Malaya Journal of Matematik, Vol. S, No. 1, 116-119, 2019

https://doi.org/10.26637/MJM0S01/0028

Irreducibility criterion for certain trinomials

Biswajit Koley[1]* and A. Satyanarayana Reddy[2]

Abstract

In this article we study the irreducibility of polynomials of the form $x^n+\varepsilon_1 x^m+p^k\varepsilon_2$, p being a prime number and $k\geq 2$. We will show that they are irreducible for $m=1$. We have also provided the cyclotomic factors and reducibility criterion for trinomials of the form $x^n+\varepsilon_1 x^m+\varepsilon_2$, where $\varepsilon_i\in\{-1,+1\}$. This corrects few of the existing results of W. Ljuggren's on $x^n+\varepsilon_1 x^m+\varepsilon_2$.

Keywords

Cyclotomic polynomials, irreducible polynomials, reciprocal polynomials.

AMS Subject Classification

11R09, 12D05,12E05.

[1,2] *Department of Mathematics, Shiv Nadar University, Greater Noida-201314, India.*

***Corresponding author**: [1] bk140@snu.edu.in; [2]satyanarayana.reddy@snu.edu.in

Article History: Received **24** March **2019**; Accepted **09** May **2019**

Contents

1. Introduction

E.S.Selmer [7] studied the irreducibility of trinomials of the form $x^n\pm x^m\pm 1$ over $\mathbb{Q}$. He provided a complete solution for $m=1$. Later Ljunggren [4] extended Selmer's result for all $m>1$ and proved for quadrimonials as well. A version of his result for trinomials is the following.

Theorem 1.1. *(Ljunggren) Let $f(x)=x^n+\varepsilon_1 x^m+\varepsilon_2$ where $\varepsilon_j\in\{-1,+1\}$. Then $f(x)$ has at most one irreducible non-reciprocal factor and a reciprocal factor of $f(x)$ if any is the product cyclotomic polynomials.*

Ljunggren provided the possible cyclotomic factors for trinomials, but they seemed to be incorrect in certain cases. For example, according to Theorem 3 of Ljunggren [4], the polynomials $x^{50}-x^4-1$ and $x^{50}+x^{22}-1$ are divisible by x^4+x^2+1 but they are divisible by x^4-x^2+1. Similarly if d is even, $d_1\equiv 5 \pmod 6, d_2\equiv 1 \pmod 6$ and d_3 is odd, then $x^{dd_1}+x^d-1, x^{dd_2}-x^{2d}-1$ and $x^{2^{d_3}d}-x^d+1$ are divisible by $x^{2d}+x^d+1$ but they are actually divisible by $x^{2d}-x^d+1$.

Based on the above examples, we revisited Ljunggren's work and corrected those errors. For similar studies and related work, the reader can look into [1, 4, 5, 7, 8].

Immediately the question appears about the reducibility of polynomials of the form $x^n+\varepsilon_1 x^m+\varepsilon_2 p$, p being a prime. If p is an odd prime, then the polynomials are irreducible directly follows from Proposition 1 of [6]. Recently, the authors[3] have shown that $x^n+\varepsilon_1 x^m+2\varepsilon_2$ has exactly one irreducible non-reciprocal factor apart from its cyclotomic factors. The method used there doesn't apply to the polynomials $x^n+\varepsilon_1 x^m+p^k\varepsilon_2$ with $k\geq 2$. With a different approach, we will prove that

Theorem 1.2. *Suppose $f(x)=x^n+\varepsilon_1 x+\varepsilon_2 p^k$ be a polynomial of degree $n\geq 2$ with p being a prime number and $\varepsilon_i\in\{-1,+1\}, k\geq 2$. Then $f(x)$ is irreducible.*

For arbitrary m there are, indeed, polynomials which are reducible. For example,

$$x^5-x^2+4=(x^2+x+2)(x^3-x^2-x+2);$$
$$x^5-x^4+9=(x^2-3x+3)(x^3+2x^2+3x+3).$$

More generally,

$$x^{3n}+\varepsilon_1 x^{2n}+4\varepsilon_1=(x^n+2\varepsilon_1)(x^{2n}-\varepsilon_1 x^n+2),$$

for every $n\geq 1$. Although $f(x)$ is reducible for $m>1$, we will show that $f(x)$ cannot have more than k factors. More precisely,

