Math. J. Okayama Univ. **37**(1995), 27–36

ON VALUES OF CYCLOTOMIC POLYNOMIALS. II

Kaoru MOTOSE

prime. Then p is the order $|2|_q$ of 2 mod q. Thus p is a divisor of $q-1$

The next shows that Fermat numbers and Mersenne numbers are almost square free.

or $2^q - 1$, *then* $2^{p-1} \equiv 1 \bmod p^2$. *If* p^2 *divides* $(10^q - 1)/9$, *then* $10^{p-1} \equiv$ $1 \bmod p^2$.

Proof. Theorem implies our assertion from

$$2^{2^n} + 1 = \Phi_{2^{n+1}}(2),\ \ 2^q - 1 = \Phi_q(2) \ \text{and}\ \ \frac{10^q - 1}{9} = \Phi_q(10).$$

The next needs later. It is easy to see $np = |a+p|_{p^2}$ from the conditions of this proposition.

Proposition 1.2. *If* p^2 *divides* $\Phi_n(a)$ *for* $n > 3$, *then* p *is the* p*-part* primitive root for every prime.

Proof. Necessity follows easily from Theorem A. So, we assume the

p-part of m. It follows from $n = |a|_q$ that q divides $a^n - 1 = \prod_{d|n} \Phi_d(a)$.
Hence q divides only $\Phi_n(a)$ by virtue of $n = |a|_q$. This shows also that

Proof. Theorem implies that every prime part of $\Phi_n(a)$ is a divisor is a divisor of $\Phi_n(a)$. Conversely, if q is a divisor of $\Phi_n(a)$ and r is a prime

divisor of q, then $p = |a|_r$ and $kp+1 = r$ is a divisor of $q = 2p+1$ for some

$k > 1$. Thus we have $q = r$ is prime and $\left(\frac{a}{q}\right) \equiv a^{(q-1)/2} = a^p = 1 \bmod q$.

numbers. If $p > 3$ is Sophie Germain prime and $p \equiv -1 \bmod 4$, then

Proof. Let p be a prime divisor of N. By the assumptions, we have $0 \equiv \Phi_q(s) \equiv \Phi_q(u^{q^{e-1}}) = \Phi_{q^e}(u) \bmod N$ where q^e is the q-part of F and

$$u \equiv a^{\frac{N-1}{q^e}} \bmod N.$$

the other hand, p is a divisor of $(t^R - 1)/(t-1) = \prod_{d|R, d>1} \Phi_d(t)$ and so

$d = |t|_p$ is a divisor of $p-1$ for a divisor $d > 1$ of R. Hence dF is a divisor

of $p-1$. Thus $p > dF \geq BF \geq \sqrt{N}$.

6. a-pseudoprime. The next shows that divisors of $\Phi_n(a)$ are almost a-pseudoprimes.

Theorem 6.1. *If D is a divisor of $\Phi_n(a)$ and D is not divided by*

the maximal prime divisor of n, then $a^{D-1} \equiv 1 \bmod D$.

Proof. Let p be a prime divisor of D and so of $\Phi_n(a)$. Then $n = |a|_p$ is a divisor of $p-1$, equivalently, $n \equiv 1 \bmod p$. Hence $D \equiv 1 \bmod n$. Since

The next contains the result of E. Malo [2] for $a = 2$.

[illegible]

is a-pseudoprime with $(n, a-1) = 1$.

Proof. Let M be the set of divisors of n different from 1. Then the assumption $(n, a-1) = 1$ is equivalent to $(n, a^n - 1) = 1$ since n is a-pseudoprime. This implies that $(d, \Phi_d(a)) = 1$ for $d|n$. Theorem together

[illegible]

Theorem 7.2. *$M_q = 2^q - 1$ is prime and $\left(\frac{D}{M_q}\right) = \left(\frac{Q}{M_q}\right) = -1$ if*

FACULTY OF SCIENCE
HIROSAKI UNIVERSITY
HIROSAKI 036, JAPAN

(*Received January 23, 1996*)