2017

A journey through Galois groups, irreducible polynomials and diophatine equations

Filaseta, M.; Luca, F.; Stnic, P.; Underwood, R.G.

A Journey through Galois Groups, Irreducible Polynomials and Diophantine Equations

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

Computing the Galois group of the splitting field of a given polynomial with integer coefficients over the rationals is a classical problem in modern algebra. A theorem of Van der Waerden [Wae] asserts that almost all (monic) polynomials in $\mathbb{Z}[x]$ have associated Galois group S_n, the symmetric group on n letters. Thus, cases where the associated Galois group is different from S_n are rare. Nevertheless, examples of polynomials where the associated Galois group is not S_n are well-known. For example, the Galois group of the splitting field of the polynomial $x^p - 1$, $p \geq 3$ prime, is cyclic of order $p - 1$. For the polynomial $x^p - 2$, $p \geq 3$, the Galois group is the subgroup of S_p generated by a cycle of length p and a cycle of length $p - 1$. One interest in this paper is to find other collections of polynomials with integer or rational coefficients whose Galois groups are isomorphic to these groups.

Using circulant matrices and determinants, for each prime $p \geq 3$ and positive integer m, we construct a degree p polynomial $f_{p,m}$ in $\mathbb{Q}[x]$ having all real roots. For $m = 1$ and $p \geq 5$, we show that the Galois group of $f_{p,1}$ is cyclic of order $p - 1$. For $m \geq 2$ and $p \geq 5$, the Galois group of $f_{p,m}$ is the subgroup of S_p generated by a cycle of length p and a cycle of length $p - 1$.

It is interesting to note that the polynomials defined with the help of a circulant matrix are connected with Chebyshev (or Dickson) polynomials. This was observed in the course

*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

of proving that a certain trinomial in our investigations is irreducible. A proof of the irreducibility of these trinomials is presented and connections are made to recent work of Bilu, Hanrot, and Voutier [BHV] (with an appendix by Mignotte) on Lucas and Lehmer numbers. The latter leads to two alternative approaches for establishing the irreducibility of our trinomials. For one approach, we solve the Diophantine equation

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

where y is rational and a, x, n, and ℓ are positive integers with $x>1$.

2 Polynomials with Real Roots and Cyclic Galois Groups

Consider the $n\times n$ *circulant matrix*

$$\mathrm{circ}(a_1,a_2,\ldots,a_n)=\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \vdots & & & & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}.$$

The determinant of $\mathrm{circ}(a_1,a_2,\ldots,a_n)$ is given by the formula

$$\det(\mathrm{circ}(a_1,a_2,\ldots,a_n))=\prod_{\mu}\left(a_1+a_2\mu+a_3\mu^2+\cdots+a_n\mu^{n-1}\right), \tag{1}$$

where the product runs over all n of the nth roots of unity.

Let n be ≥ 3, and consider the $n\times n$ circulant matrix $A=\mathrm{circ}(a,b,c,0,\ldots,0)$. In this case, Ore [O] has computed the expansion of (1). Let $\lfloor x\rfloor$ denote the greatest integer less than or equal to x.

Proposition 1 (Ore). *The determinant of A is*

$$\det(A)=a^n+(-1)^{n+1}b^n+c^n-n\sum_{i=1}^{\lfloor n/2\rfloor}(-1)^{n+i}\frac{1}{n-i}\binom{n-i}{i}(ac)^ib^{n-2i}.$$

Corollary 2. *If n is odd, then*

$$\det(A)=a^n+c^n+b^n+\sum_{i=1}^{(n-1)/2}(-1)^i\frac{n}{n-i}\binom{n-i}{i}(ac)^ib^{n-2i}.$$

Take $n=p\geq 3$ prime. We consider a and c satisfying $a^p+c^p=1$ with $m=ac$ a positive integer. It follows that a^p and c^p are the roots of the quadratic $g(x)=x^2-x+m^p$ and, hence, $(1\pm\sqrt{1-4m^p})/2$. We define $f_{p,m}(x)$ to be the determinant of the $p\times p$ circulant matrix $\mathrm{circ}(a,x,c,0,0,\ldots,0)$. Observe that a and c are necessarily algebraic integers (being

roots of $g(x^p)$) so that the coefficients of $f_{p,m}(x)$ are algebraic integers. Also, Corollary 2 implies that

$$f_{p,m}(x) = x^p - \frac{p}{p-1}\binom{p-1}{1} m\, x^{p-2} + \cdots + (-1)^{(p-1)/2} p\, m^{(p-1)/2}\, x + 1$$

so that, in particular, the coefficients of $f_{p,m}$ are rational. We deduce that $f_{p,m} \in \mathbb{Z}[x]$.

Next, we explicitly describe the zeros of $f_{p,m}$.

Proposition 3. *Let $m \geq 1$ be a positive integer, and let p be a prime ≥ 3. Set $\gamma_m = (1 + \sqrt{1 - 4m^p})/2$. The roots of $f_{p,m}$ are precisely the p numbers of the form $-\lambda - \overline{\lambda}$ where λ runs over the p^{th} roots of γ_m.*

Before going to the proof, we note that the p numbers $-\lambda - \overline{\lambda}$ are distinct. This follows, in fact, from the observations that the p choices for λ all lie on the same circle centered at the origin and no two of them are complex conjugates (since they are the p^{th} roots of a non-real complex number).

