J. Korean Math. Soc. **26**(1989), No. 1, pp. 75~82

ON THE PRIMALITY OF THE MERSENNE NUMBER M_p

SHIN-WON KANG

There are some theorems which give the practical tests for the primality of the Mersenne number M_p where p is an odd prime. [1] [2]. The purpose of this paper is to derive much more general results of the above theorems by using the properties of the polynomials $S_n(a, x)$ and $D_n(a, x)$.

Let a be a nonzero integer. For every positive integer n the polynomials $S_n(a, x)$ and $D_n(a, x)$ are defined as follows:

$$S_n(a, x) = \sum_{i=0}^{[\frac{n}{2}]} \binom{n-i}{i} a^{n-2i} x^i$$

$$D_n(a, x) = \sum_{i=0}^{[\frac{n}{2}]} \frac{n}{u-i} \binom{n-1}{i} a^{n-2i} x^i$$

If a is a nonzero fixed element in F_p where p is an odd prime, then the polynomials $S_p(a, x)$ and $S_{p-2}(a, x)$ split over F_p and have distinct $(p-1)/2$ and $(p-3)/2$ roots in F_p respectively. More precisely, if $(a, p)=1$, p is an odd prime, then [4].

$$a^2(1-x^{p-1}) \equiv S_p(a, x) S_{p-2}(a, x)(a^2+4x) \pmod{p}.$$

If n is odd, say $n=2r+1$ for some positive integer r, then we have that [3]

$$S_n(a, x) = S_r(a, x) D_{r+1}(a, x)$$

Let K be a field of characteristic p and n a positive integer not divisible by p, and ζ a primitive n-th root of unity over K. The polynomial

$$\Phi_n(x) = \prod_{\substack{s=1 \\ (n,s)=1}}^{n} (x-\zeta^s)$$

is the n-th cyclotomic polynomial over K. When we refer to the characteristic p of K in this discussion, we permit the case $p=0$ as well. The following facts are well known. [6]

Recieved June 1, 1988.
Revised October 17, 1988.

(i) $x^n-1=\prod_{d|n}\Phi_d(x)$

(ii) The coefficients of $\Phi_n(x)$ belong to the prime subfield of K, and to Z if the prime subfield of K is the field of rational numbers.

(iii) If $K=Q$, then the n-th cyclotomic polynomial $\Phi_n(x)$ is irreducible over K and $[K^{(n)}:K]=\phi(n)$, where $K^{(n)}$ is the splitting field of x^n-1 over K.

(iv) If $K=F_q$ with $(q,n)=1$, then $\Phi_n(x)$ factors into $\phi(n)/d$ distinct monic irreducible polynomials in $K[x]$ of the same degree d; $K^{(n)}$ is the splitting field of any such irreducible factor over K; and $[K^{(n)}:K]=d$, where d is the least positive integer such that $q^d\equiv 1 \pmod n$

LEMMA 1. *Let K be a field of characteristic p, and n and m the positive integers not divisible by p. Then*

$$\Phi_n(x^m)=\prod_{\substack{d|m \\ (\frac{m}{d},n)=1}}\Phi_{dn}(x)$$

Proof. See [5]

If α and β are the roots of the characteristic polynomial $f(t)=t^2-at-x$ of the polynomial $S_n(a,x)$ (or, equivalently $D_n(a,x)$), then [3]

$$S_n(a,x)=\alpha^n+\alpha^{n-1}\beta+\cdots+\alpha\beta^{n-1}+\beta^n$$
$$D_n(a,x)=\alpha^n+\beta^n.$$

If $n\geq 2$, then $\Phi_n(x)=0$ is a reciprocal equation over K and $\beta^{\phi(n)}\Phi_n\left(\frac{\alpha}{\beta}\right)$ is a symmetric polynomial of degree $\phi(n)$ in α and β over K, where $\alpha\beta\neq 0$.

