le \prod_1^t [N(\Psi(p_i^{e_i}))] .$$

To see that equality actually holds, we suppose

$$\gamma \equiv \alpha_i \pmod{p_i^{e_i}}, \qquad 1 \le i \le t .$$

Since

$$r:\Phi_3(X) - \gamma \equiv \Phi_3(X) - \alpha_i \equiv 0 \pmod{p_i^{e_i}}$$

has a solution for each i we are guaranteed a solution to the congruence

$$r:\Phi_3(X) - \gamma \equiv 0 \pmod{m} .$$

Thus γ is in $\Psi(m)$.

Property 8. $r(m) = \max r(p_i^{e_i}),\ 1 \le i \le t$.

Proof. We denote

$$\max r(p_i^{e_i})$$

by r' and consider

$$r':\Phi_3(X) \equiv \gamma \pmod{m} .$$

Since for

$$r':\Phi_3(X) \equiv \gamma \equiv \alpha_i \pmod{p_i^{e_i}} ,$$

we have α_i in

$$\Psi(p_i^{e_i}, r') = \Psi(p_i^{e_i}) ,$$

γ must be in $\Psi(m)$. On the other hand, for $n < r'$, there exists at least one p such that for $n:\Phi_3(X) \equiv \gamma \pmod{m}$,

$$n:\Phi_3(X) \equiv \gamma \equiv \alpha_i \pmod{p_i^{e_i}}$$

with α_i not in $\Psi(p_i^{e_i})$ and hence γ cannot be in $\Psi(m)$.

3. EXTENSION

We note that Properties 7 and 8 can easily be extended to the composition of other cyclotomic polynomials $n:\Phi_p(X)$ modulo m. However, the other properties given are not generally valid for $n:\Phi_p(X)$. In particular, for $\Phi_5(X)$ we have $r(2^n) = n$ and $N(\Psi(2^n)) = 1$ with

$$\Psi(2^n) = 2 + 2^2 + \cdots + 2^n - 1 \quad \text{for} \quad n = 1, \cdots, 6 .$$