Math. J. Okayama Univ. 38(1996), 115–122

ON VALUES OF CYCLOTOMIC POLYNOMIALS. III

KAORU MOTOSE

In this paper, we shall consider relations between Lucas' test (or Pépin's test) and values of cyclotomic polynomials $\Phi_n(x)$.

For Pépin's test, the next well known result shows this relations (see [1, p.378] and [2, Corollary 4(3)]).

Assume n is an odd integer. Then n is prime if and only if there exists an integer $c > 1$ such that $\Phi_{n-1}(c) \equiv 0 \bmod n$.

In this note, for an algebraic integer γ, $\mathcal{O}_\gamma$ will represents the ring of all algebraic integers in $\mathbf{Q}(\gamma)$.

The next is essential for our purpose.

Theorem 1. *Let P be a proper ideal in a ring R with the identity $1 \neq 0$. If P contains p and $\Phi_n(\gamma)$ for a prime integer p and $\gamma \in R$, then $n = p^e|\gamma|_P$ where $|\gamma|_P$ is the order of γ mod P.*

Proof. It follows from the condition that $\gamma^n \equiv 1 \bmod P$ and so $|\gamma|_P$ is a divisor of n. Thus we can set $n = tp^e|\gamma|_P$ with $(t,p) = 1$. Assume $t > 1$. Then noting $\gamma^{\frac{n}{t}} \equiv 1$ and $\Phi_n(x)$ divides $\frac{x^n-1}{x^{\frac{n}{t}}-1} = (x^{\frac{n}{t}})^{t-1} + \cdots + x^{\frac{n}{t}} + 1$, we have

$$t \equiv (\gamma^{\frac{n}{t}})^{t-1} + \cdots + \gamma^{\frac{n}{t}} + 1 \equiv 0 \mod P.$$

Thus we have a contradiction P contains the identity 1 by $(t,p) = 1$.

Theorem 2. *If there exists an algebraic integer γ of the degree ≤ 2 satisfying $\Phi_{n+1}(\gamma) \equiv 0$ or $\Phi_{n-1}(\gamma) \equiv 0 \bmod n\mathcal{O}_\gamma$, then n is prime.*

Proof. Assume $\Phi_{n+1}(\gamma) \equiv 0$ and let P be a prime ideal of $\mathcal{O}_\gamma$ containing n. Then $n \in P \cap \mathbf{Z} = p\mathbf{Z}$ and p be a divisor of n. Since $n+1 \notin P$ and $\Phi_{n+1}(\gamma) \equiv 0 \bmod P$, we have $n+1 = |\gamma|_P$ by Theorem 1 and hence $n+1$ is a divisor of $p^2 - 1$. Thus we obtain the next for some $k > 0$

$$p^2 - 1 = k(n+1) \geq k(p+1) \text{ and } k \equiv -1 \bmod p.$$

Hence $p \geq k + 1 = ps$ for some $s > 0$ and $p = k + 1$. This shows $n = p$. Similarly, we can prove from $\Phi_{n-1}(\gamma) \equiv 0$ that n is prime.

It is not so easy to find γ in Theorem 2. The next lemmas shall help us to find γ.

Lemma 1. *Assume $p > 3$ is prime. Then we have the following*

(1) *there exists an integer $c > 1$ such that $\Phi_{p-1}(c) \equiv 0 \bmod p$ and $\left(\frac{c}{p}\right) = -1$.*

(2) *there exists an integer $c > 1$ such that $(c^3 - c,\ p) = 1$, $\left(\frac{c^2-1}{p}\right) = -1$, $\gamma = c + \sqrt{c^2-1}$, $\Phi_{p+1}(\gamma) \equiv 0$ and $\gamma^{\frac{p+1}{2}} \equiv -1 \bmod p\mathcal{O}_\gamma$.*

Proof. (1): Assume that p is prime and c is a primitive root of p. Then $\prod_{d|p-1} \Phi_d(c) = c^{p-1} - 1 \equiv 0 \bmod p$ and so $\Phi_d(c) \equiv 0$ for some d. Thus $c^d \equiv 1$ and $p-1$ is a divisor of d. Hence $d = p-1$ and $\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \equiv -1$.

(2): Step 1. Existence of $c > 1$ and $(c^3 - c, p) = 1$.

