ON VALUES OF CYCLOTOMIC POLYNOMIALS. II



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

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

 $1 \mod p^2$.

Proof. Theorem implies our assertion from

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

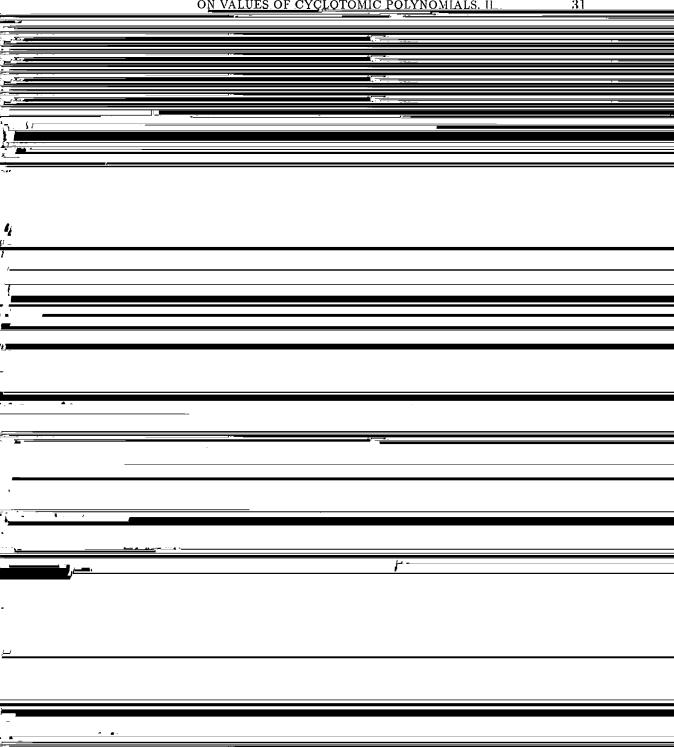
The next needs later. It is easy to see $np = |a+p|_{p^2}$ from the conditions of this proposition.

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

_	ON VALUES OF CYCLO	TOMIC POLYNOMIALS. II	29
			,
-		- Y	/
**************************************		The second secon	
		The second secon	
		, (i.e., 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	/
-			,
			,
			<u> </u>
-11 -12			
J			
_			
	-		
	·		
- · ·	primitive root for every prime.	A Commission	,
Ja e		·	
		<u> </u>	

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 g is a divisor of $\Phi_n(a)$ and r is a prime

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

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

Proof. Let p be a prime divisor of N. By the assumptions, we have $0 \equiv \Phi_q(s) \equiv \Phi_q(u^{q^{e-1}}) = \Phi_{q^e}(u) \mod N$ 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 $(t^R - 1)/(t - 1) = \prod_{d \mid R, d > 1} \Phi_d(t)$ and so d = |t|, 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 $\Phi_{\mathbf{u}}(a)$ and D is not divided by

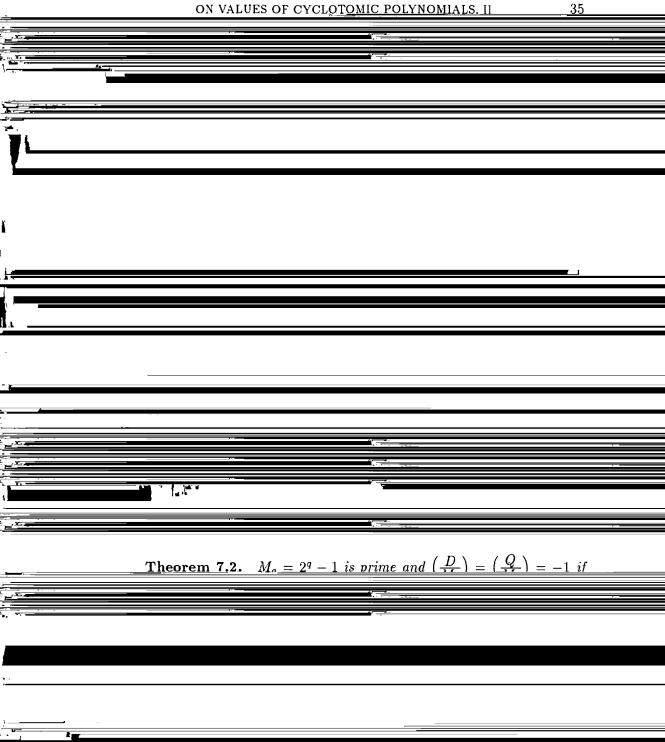
the maximal prime divisor of n, then $a^{D-1} \equiv 1 \mod D$.

Proof. Let p be a prime divisor of D and so of $\Phi_n(a)$. Then $n = |a|_p$

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

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 apsendoprime. This implies that $(d, \Phi_d(a)) = 1$ for d|n. Theorem together



Faculty of Science Hirosaki University

HIROSAKI 036, JAPAN

(Received January 23, 1996)