Theorem 1.3. *Suppose p is a prime and $f(x)=x^n+\varepsilon_1 x^m+\varepsilon_2 p^k$ with $\varepsilon_i\in\{-1,+1\}$ be a polynomial of degree n and $k\geq 2$. Then $f(x)$ is a product of atmost k distinct non-reciprocal irreducible polynomials.*

The separability of such polynomials has also been considered there. Throughout the paper, we will consider the reducibility over $\mathbb{Q}$ (and hence over $\mathbb{Z}$) only. If n is a positive integer, we define $e(n)$ as the largest even part of n, i.e. $n = 2^a n_1$ with n_1 odd implies $e(n) = 2^a$.

2. Factorization of $x^n + \varepsilon_1 x^m + \varepsilon_2$

Let $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2$ be a polynomial of degree n with $\varepsilon_i \in \{-1, +1\}$. From Theorem 1.1 $f(x)$ has a cyclotomic factor whenever it is reducible. To determine the reducibility criterion of $f(x)$, it is, therefore, sufficient to find the cyclotomic factors of $f(x)$. Before we start, we recall a few basic properties of cyclotomic polynomials which will be useful later.

Proposition 2.1. *Suppose n is a positive integer and $\Phi_n(x)$ be the n^{th} cyclotomic polynomial.*

(a) Let p be a prime. Then

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n. \end{cases}$$

(b) Define $D_n^m = \{ d \in | \ (m,d) = mn \}$. Then

$$\Phi_n(x^m) = \prod_{d \in D_n^m} \Phi_d(x).$$

(c) If p is a prime and $(p,n) = 1$ then

$$\prod_{d|p^\gamma n} \Phi_d(x) = \prod_{i=0}^{\gamma} \prod_{d|n} \Phi_{p^i d}(x).$$

In particular,

$$x^n + 1 = x^{2n} - 1 / x^n - 1 = \prod_{d|2n, d\nmid n} \Phi_d(x) = \prod_{d|n} \Phi_{2d}(x).$$

(d) If n, m are positive integers, then

$$\left(\prod_{d|n} \Phi_d(x), \prod_{d|m} \Phi_d(x) \right) = \prod_{d|(n,m)} \Phi_d(x).$$

Considering the elementary nature we omit the detailed proof. One can look into Thangadurai [9] for the same.

The polynomial $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2$ is reducible if and only if $\varepsilon_2 x^n f(x^{-1}) = x^n + \varepsilon_1 \varepsilon_2 x^{n-m} + \varepsilon_2$ is reducible. Therefore, for a given n it is sufficient to consider the reducibility of polynomials $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2$ with $n \geq 2m$. Throughout the section, we will consider $m = 2^a \cdot 3^b \cdot M, n - 2m = 2^p \cdot 3^q \cdot N$ as the prime factorization of m and $n - 2m$ respectively.

Theorem 2.2. *Let $f(x) = x^n - x^m - 1$ be reducible. Then $q > b, e(m) > e(n-2m)$ and $f(x)$ is divisible by $\Phi_6(x^{(n,m)})$.*

Proof. Since $f(x)$ is reducible, from Theorem 1.1 $f(x)$ has a reciprocal factor. Consequently, there exits an $\alpha \in \mathbb{C}$, where $\alpha \neq \pm 1, 0$ such that both α and $\frac{1}{\alpha}$ are roots of $f(x)$. That is

$$\alpha^n - \alpha^m - 1 = 0 = \alpha^n + \alpha^{n-m} - 1.$$

In other words, α is a root of the polynomial $x^{n-2m} + 1$. This evenually implies $f(x)$ is irreducible for $n = 2m$. So we need to consider $n > 2m$ for the remaining part. Since α satisfies $x^{n-2m} + 1 = 0$ and $x^n - x^m - 1 = 0$, it would satisfy $x^{2m} + x^m + 1 = 0$. In particular, α is a root of $g(x) = \gcd(x^{n-2m} + 1, x^{2m} + x^m + 1)$.

