Two Diophantine Approaches to the Irreducibility of Certain Trinomials

M. Filaseta[1*], F. Luca[2*], P. Stănică[3*†], R.G. Underwood[3]

[1] Department of Mathematics, University of South Carolina
Columbia, SC 29208; e-mail: filaseta@math.sc.edu

[2] IMATE, UNAM, Ap. Postal 61-3 (Xangari), CP. 58 089
Morelia, Michoacán, Mexico; e-mail: fluca@matmor.unam.mx

[3] Department of Mathematics, Auburn University Montgomery
Montgomery, AL 36124; e-mail: {pstanica,runderwo}@mail.aum.edu

1 Introduction

In the previous paper [FLSU], we determined the Galois groups associated with some polynomials constructed through the use of circulant matrices. In the process of determining the Galois groups, the irreducibility of the trinomial $x^{2p} + x^p + m^p$ was established, where p represents an odd prime and m an integer ≥ 2. The approach there was based on a method of Lebesgue [Le]. In this paper, we discuss two other approaches we discovered in our investigations, both relying on the nice work of Bilu, Hanrot, and Voutier [BHV] (with an appendix by Mignotte) on Lucas and Lehmer numbers.

In the next section, we consider the more general polynomials $t_p(x) = x^{2p} + bx^p + c$ where b and c are nonzero integers. There are four cases where reducibility is easily established:

(i) If $b^2 - 4c$ is a square, then $x^2 + bx + c$ factors so that $t_p(x)$ is the product of two polynomials of degree p.

(ii) If $p \geq 5$ and $b = u^p$ for some integer u and $c = b^2$, then $t_p(x)$ is divisible by $x^2 + ux + u^2$ (with roots $\zeta_3^{\pm 1} u$).

(iii) If $p \geq 3$ and $b = 2^{(p+1)/2} u^p$ for some integer u and $c = b^2/2$, then $t_p(x)$ is divisible by one of $x^2 + 2ux + 2u^2$ (with roots $\sqrt{2}\zeta_8^{\pm 3} u$) or $x^2 - 2ux + 2u^2$ (with roots $\sqrt{2}\zeta_8^{\pm 1} u$) depending on whether $p \equiv \pm 1 \pmod 8$ or $p \equiv \pm 3 \pmod 8$, respectively.

*The first author's research is supported by the National Science Foundation and the second author's by Grants SEP-CONACyT 37259E and 37260E. The third author is partially supported by a Research Award from the School of Sciences at his institution.

†Also associated with the Institute of Mathematics of Romanian Academy, Bucharest, Romania

(iv) If $p \geq 5$ and $b = 3^{(p+1)/2}u^p$ for some integer u and $c = b^2/3$, then $t_p(x)$ is divisible by one of $x^2 + 3ux + 3u^2$ (with roots $\sqrt{3}\zeta_{12}^{\pm 5}u$) or $x^2 - 3ux + 3u^2$ (with roots $\sqrt{3}\zeta_{12}^{\pm 1}u$) depending on whether $p \equiv \pm 1 \pmod{12}$ or $p \equiv \pm 5 \pmod{12}$, respectively.

The latter three cases can be shown, for example, by establishing that a root of the claimed quadratic factor is a root of $t_p(x)$. For convenience in a moment, we note that the condition $p \notin \{2, 3, 5, 7, 13\}$ can be reworded as p does not divide $(q-1)(q+1)$, when q is the prime 181. We establish the following.