There exists a square free integer $m > 1$ such that $\left(\frac{m}{p}\right) = -1$. It follows from $\left(\frac{m}{p}\right) = -1$ that $P_m = p\mathcal{O}_{\sqrt{m}}$ is prime and $|\mathcal{O}_{\sqrt{m}}/P_m| = p^2$. Let ω be a generator of the multiplicative group of $\mathcal{O}_{\sqrt{m}}/P_m$ and let $\eta \in \mathcal{O}_{\sqrt{m}}$ such that $\eta \bmod P_m = \omega^{p-1}$. Then $p+1 = |\eta|_{P_m}$. Hence $\prod_{d|p+1} \Phi_d(\eta) = \eta^{p+1} - 1 \equiv 0$ and so $\Phi_d(\eta) \equiv 0 \bmod P_m$ for some d. Thus $\eta^d \equiv 1$ and $p+1$ is a divisor of d. Hence $d = p+1$ and $\Phi_{p+1}(\eta) \equiv 0$. As for $\eta \in \mathcal{O}_{\sqrt{m}}$, $\eta^2 - u\eta + v = 0$ for some $u, v \in \mathbf{Z}$. We can set $u \equiv 2c$ $(c \geq 0)$. Using Frobenius automorphism, we can see $\eta^p (\not\equiv \eta)$ is a root of $x^2 - ux + v \equiv 0$ and so $v \equiv 1 \bmod P_m$. If $c^3 \equiv c \bmod p$, then we have a contradiction $p = 3$ using the above equations. In particular, $c > 1$.

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

In case $m \equiv 2, 3 \bmod 4$, setting $\eta = a + b\sqrt{m}$, we have $2a \equiv 2c$ and $a^2 - b^2 m \equiv 1$, and so $c^2 - 1 \equiv b^2 m \bmod p$. In case $m \equiv 1 \bmod 4$, setting $\eta = a + b\frac{1+\sqrt{m}}{2}$, we have $2a + b \equiv 2c$ and $a^2 + ab + \frac{1-m}{4}b^2 \equiv 1$, and so $4(c^2-1) \equiv b^2 m \bmod p$. In any case, $\left(\frac{c^2-1}{p}\right) = \left(\frac{m}{p}\right) = -1$.

Step 3. $\Phi_{p+1}(\gamma) \equiv 0$ and $\gamma^{\frac{p+1}{2}} \equiv -1 \bmod p\mathcal{O}_\gamma$ where $\gamma = c + \sqrt{c^2-1}$.

First, we note $\Phi_{p+1}(\eta^{-1}) \equiv \Phi_{p+1}(\eta^p) \equiv 0 \bmod P_m$ and $P_\gamma = p\mathcal{O}_\gamma$ is prime by $\left(\frac{c^2-1}{p}\right) = -1$. Let $\mathcal{P} \ni p$ be a prime ideal of the ring of algebraic integers in $\mathbf{Q}(\sqrt{m}, \sqrt{c^2-1})$. Then $\eta \equiv \gamma$ or $\eta \equiv 2c - \gamma = \gamma^{-1}$, and so $\Phi_{p+1}(\gamma) \equiv 0$ and $\gamma^{\frac{p+1}{2}} \equiv -1 \bmod \mathcal{P}$. It follows from $\mathcal{O}_\gamma \cap \mathcal{P} = P_\gamma$ that $\Phi_{p+1}(\gamma) \equiv 0$ and $\gamma^{\frac{p+1}{2}} \equiv -1 \bmod P_\gamma$.

Lemma 2. *Let p be an odd prime and let $c > 1$ be an integer with $(c^3 - c,\ p) = 1$. We set $\gamma = c + \sqrt{d}$ where $d = c^2 - 1$. Then we have the following*

(1) $\gamma^{p-\left(\frac{d}{p}\right)} \equiv 1 \bmod p\mathcal{O}_\gamma$.
(2) $\left(\frac{2c-2}{p}\right) \equiv \gamma^{\frac{p-1}{2}}$ *if* $\gamma^{p-1} \equiv 1 \bmod p\mathcal{O}_\gamma$.
(3) $\left(\frac{2c+2}{p}\right) \equiv \gamma^{\frac{p+1}{2}}$ *if* $\gamma^{p+1} \equiv 1 \bmod p\mathcal{O}_\gamma$.