From Proposition 2.1, it can be seen that $x^{2m} + x^m + 1 = \prod_{d \in D_3^m} \Phi_d(x)$, where $D_3^m = \{d \in |(m,d) = 3m\}$. If we consider the prime factorizations of m and $n - 2m$, then we have $x^{n-2m} + 1 = \prod_{i=0}^{q} \prod_{d|N} \Phi_{2^{p+1} 3^i d}(x)$ and

$$\Phi_3(x^m) = \prod_{i=0}^{a} \prod_{d|M} \Phi_{2^i 3^{b+1} d}(x).$$

Let n be odd so that $n - 2m$ odd or equivalently $p = 0$. Hence

$$\begin{aligned} g(x) &= \left(\prod_{i=0}^{a} \prod_{d|M} \Phi_{2^i 3^{b+1} d}(x), \prod_{i=0}^{q} \prod_{d|N} \Phi_{2.3^i d}(x) \right) \\ &= \left(\prod_{d|M} \Phi_{2.3^{b+1} d}(x), \prod_{i=0}^{q} \prod_{d|N} \Phi_{2.3^i d}(x) \right) \\ &= \begin{cases} \prod_{d|d_1} \phi_{2.3^{b+1} d}(x), & \text{if } q > b, \text{ where } d_1 = (N,M) \\ 1, & \text{otherwise.} \end{cases} \end{aligned}$$

If $q \geq b+1$ then $n = 2^{a+1} 3^b M + 3^q N = 3^b u_3$ where u_3 odd and $3 \nmid u_3$.
Also, $(n - 2m, m) = (n, m) = 3^b d_1$ gives $\prod_{d|d_1} \phi_{2.3^{b+1} d}(x) = \prod_{d|d_1} \phi_{6.3^b d}(x) = \Phi_6(x^{(n,m)})$.

On the other hand, if n is even then $n - 2m$ is even and $p \geq 1$. Then

$$\begin{aligned} g(x) &= \left(\prod_{i=0}^{a} \prod_{d|M} \Phi_{2^i 3^{b+1} d}(x), \prod_{i=0}^{q} \prod_{d|N} \Phi_{2^{p+1}.3^i d}(x) \right) \\ &= \begin{cases} \prod_{d|d_2} \Phi_{2^{p+1}.3^{b+1} d}(x), & \text{if } a > p, q > b \\ 1, & \text{otherwise,} \end{cases} \end{aligned}$$

where $d_2 = (N,M)$. If $a \geq p+1, q \geq b+1$ then $n = 2^{a+1} 3^b M + 2^p 3^q N = 2^p 3^b u_4$ where $(u_4, 6) = 1$. □

Corollary 2.3. *If $n = 2^a 3^b$ with $a + b > 0$ then $x^n - x^m - 1$ is irreducible for every $m < n$.*

Since the proof for the remaining three families are almost same, instead of duplicating we state them without proof. The detailed proof can be carried out by using Proposition 2.1 and Theorem 2.2.

Theorem 2.4. *Let $f(x) = x^n + \varepsilon_1 x^m - \varepsilon_1$ be reducible with $\varepsilon_1 \in \{-1,+1\}$. Then $f(x)$ is divisible by $\Phi_6(x^{(n,m)})$ and the following holds:*

(a) $\varepsilon_1 = 1, e(m) = e(n-2m), q > b$;

(b) $\varepsilon_1 = -1, e(m) < e(n-2m), q > b$.

Theorem 2.5. *Let $f(x) = x^n + x^m + 1$ be reducible. Then $f(x)$ is divisible by $\Phi_3(x^{(n,m)})$ and either of the following holds necessarily*

(a) $n = 2m, M > 1$;

(b) $n \neq 2m, q > b$.

If we summarize all the results of this section, it fits perfectly within the below tables.

If $n = 2m$ then $x^n \pm x^m - 1$ are irreducible. And $x^n - x^m + 1 = \Phi_6(x^m)$, $x^n + x^m + 1 = \Phi_3(x^m)$ are reducible or irreducible according to Proposition 2.1(b).

If $n \neq 2m$ then

1. If m is odd then $x^n - x^m - 1$ is irreducible.
2. If $m+n$ is odd then $x^n + x^m - 1$ is irreducible.
3. If n is odd then $x^n - x^m + 1$ is irreducible.