Theorem 1. *Let p be a prime and b and c be nonzero integers not satisfying the conditions in (i), (ii), (iii), and (iv) above. Then the trinomial $t_p(x) = x^{2p} + bx^p + c$ is irreducible provided*

$$p \nmid \prod_{\substack{q \text{ prime} \\ q \mid (181 \cdot b)}} \big((q-1)(q+1)\big).$$

The condition in Theorem 1 that p not divide the product appears too strong as typically the trinomial $x^{2p} + bx^p + c$ is irreducible even when p divides the product. In the case that $p \in \{2, 3, 5, 7, 13\}$, a closer analysis based on the work in [BHV] is possible. Also, the argument we will give implies $x^{2p} + bx^p + c$ is irreducible whenever $b^2 - 4c$ is not a square and c is not a p^{th} power, so examples of reducible $x^{2p} + bx^p + c$ should take this into consideration. Among the more interesting examples of reducible $x^{2p} + bx^p + c$ we found are

$$x^{10} + 2x^5 + 3^5, \quad x^{22} + 67x^{11} + 2^{11}, \quad x^{22} + 394x^{11} + 3^{11}, \quad \text{and} \quad x^{34} + 101x^{17} + 2^{17}.$$

The factorization of trinomials has been considered in great detail by Schinzel [Sc2, Sc3, Sc4]. In particular, Lemma 28 in [Sc2] gives a necessary and sufficient condition for the reducibility over any field K with characteristic different from 2 of the more general trinomial $x^{2m} + bx^m + c$, where m is a positive integer. This more general trinomial is reducible over K if and only if $b^2 - 4c$ is a square in K or there is a prime p dividing m with $x^{2p} + bx^p + c$ reducible over K or 4 divides m and $x^8 + bx^4 + c$ is reducible over K. The conditions (ii), (iii) and (iv) for the reducibility of $x^{2p} + bx^p + c$ above follow from taking $v = 1, 1/2$ and $1/3$, respectively, in (30) of Lemma 28 in [Sc2].

Theorem 1 implies that if $b^2 - 4c$ is not a square and p is sufficiently large depending on b, then $t_p(x)$ is irreducible. This follows also from Theorem 10 in [Sc2]. To see this, note that a theorem of Capelli implies that if $b^2 - 4c$ is not a square and $t_p(x)$ is reducible, then it has an irreducible quadratic factor. By taking $d = 2$ in Theorem 10 of [Sc2], one obtains that there are effective constants c_0 and c_1 such that if $b^2 - 4c$ is not a square and $t_p(x)$ is reducible, then $p < \max\{c_0, c_1 \log |b|\}$. This result is sometimes stronger and sometimes weaker than the condition implied by Theorem 1, depending on the prime factorization of b.

In the third and final section of this paper, we return to the more specific trinomials $x^{2p} + x^p + m^p$ and establish their irreducibility as a consequence of the following Diophantine result.

Theorem 2. *The equation*

$$\frac{ax^{n+2\ell} - 1}{ax^n - 1} = y^2,$$

holds for some positive integers a, x, n, and ℓ with $x > 1$ and some rational number y if and only if

$$2|\ell, \quad a = \frac{3^{\ell-1}+1}{4}, \quad x = 3, \quad n = 1 \quad \text{and} \quad y = \pm(3^\ell + 2).$$

We end the last section by establishing the following related result which is a fairly direct consequence of work of Bennett [Be].

Theorem 3. *Let $m \geq 3$, and consider the Diophantine equation*

$$\frac{ax^r - 1}{ax^n - 1} = y^m. \tag{1}$$

Suppose r and n are integers with $r > n > 0$. Then there are no solutions to (1) in integers a, x, and y with $a > 0$ and $x > 1$ if also $x^{r-n} = z^m$ for some integer z.

To clarify a connection with Theorem 2, observe that if x is an integer and $m|(r-n)$, then one has that $x^{r-n} = z^m$ for some integer z. Note, however, that y is restricted to being an integer in Theorem 3 and only restricted to being a rational number in Theorem 2.

2 The Irreducibility of More General Trinomials

In this section, we discuss the irreducibility of the trinomials $ax^{2p} + bx^p + c \in \mathbb{Z}[x]$, where p is a prime and a, b, and c are integers with $abc \neq 0$. One can multiply the trinomial by a^{2p-1}, and replace x by x/a, obtaining a monic trinomial. So, we assume throughout that $a = 1$. Our interest then is in the irreducibility of the trinomial $t_p(x) = x^{2p} + bx^p + c$.