Proof. (1): We have the assertion from the next equation.

$$\gamma^p \equiv c^p + (\sqrt{d})^p \equiv c + d^{\frac{p-1}{2}}\sqrt{d} \equiv c + \left(\frac{d}{p}\right)\sqrt{d} = \gamma^{\left(\frac{d}{p}\right)} \bmod p\mathcal{O}_\gamma.$$

(2): First we note that $\gamma^2 - 1 \bmod p\mathcal{O}_\gamma$ is invertible since $4(c^2-1) = (\gamma-\gamma^{-1})^2$ is relatively prime to p. The next equation shows our assertion.

$$\begin{aligned}\left(\frac{2c-2}{p}\right) &\equiv (2c-2)^{\frac{p-1}{2}} = ((\gamma-1)(1-\gamma^{-1}))^{\frac{p-1}{2}} \\ &= \gamma^{-\frac{p-1}{2}}(\gamma-1)^{p-1} \equiv \gamma^{\frac{p-1}{2}}(\gamma^p-1)(\gamma-1)^{-1} \\ &\equiv \gamma^{\frac{p-1}{2}}(\gamma-1)(\gamma-1)^{-1} = \gamma^{\frac{p-1}{2}} \bmod p\mathcal{O}_\gamma.\end{aligned}$$

(3): This proof is similar to (2). In fact, $\gamma^2 - 1 \bmod p\mathcal{O}_\gamma$ is invertible as stated in (2) and the next equation shows our assertion.

$$\begin{aligned}\left(\frac{2c+2}{p}\right) &\equiv (2c+2)^{\frac{p-1}{2}} = ((\gamma+1)(1+\gamma^{-1}))^{\frac{p-1}{2}} \\ &= \gamma^{-\frac{p-1}{2}}(\gamma+1)^{p-1} \equiv \gamma^{-\frac{p-1}{2}}(\gamma^p+1)(\gamma+1)^{-1} \\ &\equiv \gamma^{-\frac{p-1}{2}}(\gamma^{-1}+1)(\gamma+1)^{-1} = \gamma^{-\frac{p-1}{2}}\gamma^{-1} \\ &\equiv \gamma^{\frac{p+1}{2}} \bmod p\mathcal{O}_\gamma.\end{aligned}$$

Remark 1. The next equation shows all assertions in Lemma 2.

$$\left(\frac{2c-2\left(\frac{d}{p}\right)}{p}\right) \equiv \gamma^{\frac{p-\left(\frac{d}{p}\right)}{2}} \bmod p\mathcal{O}_\gamma.$$

The next follows from Theorem 2 and Lemmas 1, 2.

Theorem 3. Let $p > 3$ be an integer. Then we have the following.

(1) p is prime if and only if there exists an integer $c > 1$ such that $\left(\frac{c}{p}\right) = -1$ and $\Phi_{p-1}(c) \equiv 0 \bmod p$.

(2) p is prime if and only if there exists an integer $c > 1$ such that $(c^3-c, p) = 1, \gamma = c + \sqrt{c^2-1}, \left(\frac{2c+2}{p}\right) = \left(\frac{c^2-1}{p}\right) = -1$ and $\Phi_{p+1}(\gamma) \equiv 0 \bmod p\mathcal{O}_\gamma$.

Remark 2. Let $n = M_q = 2^q - 1$ be a Mersenne number where q is an odd prime and let $\gamma = 2 + \sqrt{3}$ in the above, we set $S_k = \gamma^{2^k} + \gamma^{-2^k}$.