The following tables summarize the irreducibility of all polynomials for $n \neq 2m$. Suppose $m = 2^a \cdot 3^b \cdot M$, $n - 2m = 2^p \cdot 3^q \cdot N$. And F is the nontrivial reciprocal factor of $x^n \pm x^m \pm 1$.

m	n	$x^n - x^m - 1$	$x^n + x^m - 1$
even	odd	reducible if $q > b$ $F = \Phi_6(x^{(n,m)})$	irreducible
even	even	reducible if $q > b, a > p$ $F = \Phi_6(x^{(n,m)})$	reducible if $a = p$, $q > b$ $F = \Phi_6(x^{(n,m)})$
odd	even	irreducible	irreducible
odd	odd	irreducible	same as even-even

and

m	n	$x^n - x^m + 1$	$x^n + x^m + 1$
even	odd	irreducible	reducible if $q > b$ $F = \Phi_3(x^{(n,m)})$
even	even	reducible if $p > a, q > b$ $F = \Phi_6(x^{(n,m)})$	same as above
odd	even	same as above	same as above
odd	odd	irreducible	same as above

3. Factorization of $x^n + \varepsilon_1 x^m + p^k \varepsilon_2$

Suppose $f(x) = x^n + \varepsilon_1 x^m + p^k \varepsilon_2$ be a polynomial of degree n with $\varepsilon_i \in \{-1,+1\}, k \geq 2$. We will first prove the separability of such polynomials using discriminant. It is known that

Theorem 3.1. *[2] The discriminant of the trinomial $x^n + ax^m + b$ is*

$$D = (-1)^{\binom{n}{2}} b^{m-1} \left[n^{n/d} b^{n-m/d} - (-1)^{n/d} (n-m)^{n-m/d} m^{m/d} a^{n/d} \right]^d$$

where $d = (n,m)$.

Theorem 3.2. *Let p be a prime. The polynomial $f(x) = x^n + \varepsilon_1 x^m + p^k \varepsilon_2$ is separable over , $\varepsilon_i \in \{-1,+1\}$.*

Proof. By Theorem 3.1, the discriminant of $f(x)$ is

$$D_f = (-1)^{\binom{n}{2}} (p^k \varepsilon_2)^{m-1} \left[n^{n/d} (p^k \varepsilon_2)^{n-m/d} - (-\varepsilon_1)^{n/d} (n-m)^{n-m/d} m^{m/d} \right]^d \tag{3.1}$$

with $d = (n,m)$. Since $f(x)$ is separable over $\mathbb{Q}$ if and only if $f(x^d)$ is separable, it is sufficient to consider $d = 1$. $f(x)$ has multiple root if and only if $D_f = 0$. Then from (3.1), we have

$$n^n (p^k \varepsilon_2)^{n-m} = (-\varepsilon_1)^n (n-m)^{n-m} m^m$$

which is not possible as $d = 1$ and p being a prime. □

Theorem 3.3. *Let p be a prime and $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 p^k$ be a polynomial of degree n with $k \geq 2$. Then $f(x)$ has all its root on the region $|z| > 1$.*

Proof. Let z_1 be a root of $f(x)$ with $|z_1| \leq 1$. Then $f(z_1) = 0$ gives

$$p^k \varepsilon_2 = -(z_1^n + \varepsilon_1 z_1^m).$$

Taking modulus on both side gives $p^k = |z_1^n + \varepsilon_1 z_1^m| \leq |z_1|^n + |z_1|^m \leq 2$, which contradicts the fact that p is a prime number and $k \geq 2$. Hence all the roots of $f(x)$ lies in the region $|z| > 1$. □

By using this theorem, we will prove Theorem 1.3.

Proof of Theorem 1.3: Suppose $f(x) = \prod_{i=1}^{t} f_i(x)$ be the non-trivial factorization of $f(x)$, where each $f_i(x)$ is irreducible. Since $f(x)$ is a monic polynomial, we assume that each $f_i(x)$ is monic. From Theorem 3.2 $f(x)$ being separable, $f_i(x) \neq f_j(x)$ for $i \neq j$. By using Theorem 3.3, from $|f(0)| = p^k = \prod_{i=1}^{t} |f_i(0)|$, we have $|f_i(0)| \geq p$. In other words, $t \leq k$ and consequently they are non-reciprocal. □

Now we will prove the irreducibility of $x^n+\varepsilon_1 x+\varepsilon_2 p^k$ for every $k\geq 2$.