Our approaches in this paper take advantage of recent work of Bilu, Hanrot, and Voutier [BHV]. A Lucas pair (α, β) is a pair of algebraic integers for which $\alpha\beta$ and $\alpha+\beta$ are nonzero coprime rational integers and α/β is not a root of unity. A Lehmer pair (α, β) is a pair of algebraic integers for which $\alpha\beta$ and $(\alpha+\beta)^2$ are nonzero coprime rational integers and α/β is not a root of unity. The Lucas numbers u_n and Lehmer numbers $\tilde{u}_n$ are defined for nonnegative integers n by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

and

$$\tilde{u}_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \equiv 1 \pmod 2 \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \equiv 0 \pmod 2, \end{cases}$$

respectively. A prime p is called a primitive divisor of u_n provided that p divides u_n and p does not divide $(\alpha-\beta)^2 u_1 u_2 \cdots u_{n-1}$. A prime p is called a primitive divisor of $\tilde{u}_n$ if p divides $\tilde{u}_n$ and p does not divide $(\alpha^2-\beta^2)^2 \tilde{u}_1 \tilde{u}_2 \cdots \tilde{u}_{n-1}$. The work of Bilu, Hanrot, and Voutier [BHV] settles a long-standing problem of classifying all cases of α, β, and n where a primitive divisor of u_n or a primitive divisor of $\tilde{u}_n$ does not exist. Two consequences of their work that we will make use of here are as follows. In the next section, we will use

Result 1. *For odd $n \geq 5$, a Lehmer number $\tilde{u}_n$ defined from a Lehmer pair of the form*

$$(\alpha, \beta) = (\sqrt{a} + \sqrt{a+1}, \sqrt{a} - \sqrt{a+1})$$

for some rational integer a has a primitive prime divisor.

In the current section, we will make use of

Result 2. *If $p \notin \{2, 3, 5, 7, 13\}$ and p is a prime, then each of u_{2p} and $\tilde{u}_p$ contains at least one primitive prime divisor.*

Both of these follow from Theorem C, Theorem 1.3, and Theorem 1.4 in [BHV]. Also, it follows from (3), Proposition 2.1 (i) and Corollary 2.2 all from [BHV], that if p is an odd prime, then every primitive prime divisor q of u_{2p} or $\tilde{u}_p$ satisfies p divides $(q-1)(q+1)$.

We are ready to prove Theorem 1. We consider p not dividing the product appearing in the theorem. In particular, $p \notin \{2, 3, 5, 7, 13\}$. Let $\gamma = (-b + \sqrt{N})/2$, where $N = b^2 - 4c$, and let λ be a p^{th} root of γ. Note that λ is a root of $t_p(x)$. Also, the conditions in Theorem 1 imply that N is not a square. By a theorem of Capelli (see [Sc1] or [Sc2] or, for an alternative to Capelli's theorem, see the proof of Lemma 8 in [FLSU]), it suffices to show that γ is not a p^{th} power in $\mathbb{Q}(\sqrt{N})$. Assume otherwise. Then

$$\alpha^p = \frac{-b + \sqrt{N}}{2} \quad \text{and} \quad \beta^p = \frac{-b - \sqrt{N}}{2}$$

for some distinct α and β in $\mathbb{Q}(\sqrt{N})$ with $\alpha\beta$ and $\alpha + \beta$ in $\mathbb{Z}$ satisfying $(\alpha\beta)^p = c$ and $\alpha + \beta$ divides b. In particular, c is a p^{th} power. Our goal is to show that under the conditions of the theorem, we obtain a contradiction.