Then $\left(\frac{3}{M_q}\right) = -1, S_0 = 4$ and $S_{k+1} = S_k^2 - 2$. We have from Theorem 3(2) and Lemma 2 that

$$M_q \text{ is prime if and only if } S_{q-2} \equiv 0 \bmod M_q.$$

Remark 3. Let $n = F_m = 2^{2^m} + 1$ $(m \geq 1)$ be a Fermat number. $\left(\frac{3}{F_m}\right) = -1$ follows from $n \equiv 2 \bmod 3$. Thus Theorem 3(1) shows that

$$F_m \text{ is prime if and only if } 3^{\frac{F_m - 1}{2}} \equiv -1 \bmod F_m.$$

We set $3s \equiv 1 \bmod n$ and $S_i = 3^{2^i} + s^{2^i}$. Then we have $S_0 = 3 + s$ and $S_{i+1} \equiv S_i^2 - 2 \bmod n$. Thus

$$F_m \text{ is prime if and only if } S_{2^m-2} \equiv 0 \bmod F_m.$$

Theorem 4. (1) *Let* $n = 2^\ell h + 1$, *where* $2^\ell > h \geq 1$ *is odd, and let* $c > 1$ *be an integer with* $(c,\ n) = 1$. *We set* $cc_0 \equiv 1 \bmod n$ *and*

$$S_0 = c^h + c_0^h,\ S_{j+1} = S_j^2 - 2.$$

If $S_{\ell-2} \equiv 0 \bmod n$, *then* n *is prime.*

(2) *Let* $n = 2^\ell h - 1$, *where* $2^\ell > h \geq 1$ *is odd, and let* $c > 1$ *be an integer. We set* $\gamma = c + \sqrt{c^2 - 1}$ *and*

$$S_0 = \gamma^h + \gamma^{-h},\ S_{j+1} = S_j^2 - 2.$$

If $S_{\ell-2} \equiv 0 \bmod n$, *then* n *is prime.*

Proof. (1): Assume that $S_{\ell-2} \equiv 0 \bmod n$. Then we have the next for a prime divisor p of n and $b = c^h$,

$$\Phi_{2^\ell}(b) = \Phi_2(b^{2^{\ell-1}}) = b^{2^{\ell-1}} + 1 \equiv 0 \bmod p$$

Thus by Theorem 1, we have $2^\ell = |b|_p$. Since $b^{p-1} \equiv 1 \bmod p$, 2^ℓ is a divisor of $p-1$ and $p \geq 2^\ell + 1$. The inequality $p^2 \geq (2^\ell + 1)^2 > 2^\ell h + 1 = n$ implies n is prime.

(2): Assume that $S_{\ell-2} \equiv 0 \bmod n$. Then we have the next for a prime divisor p of n and $\eta = \gamma^h$,

$$\Phi_{2^\ell}(\eta) = \Phi_2(\eta^{2^{\ell-1}}) = \eta^{2^{\ell-1}} + 1 \equiv 0 \bmod p\mathcal{O}_\gamma.$$

Thus by Theorem 1, we have $2^\ell = |\eta|_{p\mathcal{O}_\gamma}$. Since η^{p-1} or $\eta^{p+1} \equiv 1 \bmod p\mathcal{O}_\gamma$ by Lemma 2 (1), 2^ℓ is a divisor of $p \pm 1$. If $p = 2^\ell - 1$, then $0 \equiv n =$

$h(p+1)-1 \equiv h-1 \bmod p$ and so $h=1$ by $h-1<2^{\ell}-1=p$. Thus $n=2^{\ell}-1=p$. Hence, we may assume $p>2^{\ell}$ and so the inequality $p^2>2^{\ell}h>n$ implies n is prime.

Remark 4. If we want to find primes using Theorem 4, then conditions on c as in Theorem 3 are useful for calculations though the condition $S_{\ell-2} \equiv 0$ contains these.

Example 1. If we set $c=23$, then we can see from Theorem 4 (1) that numbers $n=15\cdot 2^{\ell}+1$ $(4 \leq \ell \leq 1000)$ are prime for ℓ (digits) =

4(3), 9(4), 10(5), 27(10), 37(13), 38(13), 48(16), 112(35), 229(71), 339(104), 522(159), 654(199), 900(273).

Example 2. If we set $c=25$, then we can see from Theorem 4 (2) that numbers $n=15\cdot 2^{\ell}-1$ $(4 \leq \ell \leq 1000)$ are prime for ℓ (digits) =

4(3), 5(3), 10(5), 14(6), 17(7), 31(11), 41(14), 82(26), 125(39), 172(53), 202(62), 266(82), 293(90), 463(141).

