ON THE IRREDUCIBILITY OF $\{-1,0,1\}$–QUADRINOMIALS

Carrie Finch
Department of Mathematics, University of South Carolina, Columbia, SC 29208, USA
cfinch@math.sc.edu

Lenny Jones
Department of Mathematics, Shippensburg University, Shippensburg, PA 17257, USA
lkjone@ship.edu

Received: 12/14/05, Revised: 4/12/06, Accepted: 4/25/06, Published: 5/15/06

Abstract

Let $a > b > c > 0$ be integers, and let $\beta, \gamma, \delta \in \{-1, 1\}$. We give necessary and sufficient conditions, in terms of a, b and c, for the irreducibility of $f(x) = x^a + \beta x^b + \gamma x^c + \delta$ over $\mathbb{Q}$.

1. Introduction

Throughout this note we let $a > b > c > 0$ be integers; $\beta, \gamma, \delta \in \{-1, 1\}$; and $f(x) = x^a + \beta x^b + \gamma x^c + \delta$. Previous investigations into the irreducibility of $f(x)$ over $\mathbb{Q}$ have focused mainly on the nature of the possible factors or zeros of $f(x)$. In particular, Ljunggren proved the following theorem in [2].

Theorem 1. [Ljunggren] *The polynomial $f(x)$ is reducible over $\mathbb{Q}$ if and only if $f(\zeta) = 0$ for some root of unity ζ.*

In [2], Ljunggren actually indicated how $f(x)$ factors when it is reducible. His statement, however, was incorrect in that he overlooked several cases. Mills [3], still using the methods developed by Ljunggren, later published a correct version of the theorem. At the end of [2], Ljunggren stated correctly that if a, b and c are all odd, then $x^a + x^b + x^c + \delta$ is irreducible. He went on to mention that, in all cases, similar criteria for irreducibility could be straightforwardly determined using his methods, although, citing the tediousness of such a task, he did not provide them.

Recently, using a different and less arduous approach, Dubickas [1] has given sufficient conditions for the irreducibility of a larger class of the quadrinomials $f(x)$ in terms of the exponents a, b and c. In addition to proving the condition stated by Ljunggren for $x^a + x^b + x^c + \delta$, Dubickas shows that if a and b are even, and c is odd, then $x^a + x^b + \gamma x^c + 1$ is irreducible. In this paper we use techniques similar to those of Dubickas to give both necessary and sufficient conditions, based solely on the exponents, for the irreducibility of all quadrinomials $f(x)$ over $\mathbb{Q}$. The proof of our result relies on Theorem 1 and Lemma 1.

Our Lemma 1 is equivalent to Lemma 1 in [1], where the proof is geometric in nature. Nonetheless, we provide a proof here since our proof is algebraic.

Lemma 1. [Dubickas] *Let z_1, z_2 and z_3 be complex numbers which lie on the unit circle, and suppose that $z_1 + z_2 + z_3 + 1 = 0$. Then $z_j = -1$ for some j.*

Proof. Since $\mathrm{Im}(z_1) + \mathrm{Im}(z_2) + \mathrm{Im}(z_3) = 0$, we can assume, without loss of generality, that $\mathrm{Im}(z_1)\,\mathrm{Im}(z_2) \geq 0$. Because $0 \leq |\,\mathrm{Re}(z_j)| \leq 1$ for each j, we also have that $(\mathrm{Re}(z_1) + 1)(\mathrm{Re}(z_2) + 1) \geq 0$. Now, note that $|1 + z_1 + z_2| = 1$. We can expand and rewrite this equation to get

$$(\mathrm{Re}(z_1) + 1)(\mathrm{Re}(z_2) + 1) + \mathrm{Im}(z_1)\,\mathrm{Im}(z_2) = 0.$$

Therefore, it follows that $\mathrm{Im}(z_1)\,\mathrm{Im}(z_2) = (\mathrm{Re}(z_1) + 1)(\mathrm{Re}(z_2) + 1) = 0$. Suppose that $\mathrm{Im}(z_1) = 0$. Then $z_1 = \pm 1$. If $z_1 = -1$, we are done. If $z_1 = 1$, then $\mathrm{Re}(z_2) = -1$, and consequently, $z_2 = -1$. Since the same argument can be used if $\mathrm{Im}(z_2) = 0$, the proof is complete. $\square$

2. The Main Result

We begin with some notation. Suppose that $\gcd(a, b, c) = 2^k m$, where m is odd. Let $a' = a/2^k$, $b' = b/2^k$ and $c' = c/2^k$. Define $\bar{a} := \gcd(a', b' - c')$. Similarly, define $\bar{b}$ and $\bar{c}$.