We claim that α/β is not a root of unity. Assume otherwise. Since $b^2 - 4c$ is not a square,

$$(\alpha/\beta)^p = \frac{-b + \sqrt{N}}{-b - \sqrt{N}} = \frac{b^2 + N - 2b\sqrt{N}}{b^2 - N} = \frac{b^2 - 2c - b\sqrt{b^2 - 4c}}{2c}$$

is a quadratic irrational that is a root of unity. It follows that the last expression above is one of the six numbers $\pm\mathrm{i}$, $(\pm 1 \pm \sqrt{-3})/2$. Hence, $b^2 - 2c \in \{0, \pm c\}$, so that $c \in \{b^2, b^2/2, b^2/3\}$. One checks that c being a p^{th} power now implies that one of the conditions in (ii), (iii), or (iv) holds, contrary to our conditions on b and c. Thus, α/β is not a root of unity.

We consider two cases depending on whether the rational integers $\alpha\beta$ and $\alpha + \beta$ are relatively prime. First, suppose that they are. Consider the Lucas number

$$u_{2p} = \frac{\alpha^{2p} - \beta^{2p}}{\alpha - \beta} = \frac{\alpha^p - \beta^p}{\alpha - \beta} \cdot (\alpha^p + \beta^p) = \frac{\alpha^p - \beta^p}{\alpha - \beta} \cdot (-b).$$

As $p \notin \{2, 3, 5, 7, 13\}$, we deduce from Result 2 that u_{2p} has a primitive prime divisor q dividing b. As then p divides $(q-1)(q+1)$ and $q|b$, we obtain a contradiction.

Now, suppose that $s = \alpha\beta$ and $r = \alpha + \beta$ are not coprime. Note that α and β are roots of $x^2 - rx + s$. Let $d = \gcd(r^2, s)$, and set

$$\alpha' = \frac{\alpha}{d^{1/2}}, \quad \text{and} \quad \beta' = -\frac{\beta}{d^{1/2}}.$$

Then

$$s' = \alpha'\beta' = -\frac{s}{d} \quad \text{and} \quad r' = (\alpha' + \beta')^2 = \frac{r^2 - 4s}{d}$$

are rational coprime integers. Observe that $\alpha^p - \beta^p = \sqrt{N}$ is nonzero so that $\alpha - \beta \neq 0$. Hence, $r^2 - 2s = (\alpha - \beta)^2 \neq 0$. Therefore, r' and s' are also nonzero. As $\alpha'/\beta' = -\alpha/\beta$, we furthermore have that α'/β' is not a root of unity. Thus, (α', β') is a Lehmer pair. Observe that

$$d^{(p-1)/2}(\alpha + \beta)\tilde{u}_p = d^{(p-1)/2}(\alpha + \beta) \cdot \frac{(\alpha')^p - (\beta')^p}{\alpha' - \beta'} = \alpha^p + \beta^p = -b.$$

It follows that the Lehmer number $\tilde{u}_p$ divides b. As before, we obtain a contradiction as $\tilde{u}_p$ must have a primitive prime divisor q dividing b for which p divides $(q-1)(q+1)$.

The reduction going from Lucas numbers to Lehmer numbers at the end of the argument above is not new. The idea is used, for example, by Shorey and Tijdeman [ST, see Lemma A.10].

3 A Ljunggren-Type Diophantine Equation

In the previous section, we established an irreducibility result for $ax^{2p} + bx^p + c \in \mathbb{Z}[x]$, partially generalizing our earlier demonstration in [FLSU] of the irreducibility of the trinomial $p_m(x) = x^{2p} + x^p + m^p$ where $m \geq 2$. Our consideration of the more general trinomial in the last section required some restrictions on the primes leading to irreducibility. However, it did present an alternative approach to dealing with the irreducibility of $p_m(x)$ as well as a more general class of similar polynomials. In this section, we present yet another approach which associates the irreducibility of $p_m(x)$ with a certain Diophantine equation. We will make use of Result 1 of the previous section.