Theorem 5. (1) *Assume* $n=2^{\ell}3^k+1$ $(k,\ell \geq 1)$ *and* $c>1$ *is an integer with* $(c,\ n)=1$ *and* $\left(\frac{c}{n}\right)=-1$. *We set* $cc_0 \equiv 1 \bmod n$. *We consider two sequences*

$$R_0=c+c_0,\ R_{i+1}=R_i^3-3R_i \text{ and } S_0=R_{k-1},\ S_{j+1}=S_j^2-2.$$

Under this setting, we obtain that

$$S_{\ell-1} \equiv 1 \bmod n \text{ if and only if } n \text{ is prime and } S_{\ell-1} \not\equiv -2 \bmod n.$$

(2) *Assume* $n=2^{\ell}3^k-1$ $(k,\ell \geq 1)$ *and* $c>1$ *is an integer with* $(c^3-c,\ n)=1$ *and* $\left(\frac{c^2-1}{n}\right)=\left(\frac{2c+2}{n}\right)=-1$. *We set* $\gamma=c+\sqrt{c^2-1}$. *We consider two sequences*

$$R_0=2c,\ R_{i+1}=R_i^3-3R_i \text{ and } S_0=R_{k-1},\ S_{j+1}=S_j^2-2.$$

Under this setting, we obtain that

$$S_{\ell-1} \equiv 1 \bmod n \text{ if and only if } n \text{ is prime and } S_{\ell-1} \not\equiv -2 \bmod n.$$

Proof. (1): we set $b=c^{3^{k-1}}$ and assume that $S_{\ell-1} \equiv 1 \bmod n$. Then $S_{\ell-1} \not\equiv -2$ and we have

$$\Phi_{n-1}(c)=\Phi_{3^k\cdot 2^{\ell}}(c)=\Phi_6(b^{2^{\ell-1}})=(b^{2^{\ell-1}})^2-b^{2^{\ell-1}}+1 \equiv 0 \bmod n.$$

Thus by Theorem 2, we have n is prime.

We shall prove the converse. We obtain $c^{\frac{n-1}{2}} \equiv \left(\frac{c}{n}\right) = -1$. Thus $(b^{2^{\ell-1}})^3 + 1 \equiv c^{\frac{n-1}{2}} + 1 \equiv 0$. It follows from $S_{\ell-1} \not\equiv -2$ that $b^{2^{\ell-1}} + 1 \not\equiv 0$ and so $b^{2^\ell} - b^{2^{\ell-1}} + 1 \equiv 0$ which means $S_{\ell-1} \equiv 1 \bmod n$.

(2): We set $\eta = \gamma^{3^{k-1}}$ and assume that $S_{\ell-1} \equiv 1 \bmod n$. Then $S_{\ell-1} \not\equiv -2$ and we have

$$\Phi_{n+1}(\gamma) = \Phi_{3^k.2^\ell}(\gamma) = \Phi_6(\eta^{2^{\ell-1}}) = (\eta^{2^{\ell-1}})^2 - \eta^{2^{\ell-1}} + 1 \equiv 0 \bmod n.$$

Thus by Theorem 2, we have n is prime.

We shall prove the converse. We obtain $\gamma^{\frac{n+1}{2}} \equiv -1$ from the conditions and Lemma 2. Thus $(\eta^{2^{\ell-1}})^3 + 1 \equiv \gamma^{\frac{n+1}{2}} + 1 \equiv 0$. It follows from $S_{\ell-1} \not\equiv -2$ that $\eta^{2^{\ell-1}} + 1 \not\equiv 0$ and so $\eta^{2^\ell} - \eta^{2^{\ell-1}} + 1 \equiv 0$ which means $S_{\ell-1} \equiv 1 \bmod n$

Example 3. If we set $c = 13$, then we can see from Theorem 5 (1) that numbers $n = 2^6 3^\ell + 1$ $(4 \le \ell \le 1000)$ are prime for ℓ (digits) =

7(6), 11(8), 13(9), 31(17), 41(22), 61(31), 121(60), 127(63), 157(77), 167(82), 181(89), 203(99), 229(112), 415(200), 427(206), 463(223), 503(242), 559(269).

Example 4. If we set $c = 72$, then we can see from Theorem 5 (2) that numbers $n = 2^{12} 3^\ell - 1$ $(8 \le \ell \le 1000)$ are prime for ℓ (digits) =

19(13), 23(15), 25(16), 67(36), 773(373).