DEFINITION. Let a and b vary over nonzero integers and α and β the roots of the polynomial $f(x)=x^2-ax-b$ over Q. If $n\geq 2$, then $\beta^{\phi(n)}\Phi_n\left(\frac{\alpha}{\beta}\right)$ is a polynomial in a and b over Z and is denoted by $K_n(a,b)$.

Simple calculation shows that $K_2(a,b)=a$, $K_3(a,b)=a^2+b$, $K_4(a,b)=a^2+2b$, $K_5(a,b)=a^4+3a^2b+b^2$, $K_6(a,b)=a^2+3b, \cdots$

LEMMA 2. *Let a and b be any nonzero integers and $n\geqq 2$ is a positive integer.* Then

$$S_n(a,b)=\prod_{\substack{d\mid(n+1)\\ d>1}} K_d(a,b),$$

$$D_n(a,b)=\prod_{\substack{d\mid n\\ \left(\frac{n}{d},2\right)=1}} K_{2d}(a,b).$$

Proof. Since $\Phi_1(x)=x-1$ and $x^{n+1}-1=(x-1)(x^n+x^{n-1}+\cdots+x+1)=\prod_{d\mid(n+1)}\Phi_d(x)$ we have that $x^n+x^{n-1}+\cdots+x+1=\prod_{\substack{d\mid(n+1)\\ d>1}}\Phi_d(x)$.

So, $S_n(a,b)=\alpha^n+\alpha^{n-1}\beta+\cdots+\alpha\beta^{n-1}+\beta^n=\prod_{\substack{d\mid(n+1)\\ d>1}}\beta^{\phi(d)}\Phi_d\left(\frac{\alpha}{\beta}\right)$

$$=\prod_{\substack{d\mid(u+1)\\ d>1}} K_d(a,b).$$

$$D_n(a,b)=\alpha^n+\beta^n=\beta^n\left[\left(\frac{\alpha}{\beta}\right)^n+1\right]=\beta^n\Phi_2\left[\left(\frac{\alpha}{\beta}\right)^n\right]$$

$$=\beta_n\prod_{\substack{d\mid n\\ \left(\frac{n}{d},2\right)=1}}\Phi_{2d}\left(\frac{\alpha}{\beta}\right)=\prod_{\substack{d\mid n\\ \left(\frac{n}{d},2\right)=1}}\beta^{\phi(2d)}\Phi_{2d}\left(\frac{\alpha}{\beta}\right)=\prod_{\substack{d\mid n\\ \left(\frac{n}{d},2\right)=1}}K_{2d}(a,b).$$

Here we used the fact that $\sum_{\substack{d\mid n\\ \left(\frac{n}{d},2\right)=1}}\phi(2\mathrm{d})=n$ which can be proved easily.

LEMMA 3. $\Phi_n(1)=K_n(2,-1)$

Proof. If $a=2$ and $b=-1$, then $f(x)=x^2-2x+1$ has the roots $\alpha=\beta=1$ and the lemma is true.

COROLLARY 1. *If p is an odd prime, then*

$$K_p(2,-1)\equiv 0 \ (mod\ p)$$

Proof. If p is an odd prime, then $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ and $\Phi_p(1)=p\equiv 0 \pmod p$.

COROLLARY 2. *If p is an add prime, then*

$$K_p(a,b)\equiv(a^2+4b)^{(p-1)/2}\ (mod\ p)$$

Proof. If p is an add prime, then [3]

$$S_{p-1}(a, b) \equiv (a^2+4b)^{(p-1)/2} \pmod{p}.$$

From Lemma 2, $S_{p-1}(a, b) = \prod_{\substack{d|p \\ d>1}} K_d(a, b) = K_p(a, b)$.