We consider p to be an odd prime and $m \geq 2$ an integer. As in the beginning of the proof of Theorem 1, if $p_m(x)$ is reducible, then there are α and β in $\mathbb{Q}(\sqrt{N})$, where $N = 1 - 4m^p$, that are roots of the quadratic $x^2 \pm x + m$. The discriminant of the quadratic is $D = 1 - 4m < 0$ and, hence, not a square. We deduce that $\mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{D})$. This equality can hold if and only if there is a rational number $x \in \mathbb{Q}$ such that

$$\frac{4m^p - 1}{4m - 1} = x^2.$$

Thus, the irreducibility of $p_m(x)$ follows as a consequence of Theorem 2.

A solution to the equation

$$\frac{ax^{n+2\ell} - 1}{ax^n - 1} = y^2$$

implies that there exist positive integers u and v satisfying

$$ax^n - 1 = du^2 \quad \text{and} \quad ax^{n+2\ell} - 1 = dv^2,$$

where d is a positive squarefree integer dividing $\gcd(ax^{n+2\ell} - 1, ax^n - 1)$. We then have the equation

$$ax^n(x^\ell)^2 - dv^2 = 1.$$

Therefore,

$$(du^2+1)(x^\ell)^2 - dv^2 = 1.$$

Let $A = ax^n = du^2+1$ and $B = d$, and let (X_1, Y_1) be the minimal solution in positive integers to the Pell equation

$$AX^2 - BY^2 = 1. \tag{2}$$

Define

$$\alpha_0 = X_1\sqrt{A} + Y_1\sqrt{B} \quad \text{and} \quad \beta_0 = X_1\sqrt{A} - Y_1\sqrt{B}. \tag{3}$$

It is well-known (see [Wal]), that if $A \neq 1$ and A and B are positive integers with at least one of A and B not a square, then all the positive integer solutions of (2) are of the form

$$(X, Y) = (X_t, Y_t),$$

for some odd integer $t \geq 1$, where

$$(X_t, Y_t) = \Big(\frac{\alpha_0^t + \beta_0^t}{\alpha_0 + \beta_0}X_1, \frac{\alpha_0^t - \beta_0^t}{\alpha_0 - \beta_0}Y_1\Big).$$

We now use this description of the solutions to (2). Observe first that $A > 1$. Also, d is squarefree so that $B = d$ is not a square unless $d = 1$. In that case, $A = u^2+1$ cannot be a square (as both A and $A-1$ would be consecutive positive integral squares, which is impossible). Hence, at least one of A and B is not a square. It is not difficult to see that $(1, u)$ is the minimal solution to (2) with A and B as above (both X and Y are larger for any other solution in positive integers to (2)); thus, $X_1 = 1$, and $Y_1 = u$. We deduce that there is an odd positive integer t for which

$$\begin{aligned} x^\ell = X_t &= \frac{(\sqrt{du^2+1} + u\sqrt{d})^t + (\sqrt{du^2+1} - u\sqrt{d})^t}{2\sqrt{du^2+1}} \\ &= \frac{(\sqrt{ax^n} + \sqrt{ax^n-1})^t + (\sqrt{ax^n} - \sqrt{ax^n-1})^t}{2\sqrt{ax^n}}. \end{aligned} \tag{4}$$

As $x > 1$ and $\ell > 0$, we must have $t > 1$.

Fix $\alpha = \alpha_0$ and $\beta = -\beta_0$. Observe that $\alpha\beta = -1$ and $(\alpha+\beta)^2 = 4(ax^n - 1)$ are relatively prime nonzero rational integers. One checks that α/β is a real number less than -1, so clearly α/β is not a root of unity. Thus, (α, β) is a Lehmer pair. As t is odd, (4) implies $x^\ell = \tilde{u}_t$, a Lehmer number as defined in the previous section. We show that $t = 3$. Assume $t \geq 5$. By Result 1, $\tilde{u}_t$ must have a primitive prime divisor. On the other hand, $x|(\alpha^2 - \beta^2)^2$. By the definition of being a primitive prime divisor of a Lehmer number, $\tilde{u}_t$ in fact has no primitive prime divisor. We obtain a contradiction; hence, $t = 3$.