We would like to state that computations in Examples 1 ~ 4 were executed in virtue of a personal computer NEC PC9821 Xa and a program that was written in Ubasic developed by Y. Kida.

In the remainder of this paper, we should give the complete proof of [3, Theorems 7.2, and 7.3] because these proof was not complete about conditions for Legendre symbols by reason of my negligence.

Let u, v be nonzero integers, let α, β be distinct roots of the quadratic equation $x^2 - ux + v = 0$ and $d = u^2 - 4v$. Then $u = \alpha + \beta, v = \alpha\beta$, and $d = (\alpha - \beta)^2$. We set $V_n = \alpha^n + \beta^n$.

Theorem 6. *We set $M_q = 2^q - 1$ and $F_m = 2^{2^m} + 1$ where q is an odd prime and $m \ge 1$.*

(1) *If $(vd, M_q) = 1$ and $V_{\frac{M_q+1}{2}} \equiv 0 \bmod M_q$, then M_q is prime, $\left(\frac{d}{M_q}\right) = -1$ and $\left(\frac{v}{M_q}\right) = -1$.*

(2) *If* $(vd, F_m) = 1$ *and* $V_{\frac{F_m-1}{2}} \equiv 0 \bmod F_m$, *then* F_m *is prime*, $\left(\frac{d}{F_m}\right) = 1$ *and* $\left(\frac{v}{F_m}\right) = -1$.

Proof. (1): We set $n = M_q$ and P is a prime ideal of $\mathcal{O}_\alpha$ containing n. It follows from $(vd, n) = 1$ that $\alpha, \beta, \alpha - \beta \bmod n\mathcal{O}_\alpha$ are invertible. We set $\gamma \equiv \alpha\beta^{-1} \bmod n\mathcal{O}_\alpha$. Then we have

$$\Phi_{n+1}(\gamma) \equiv \beta^{-\frac{n+1}{2}} V_{\frac{n+1}{2}} \equiv 0 \bmod n\mathcal{O}_\alpha$$

Thus we have $p = n$ is prime from Theorem 2.

We note $|\gamma|_P = p + 1$ by Theorem 1 and $\gamma^{p+1} \equiv 1 \bmod P$. Using Frobenius automorphism of the finite field $\mathcal{O}_\alpha/P$, we can see both $\{\alpha, \beta\}$ and $\{\alpha^p, \beta^p\}$ are sets of roots of $x^2 - ux + v \equiv 0 \bmod P$. Assume that $\alpha \equiv \alpha^p \bmod P$. Then we have $\beta \equiv \beta^p \bmod P$ and so

$$\gamma^2 \equiv \alpha\beta^{-1}\gamma \equiv \alpha^p\beta^{-p}\gamma \equiv \gamma^{p+1} \equiv 1 \bmod P.$$

This contradicts to $|\gamma|_P = p + 1 > 2$. Hence we have $\alpha^p \equiv \beta$ and $\beta^p \equiv \alpha \bmod P$. Thus we obtain the next

$$\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \equiv (\alpha - \beta)^{p-1} \equiv (\alpha^p - \beta^p)(\alpha - \beta)^{-1} \equiv -1 \bmod P.$$

It follows from $\beta^{p+1} \equiv v$ and $\alpha^{\frac{p+1}{2}} \equiv -\beta^{\frac{p+1}{2}} \bmod P$ that

$$\left(\frac{v}{p}\right) \equiv v^{\frac{p-1}{2}} \equiv v^{\frac{p+1}{2}} v^{-1} \equiv -\beta^{p+1} v^{-1} = -1 \bmod P.$$

(2) follows from the same method as in the proof of (1).

References

[1] L. E. Dickson: History of the theory of numbers, vol.1, Chelsea, 1971.

[2] K. Motose: Values of cyclotomic polynomials, Math. J. Okayama Univ. **35** (1993), 35–40.

[3] K. Motose: Values of cyclotomic polynomials. II, Math. J. Okayama Univ. **37** (1995), 27–36.

Department of Mathematical System Science
Faculty of Science and Technology
Hirosaki University
Hirosaki 036 Japan
E-mail: skm@cc.hirosaki-u.ac.jp

(*Recived March 24, 1997*)