Proof of Theorem 1.2: If $f(x)=x^2+\varepsilon_1 x+p^k\varepsilon_2$ is reducible then all of its roots are integers only, by Rational Root theorem. But $u(u+\varepsilon_1)=-\varepsilon_2 p^k$ and $k\geq 2$ is not possible for any integer u.

Suppose $n\geq 3$ and $f(x)$ is reducible. Let $f(x)=f_1(x)f_2(x)$ be a non-trivial factorization of $f(x)$ with $\deg(f_1)=s$. Without loss of generality, we assume that both $f_1(x), f_2(x)$ are monic polynomials. From Theorem 3.3 we have $|f_i(0)|\geq p$. Since $f_1(0)f_2(0)=p^k\varepsilon_2$, let $|f_1(0)|=p^v$ and $|f_2(0)|=p^{k-v}$ for some $v\geq 1$. We consider the following two polynomials

$$g(x)=x^s f_1(x^{-1})f_2(x)=\sum_{i=0}^{n} b_i x^i, \text{say}$$

and $\tilde{g}(x)=\sum_{i=0}^{n} b_{n-i}x^i$. The way the polynomials has been defined, we have $f_1(0)=b_n$ and $f_2(0)=b_0$. Let $b_n=p^v\varepsilon_2'$ with $|\varepsilon_2'|=1$. Since $g(x)\tilde{g}(x)=x^n f(x)f(x^{-1})$, comparing the coefficients of x^n, we get

$$\sum_{i=1}^{n-1} b_i^2 = p^{2k}-p^{2(k-v)}-p^{2v}+2.$$

Suppose there are r number of non-zero b_i's, say $0<j_r<j_{r-1}<\cdots<j_1<n$ such that $b_{j_l}\neq 0$. Then $g(x)=b_n x^n+b_{j_1}x^{j_1}+\cdots+b_{j_r}x^{j_r}+b_0$ and

$$g(x)\tilde{g}(x)=p^k\varepsilon_2 x^{2n}+b_n b_{j_r}x^{2n-j_r}+b_0 b_{j_1}x^{n+j_1}+\cdots+p^k\varepsilon_2. \tag{3.2}$$

Whereas

$$f(x)x^n f(x^{-1})=p^k\varepsilon_2 x^{2n}+\varepsilon_1 x^{2n-1}+p^k\varepsilon_1\varepsilon_2 x^{n+1}+\cdots+p^k\varepsilon_2. \tag{3.3}$$

Since $n\geq 3$, the second largest term in (3.3) is x^{2n-1} and has coefficient ε_1. The second largest term in (3.2) is either x^{2n-j_r} or x^{n+j_1} or both. That is either $j_r=1$ or $j_1=n-1$ or $n=j_r+j_1=1+(n-1)$ respectively. In all these cases, the corresponding coefficient is divisible by p which is impossible. Therefore $f(x)$ has to be irreducible. □

References

[1] C. Finch and L. Jones, On the irreducibility of $\{-1,0,1\}$-quadrinomials, *Integers* 6(A16), 2006.

[2] C.R. Greenfield and D. Drucker, On the Discriminant of a Trinomial, *Linear Algebra its Appl.* 62(1984), 105–112.

[3] B.Koley and A.S. Reddy, On an irreducibility criterion for polynomials, (preprint).

[4] W.Ljunggren, On the irreducibility of certain trinomials and quadrinomials, *Math.Scand.* 8 (1960), 65–70.

[5] W.H. Mills, The factorization of certain quadrinomials, *Math. Scand.* 57 (1985), 44–50.

[6] L. Panitopol and D. Stefänescu, Some criteria for irreducibility of polynomials,*Bull. Math. Soc. Sci. Math. R. S. Roumanie (N. S.),* 29 (1985), 69–74.

[7] E. S. Selmer, On the irreducibility of certain trinomials, *Math.Scand.* 4 (1956), 287–302.

[8] H. Tverberg, On the irreducibility of the trinomials $x^n\pm x^m\pm 1$, *Math.Scand.* 8 (1960), 121–126.

[9] R. Thangadurai, *On the coefficients of cyclotomic polynomials, Cyclotomic fields and related topics (Pune, 1999),* Bhaskaracharya Pratishthana, Pune, 2000, 311—322.

★★★★★★★★★

ISSN(P):2319 – 3786

Malaya Journal of Matematik

ISSN(O):2321 – 5666

★★★★★★★★★