Using the binomial theorem in (4) and reducing modulo x we get

$$0 \equiv t \cdot (ax^n - 1)^{(t-1)/2} \pmod{x}.$$

Hence, $x|t$. As $x > 1$ and $t = 3$, we deduce $x = 3$. Substituting $t = 3$ into (4), we obtain

$$x^\ell = ax^n + 3(ax^n - 1) = 4ax^n - 3.$$

Therefore, $3^\ell = 4a3^n - 3$. Working modulo 4, we see that $\ell \neq 1$. It follows that $\ell > 1$ and, hence, $n = 1$. We obtain $3^{\ell-1} = 4a - 1$ from which we deduce $a = (3^{\ell-1}+1)/4$. As $3^{\ell-1}+1$ is divisible by 4, we get $2|\ell$. Rewriting the equation in the statement of the theorem, we have

$$y^2 = \frac{3^{3\ell} + 3^{2\ell+1} - 4}{3^\ell - 1} = (3^\ell + 2)^2.$$

The theorem follows.

We note that Ljunggren [Lj] previously solved the case of $a = 1$ and $n = 1$ of Proposition 2. A related result with y integral can also be obtained from the following nice theorem of Bennett [Be].

> *If a, b and m are integers with $ab \neq 0$ and $m \geq 3$, then the equation $|ax^m - by^m| = 1$ has at most one solution in positive integers (x, y).*

We now prove Theorem 3.

Assume (1) holds with the variables satisfying the conditions in Theorem 3. In particular, the numerator and denominator on the left side of (1) are positive. Thus, if m is odd, then $y > 0$; furthermore, in the case that m is even, we may suppose $y > 0$ (by replacing y with $-y$ if necessary). Also, as $x > 0$, we may take $z > 0$. Rewriting (1), we have

$$ax^n z^m - (ax^n - 1)y^m = 1. \tag{5}$$

Therefore, (z, y) is a solution of the Diophantine equation

$$AX^m - BY^m = 1, \tag{6}$$

where $A = ax^n$ and $B = ax^n - 1$. But $(1, 1)$ is also a solution of the above equation. Observe that the conditions $x > 1$ and $x^{r-n} = z^m$ imply $z \neq 1$. In particular, $(z, y) \neq (1, 1)$. By Bennett's theorem, we obtain a contradiction.

References

[Be] M. Bennett, *Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$*, J. Reine Angew. Math. **535** (2001), 1–49.

[BHV] Y. Bilu, G. Hanrot, P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte)*, J. Reine Angew. Math. **539** (2001), 75–122.

[FLSU] M. Filaseta, F. Luca, P. Stănică, R.G. Underwood, *On Galois groups of some polynomials arising from circulant matrices*, Journal of Number Theory, to appear.

[Le] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$*, Nouv. Ann. Math. **9** (1850), 178–181.

[Lj] W. Ljunggren, *Some theorems on indeterminate equations of the form $(x^n - 1)/(x - 1) = y^q$*, Norsk Mat. Tidsskr. **25** (1943), 17–20.

[Sc1] A. Schinzel, Selected Topics on Polynomials, Univ. of Michigan Press, Ann Arbor, 1982.

[Sc2] A. Schinzel, *On reducible trinomials*, Dissert. Math. **329** (1993).

[Sc3] A. Schinzel, *On reducible trinomials, II*, Publ. Math. Debrecen 56 (2000), 575–608.

[Sc4] A. Schinzel, *On reducible trinomials, III*, Period. Math. Hungar. 43 (2001), 43–69.

[ST] T. N. Shorey, R. Tijdeman, Exponential Diophantine Equations, Cambridge Univ. Press, Cambridge, 1986.

[Wal] D. T. Walker, *On the Diophantine Equation* $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly **74** (1967), 504–513.