LEMMA 4. *Let q be an odd prime and a_1 and b_1 the integers not divisible by q. If $K_n(a_1, b_1) \equiv 0 \pmod{q}$, $n \geqq 3$, then $K_n(a, b)$ has a factor of the form a^2+cb over F_q, where $c = -(a_1^2)/b_1$.*

Proof. Since $\Phi_n(x) = x^r[(x+1/x)^r + d_1(x+1/x)^{r-1} + \cdots + d_r]$, suppose that $K_n(a, b) = (a^2)^r + s_1(a^2)^{r-1}b + \cdots + s_r b^r$ where $r = \phi(n)/2$ and $K_n(a_1, b_1) \equiv 0 \pmod{q}$. Let us denote $(b^{-1})^r K_n(a, b)$ by $F(b^{-1}a^2)$, then $F(x) = x^r + s_1 x^{r-1} + \cdots + s_r$ has a root $x = b_1^{-1}a_1^2$ over F_q. This means that $x - b_1^{-1}a_1^2$ is a linear factor of $F(x)$ and equivalently a^2+cb is a factor of $K_n(a, b)$, where $c = -(a_1^2)/b_1$.

LEMMA 5. *Let a and b be integers, then for a positive integer n, $D_{2n}(a, b) = [D_n(a, b)]^2 - 2(-b)^n$*

Proof. $[D_n(a, b)]^2 = (\alpha^n + \beta^n)^2 = \alpha^{2n} + \beta^{2n} + 2(\alpha\beta)^n = D_{2n}(a, b) + 2(-b)^n$. So the lemma is true.

Let p be an odd prime and $M = M_p = 2^p - 1$. Suppose that $M = M_p$ is prime. Since $S_M(a, x)$ and $S_{M-2}(a, x)$ split over F_M and have distinct $(M-1)/2$ and $(M-3)/2$ roots in F_M respectively, they can be factored over F_M as follows:

$$S_M(a, x) = S_{2^p-1}(a, x) = S_1(a, x) D_2(a, x) D_{2^2}(a, x) \cdots D_{2^{p-1}}(a, x)$$
$$= a(a^2+c_1x) \cdots (a^2+c_ix) \cdots (a^2+c_{(M-1)/2}x)$$

$S_{M-2}(a, x) = S_{2^{p-1}-2}(a, x) D_{2^{p-1}-1}(a, x)$ and consequently

$$S_{2^{p-1}-2}(a, x) = (a^2+d_1x) \cdots (a^2+d_{2^{p-2}-1}x)$$
$$D_{2^{p-1}-1}(a, x) = a(a^2+e_1x) \cdots (a^2+e_{2^{p-2}-1}x).$$

If a^2+cx is a factor of $D_{2^{i-1}}(a, x)$, $2 \leqq i \leqq p-1$, then $(\alpha+\beta)^2 - c\alpha\beta = \alpha^2+\beta^2+(2-c)\alpha\beta$ is a factor of $\alpha^{2^{i-1}} + \beta^{2^{i-1}}$. So of course $\alpha^4+\beta^4+(2-c)\alpha^2\beta^2$ is a factor of $\alpha^{2^i} + \beta^{2^i} = D_{2^i}(a, x)$ and must be factored over F_M as $\alpha^4+\beta^4+(2-c)\alpha^2\beta^2 = (\alpha^2+\beta^2)^2 - c\alpha^2\beta^2 = (\alpha^2+\beta^2+k\alpha\beta)(\alpha^2+\beta^2-k\alpha\beta)$ where $k^2 = c$ and we have that $\left(\frac{c}{M}\right) = 1$. On the other-hand, if $a^2+dx = \alpha^2+\beta^2+g\alpha\beta$ is a factor of $S_{2^{p-1}-2}(a, x)$, then there exists $\alpha^2+\beta^2+h\alpha\beta = a^2+fx$ which is also a factor of $S_{2^{p-1}-2}(a, x)$