Theorem 2. *The quadrinomial $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f(x)$ satisfies one of the following sets of conditions.*

1. $(\beta, \gamma, \delta) = (1, 1, 1)$
   $\bar{a}\bar{b}\bar{c} \equiv 1 \pmod 2$

2. $(\beta, \gamma, \delta) = (-1, 1, 1)$
   $b' - c' \not\equiv 0 \pmod{2\bar{a}}$, $b' \not\equiv 0 \pmod{2\bar{b}}$, $a' - b' \not\equiv 0 \pmod{2\bar{c}}$

3. $(\beta, \gamma, \delta) = (1, -1, 1)$
   $b' - c' \not\equiv 0 \pmod{2\bar{a}}$, $a' - c' \not\equiv 0 \pmod{2\bar{b}}$, $c' \not\equiv 0 \pmod{2\bar{c}}$

4. $(\beta, \gamma, \delta) = (1, 1, -1)$
$a' \not\equiv 0 \pmod{2\bar{a}}$, $b' \not\equiv 0 \pmod{2\bar{b}}$, $c' \not\equiv 0 \pmod{2\bar{c}}$

5. $(\beta, \gamma, \delta) = (-1, -1, -1)$
$a' \not\equiv 0 \pmod{2\bar{a}}$, $a' - c' \not\equiv 0 \pmod{2\bar{b}}$, $a' - b' \not\equiv 0 \pmod{2\bar{c}}$

Remark. It is easy to show that the case $(\beta, \gamma, \delta) = (1, 1, 1)$ can be rewritten in a somewhat more appealing manner as follows:

> *The polynomial $f(x) = x^a + x^b + x^c + 1$ is reducible over $\mathbb{Q}$ if and only if exactly one of the integers a', b' and c' is even.*

Proof. First observe that $f(1) = 0$ for any other choice of (β, γ, δ), so that then $f(x)$ is reducible.

Note that case (2) is transformed into case (3) by replacing $f(x)$ with its reciprocal, $x^a f(1/x)$. Similarly, case (4) is transformed into case (5) by replacing $f(x)$ with the negative of its reciprocal. Since $f(x)$ is irreducible if and only if $\pm x^a f(1/x)$ is irreducible, it suffices to prove cases (1), (2) and (4) to establish the theorem.

To prove the case $(\beta, \gamma, \delta) = (1, 1, 1)$, assume first that $f(x)$ is reducible. Then, by Theorem 1, we have that $f(\zeta) = 0$, where ζ is some root of unity. By Lemma 1, either ζ^a, ζ^b or ζ^c equals -1. If $\zeta^a = -1$, then $\zeta^{b-c} = -1$. Thus,

$$(-1)^{a'} = \left(\zeta^{b-c}\right)^{a'} = \left(\zeta^{2^k(b'-c')}\right)^{a'} = (\zeta^a)^{b'-c'} = (-1)^{b'-c'},$$

which implies that a' and $b' - c'$ have the same parity. Similarly, if $\zeta^b = -1$, or $\zeta^c = -1$, then b' and $a' - c'$, or c' and $a' - b'$, respectively, have the same parity. Therefore, in any case, since at least one of the integers a', b' and c' is odd, we obtain that exactly one of a', b' and c' is even, which finishes the proof in this direction.

Conversely, if exactly one of the integers a', b' and c' is even, then, either $a' - b'$ and c' are both odd, or a' and $b' - c'$ are both odd. Consequently, $x^{2^k} + 1$ divides $f(x)$ in any situation, since

$$\begin{aligned} f(x) &= x^{2^k b'}\left(x^{2^k(a'-b')} + 1\right) + \left(x^{2^k c'} + 1\right) \\ &= \left(x^{2^k a'} + 1\right) + x^{2^k c'}\left(x^{2^k(b'-c')} + 1\right). \end{aligned}$$

We now examine case (2): $(\beta, \gamma, \delta) = (-1, 1, 1)$. First suppose that the conditions hold, but that $f(x)$ is reducible. From Theorem 1, we know that $f(\zeta) = 0$ for some root of unity ζ. Invoking Lemma 1, suppose that $\zeta^a = -1$. Then $\zeta^{b-c} = 1$. Write $a' = 2^r m_1$ and $b' - c' = 2^s m_2$, where m_1 and m_2 are odd. If $s \leq r$, then

$$(-1)^{m_2} = (\zeta^a)^{m_2} = \left(\zeta^{2^k m_2}\right)^{a'} = \left(\zeta^{2^{k+s} m_2}\right)^{a'/2^s} = \left(\zeta^{b-c}\right)^{a'/2^s} = 1,$$

which contradicts the fact that m_2 is odd. Hence, $r < s$. Then

$$2\bar{a} = 2 \cdot \gcd(a', b' - c') = 2^{r+1} \gcd\left(m_1, 2^{s-r} m_2\right).$$

Now, $b' - c'$ is divisible by both 2^{r+1} and $\gcd(m_1, 2^{s-r} m_2)$, and since they are of different parity, it follows that $b' - c'$ is divisible by their product $2\bar{a}$, which is a contradiction. The argument is similar if $\zeta^b = 1$ or $\zeta^c = -1$.

For the converse, first suppose that $b' \equiv 0 \pmod{2\bar{b}}$. Then $b'/\bar{b}$ is even, and since $b'/\bar{b}$ and $(a' - c')/\bar{b}$ are relatively prime, we have that $(a' - c')/\bar{b}$ is odd. Therefore, $x^{2^k \bar{b}} + 1$ divides $f(x)$ since

$$f(x) = x^{2^k c'} \left(x^{2^k (a' - c')} + 1\right) - \left(x^{2^k b'} - 1\right).$$

Similar arguments show that $f(x)$ is reducible if $a' - b'$ is divisible by $2\bar{c}$, or if $b' - c'$ is divisible by $2\bar{a}$.

We omit the proof of case (4) since it is similar to the proof of case (2). □

Acknowledgments

The authors thank the referee for the valuable suggestions.

References

[1] Dubickas, A., *Nonreciprocal algebraic numbers of small measure*, Comment. Math. Univ. Carolinae **45** (2004), no. 4, 693-697

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

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