such that $2-h^2=g$ over F_M [4]. This means that $\alpha^2+\beta^2+g\alpha\beta=a^2+dx=\alpha^2+\beta^2+(2-h^2)\alpha\beta=(\alpha+\beta)^2-h^2\alpha\beta=a^2+h^2x$ and we have that $d=h^2$ and $\left(\frac{d}{M}\right)=1$. Since $a^2(1-x^{M-1})\equiv S_M(a,x)(S_{M-2}(a,x)(a^2+4x)$ (mod M) and there are $(M-3)/2$ elements of F_M such that $\left(\frac{c}{M}\right)=1$, $c\neq 4$, we conclude that if $\left(\frac{c}{M}\right)=1$, then a^2+cx is a factor of $D_{2^{i-1}}(a,x)$, $2\leqq i\leqq p-1$, or $S_{2^{p-1}-2}(a,x)$ and if $\left(\frac{c}{M}\right)=-1$, then a^2+cx is a factor of $D_{2^{p-1}}(a,x)$ or $D_{2^{p-1}-1}(a,x)$ because there are $(M-1)/2$ elements of F_M such that $\left(\frac{c}{M}\right)=-1$. So we have the following result:

LEMMA 6. *Let p be an odd prime and $M=M_p=2^p-1$. If M is prime, then a^2+cx is a factor of $D_{2^{p-1}}(a,x)$ or $D_{2^{p-1}-1}(a,x)$ over F_M, if and only if* $\left(\frac{c}{M}\right)=-1$.

THEOREM 1. *Let p be any odd prime and $M=M_p=2^p-1$. Suppose that for nonzero integers a_1 and b_1, $\left(\frac{b_1}{M}\right)=1$ and $\left(\frac{a_1^2+4b_1}{M}\right)=-1$. Then M is prime if and only if $K_{2^p}(a_1,b_1)=D_{2^{p-1}}(a_1,b_1)\equiv 0$ (mod M).*

Proof. Suppose that $M=M_p$ is prime and $\left(\frac{a_1^2+4b_1}{M}\right)=-1$. Then $f(t)=t^2-a_1t-b_1$ is irreducible over F_M and so $S_M(a_1,b_1)=0$ in F_M. [3] This means that

$$S_M(a_1,b_1)=S_1(a_1,b_1)D_2(a_1,b_1)D_{2^2}(a_1,b_1)\cdots D_{2^{p-1}}(a_1,b_1)=0$$

in F_M, and for some positive integer r, $2<r\leqq p-1$, we must have that $D_{2^r}(a_1,b_1)=0$ in F_M. As $S_M(a_1,x)$ splits over F_M, so does $D_{2^r}(a_1,x)$ and there exists a factor a_1^2+cx of $D_{2^r}(a_1,x)$ over F_M such that $a_1^2+cb_1=0$ in F_M. Consequently we have that $1=\left(\frac{a_1^2}{M}\right)=\left(\frac{-cb_1}{M}\right)=\left(\frac{-1}{M}\right)\left(\frac{c}{M}\right)\left(\frac{b_1}{M}\right)=-\left(\frac{c}{M}\right)$ and from Lemma 6, a_1^2+cx must be a factor of $D_{2^{p-1}}(a_1,x)$, and $D_{2^{p-1}}(a_1,b_1)\equiv 0$ (mod M)

is evident. From Lemma 2, we have that $D_{2^{p-1}}(a_1, b_1)=K_{2^p}(a_1, b_1)$.

Conversely, assume that M is composite and $D_{2^{p-1}}(a_1, b_1)=K_{2^p}(a_1, b_1)\equiv 0 \pmod{M}$ holds. Then the same congruence is true to any modulus q which divides M. Suppose that $K_{2^p}(a_1, b_1)\equiv 0 \pmod{q}$ where q is an odd prime factor of M. Then from Lemma 4, $K_{2^p}(a, b)$ has a factor a^2+cb where $c=-(a_1)^2/b_1$ over F_q. Since $a^2+cb=(\alpha+\beta)^2-c\alpha\beta=\alpha^2+\beta^2+(2-c)\alpha\beta$ is a factor of $K_{2^p}(a, b)=\alpha^{2^{p-1}}+\beta^{2^{p-1}}=\beta^{\phi(2^p)}\Phi_{2^p}\left(\frac{\alpha}{\beta}\right)$, $K_{2^p}(a, b)$ factors into the product of quadratic symmetric polynomials in α and β over F_q and $q^2\equiv 1 \pmod{2^p}$. From the theorems of factorization of $\Phi_{2^p}(x)$ over F_q we must have that

$$q-1=k(2^p) \text{ or } q+1=k(2^p).$$

The former is impossible because q is greater than M and the latter is impossible unless $k=1$. Hence $q=M$ and M is prime.

To compute the value of $D_{2^{p-1}}(a_1, b_1)=K_{2^p}(a_1, b_1)$, we use the following sequence $\{r_i\}$ which is obtained from Lemma 5.

$$r_1=D_2(a_1, b_1)=a_1^2+2b_1$$
$$r_2=D_{2^2}(a_1, b_1)=\{D_2(a_1, b_1)\}^2-2(-b_1)^2=r_1^2-2(-b_1)^2$$
$$\cdots\cdots\cdots\cdots$$
$$r_i=D_{2^i}(a_1, b_1)=\{D_{2^{i-1}}(a_1, b_1)\}^2-2(-b)^{2^{i-1}}=r_{i-1}^2-2b^{2^{i-1}}$$

Corollary 1. *Let p be any odd prime and $M=M_p=2^p-1$. M is prime if and only if $r_{p-1}\equiv 0 \pmod{M}$*
where $r_1=4$, $r_i=r_{i-1}^2-2$, $i\geqq 2$. [1].

Proof. Since $M=2^p-1$, $2^p\equiv 1 \pmod{M}$ and $2^{p+1}\equiv 2 \pmod{M}$. Put $2^{(p+1)/2}=a_1$, and $1=b_1$, then $a_1^2\equiv 2 \pmod{M}$ and $\left(\frac{2}{M}\right)=1$. So we have that

$$\left(\frac{a_1^2+4b_1}{M}\right)=\left(\frac{2+4}{M}\right)=\left(\frac{6}{M}\right)=\left(\frac{2}{M}\right)\left(\frac{3}{M}\right)=-1$$

because $M\equiv 1 \pmod{3}$. Now, $r_1=D_2(a_1, b_1)=a_1^2+2b_1\equiv 4 \pmod{M}$, $r_2=D_4(a_1, b_1)\equiv 4^2-2=14 \pmod{M}$, $\cdots$, $r_{p-1}\equiv(r_{p-2})^2-2 \pmod{M}$. This completes the proof.

Corollary 2. *Let p be a prime of the form $4n+3$ where n is a* *positive integer. Then* $M=M_p=2^p-1$ *is prime if and only if* $r_{p-1} \equiv 0 \pmod{M}$ where $r_1=3$, $r_i=r_{i-1}^2-2$, $i \geqq 2$. [1] [2].

Proof. If p is a prime of the form $4n+3$, then $2^p-1=2^{4n+3}-1=(16)^n \cdot 8-1 \equiv 2 \pmod{5}$.

So we have that $\left(\frac{5}{M}\right)=-1$ and we may put $a_1=1$, and $b_1=1$ in Theorem 1. Now $r_1=D_2(a_1, b_1)=a_1^2+2b_1=3$, $r_2=3^2-2=7$, $\cdots$ The corollary is true.

Theorem 2. *Let p be any odd prime and $M=M_p=2^p-1$. Suppose that for some nonzero integers a_1 and b_1, $\left(\frac{b_1}{M}\right)=1$, $\left(\frac{a_1^2+4b_1}{M}\right)=1$ and $D_d(a_1, b_1) \not\equiv 0$ (mod M) where d is a divisor of $2^{p-1}-1$ such that $1<d<2^{p-1}-1$. Then M is prime if and only if $K_{2^p-2}(a_1, b_1) \equiv 0$ (mod M).*

Proof. Suppose that $M=M_p$ is prime and $\left(\frac{a_1^2+4b_1}{M}\right)=1$. Then $f(t)=t^2-a_1t-b_1$ is reducible over F_M and $S_{M-2}(a_1, b_1)=0$ in F_M. [4] This means that $S_{M-2}(a_1, b_1)=S_{2^{p-1}-2}(a_1, b_1)D_{2^{p-1}-1}(a_1, b_1)=0$ in F_M. Since $S_{M-2}(a_1, x)$ splits over F_M, there exists a factor a_1^2+cx of $S_{M-2}(a_1, x)$ such that $a_1^2+cb_1 \equiv 0 \pmod{M}$. Then $\left(\frac{c}{M}\right)=-1$ and from Lemma 6. a_1^2+cx is a factor of $D_{2^{p-1}-1}(a_1, x)$, and $D_{2^{p-1}-1}(a_1, b_1) \equiv 0 \pmod{M}$. Since
$$D_{2^{p-1}-1}(a, b)=\prod_{\substack{d \mid n \\ \left(\frac{n}{d}, 2\right)=1 \\ n=2^{p-1}-1}} K_{2d}(a, b)$$
and $D_d(a_1, b_1) \equiv 0 \pmod{M}$ where d is a divisor of $2^{p-1}-1$ such that $1<d<2^{p-1}-1$, $K_{2^p-2}(a_1, b_1) \equiv 0 \pmod{M}$ is evident, because if d is a divisor of $2^{p-1}-1$, $1<d<2^{p-1}-1$, then $D_d(a_1, b_1) \equiv 0 \pmod{M}$ implies that $K_{2d}(a_1, b_1) \not\equiv 0 \pmod{M}$.

Conversely, assume that $M=M_p$ is composite and $K_{2^p-2}(a_1, b_1) \equiv 0 \pmod{M}$ holds. This congruence is true to any modulus q which devides M. Suppose that $K_{2^p-2}(a_1, b_1) \equiv 0 \pmod{q}$ where q is an odd prime factor of M. Then from Lemma 4, $K_{2^p-2}(a, b)$ has a factor a^2+cb where $c=-(a_1^2)/b_1$. Since $a^2+cb=(a+\beta)^2-c\alpha\beta=\alpha^2+\beta^2+(2-c)\alpha\beta$ is a factor of $K_{2^p-2}(a, b)=\alpha^{2^{p-1}-1}+\beta^{2^{p-1}-1}=\beta^{\phi(2^p-2)}\Phi_{2^p-2}$

$\left(\frac{\alpha}{\beta}\right)$, $K_{2^p-2}(a,b)$ factors into the product of quadratic symmetric polynomials in α and β over F_q and $q^2 \equiv 1 \pmod{2^p-2}$. From the theorems of factorization of the cyclotomic polynomial $\Phi_{2^p-2}(x)$ over F_q we must have that $q+1=k(2^p-2)$ or $q-1=k(2^p-2)$. The former is impossible unless $q=1$ which is unthinkable and the latter is impossible unless $k=1$. Hence $q=M$ and M is prime.

References

1. G.H. Hardy and E.M. Wright, *An itroducton to the theory of numbers*, 4th. ed. Oxford, 1960.
2. L.K. Hua, *Introduction to number theory*, Springer-Verlag, 1982.
3. Shinwon Kang, *Remarks on finite fields III*, Bull. Korean Math. Soc. **23** (1986), 103-111.
4. Shinwon Kang, *On the factors of the polynomial $S_n(a,x)$ over F_p*, J. of Basic Sciences. Hanyang Univ. Vol. 6(1987).
5. Shinwon Kang, *A note on cyclotomic polynomials*, J. of Basic Sciences. Hanyang Univ. Vol. 7(1988).
6. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge Univ. Press 1984.

Hanyang University
Seoul 133-791 Korea