Proof of Proposition 3. Fix λ as above, and let $\zeta_n = e^{2\pi \mathrm{i}/n}$. Observe that

$$\lambda^p + \overline{\lambda}^p = 1 \qquad \text{and} \qquad \lambda\overline{\lambda} = |\lambda|^2 = |\gamma_m|^{2/p} = m.$$

Thus, $f_{p,m}$ is the determinant of the $p \times p$ circulant matrix $\mathrm{circ}(\lambda, x, \overline{\lambda}, 0, 0, \ldots, 0)$. Using formula (1), $f_{p,m}(x)$ factors as

$$f_{p,m}(x) = \prod_{j=0}^{p-1} (\lambda + x\zeta_p^j + \overline{\lambda}\zeta_p^{2j}).$$

We deduce that $-\lambda - \overline{\lambda}$ is a root of $f_{p,m}$ (consider $j = 0$). Since this is true for an arbitrary λ as in the proposition, the result follows. □

We will not be using it explicitly, but we make the observation that

$$f_{p,m}(x) = 2m^{p/2} T_p(x/(2m^{1/2})) + 1,$$

where $T_p(x)$ is a Chebyshev polynomial of the first kind (see (1.10) and (1.96) in [Ri]). Alternatively, $f_{p,m}(x)$ can also be viewed as being connected to Dickson polynomials with this work being motivated in part by work of Abhyankar, Cohen, and Zieve [ACZ].

Before proceeding, we note that $|\gamma_m| = m^{p/2}$ implies that each root of $f_{p,m}$ is a real number with absolute value $< 2\sqrt{m}$. Furthermore, it is not too difficult to show that as p varies, the roots of $f_{p,m}$ are dense in the interval $[-2\sqrt{m}, 2\sqrt{m}]$.

We specialize to the case when $m = 1$ in the definition of $f_{p,m}$. In this case, the roots of $f_{p,m}$ are in the interval $(-2, 2)$. Also, for $p \geq 5$, -1 is a root of $f_{p,1}$. To see this, observe that

$$\gamma_1 = \big(1 + \mathrm{i}\sqrt{3}\big)/2 = \zeta_6.$$

From Proposition 3, we have that the zeros of $f_{p,1}$ are of the form $-\lambda - \overline{\lambda}$ where λ runs over the p^{th} roots of ζ_6. Observe that $\lambda = \zeta_6^p \in \{\zeta_6, \zeta_6^5\}$ is a p^{th} root of ζ_6. Furthermore, for this λ, we have $-\lambda - \overline{\lambda} = -1$, so -1 is a root of $f_{p,1}$.

A polynomial $f(x) \in \mathbb{Z}[x]$ is called Eisenstein if Eisenstein's criterion applies to a translation of $f(x)$. In particular, Eisenstein polynomials are irreducible over $\mathbb{Q}$.

Proposition 4. *The polynomial $f_{3,1}(x)$ is Eisenstein, and for each $p \geq 5$ the polynomial $f_{p,1}(x)/(x+1)$ is Eisenstein.*

Proof. We have $f_{3,1}(x) = x^3 - 3x + 1$, and one checks that Eisenstein's criterion applies to $f_{3,1}(x+2)$. For $p \geq 5$, define $h_p(x) = f_{p,1}(x)/(x+1)$. Observe that

$$\begin{aligned} h_p(x-1) &= f_{p,1}(x-1)/x \\ &= \frac{1}{x}\left((x-1)^p - \frac{p}{p-1}\binom{p-1}{1}(x-1)^{p-2} + \cdots + (-1)^{(p-1)/2}p(x-1) + 1\right). \end{aligned}$$

We deduce that $h_p(x-1)$ is a monic polynomial in $\mathbb{Z}[x]$ with every coefficient except the leading coefficient divisible by p. To complete the proof, we show that p^2 does not divide the constant term of $h_p(x-1)$. Proposition 3 implies that the roots of $f_{p,1}(x-1)$ are of the form

$$1 - \lambda\zeta_p^j - \overline{\lambda}\zeta_p^{-j} \qquad \text{for } j \in \{0, 1, \ldots, p-1\},$$

where λ is any fixed p^{th} root of $\gamma_1 = \zeta_6$. We consider $\lambda = \zeta_6^p$. Thus, $\lambda - \lambda^2 = 1$, $\lambda^2 = -\overline{\lambda}$, and consequently $1 - \lambda\zeta_p^j - \overline{\lambda}\zeta_p^{-j} = 0$ for $j = 0$. In particular, the root corresponding to $j = 0$ accounts for the factor x in $f_{p,1}(x-1)$. Thus, the constant term in $h_p(x-1)$ is

$$\begin{aligned} \prod_{j=1}^{p-1}\left(1 - \lambda\zeta_p^j - \overline{\lambda}\zeta_p^{-j}\right) &= \prod_{j=1}^{p-1}\left(\lambda\zeta_p^{-j}\left(\lambda + \zeta_p^j\right)\left(1 - \zeta_p^j\right)\right) \\ &= \lambda^{p-1}\prod_{j=1}^{p-1}\left(\lambda + \zeta_p^j\right)\prod_{j=1}^{p-1}\left(1 - \zeta_p^j\right). \end{aligned}$$

Using $\Phi_m(x)$ to denote the m^{th} cyclotomic polynomial, the last product above is simply $\Phi_p(1) = p$. We also use that $\Phi_{3p}(1) = 1$ (indeed, $\Phi_m(1) = 1$ whenever m is not a prime power). From $\lambda = \zeta_6^p = -\zeta_3^{2p}$, we obtain

$$\lambda + \zeta_p^j = \lambda\left(1 - \zeta_{3p}^{3j-2p^2}\right)$$

and $3j - 2p^2$ is relatively prime to $3p$ for $1 \leq j \leq p-1$. As

$$1 = \Phi_{3p}(1) = \prod_{\substack{1 \leq j \leq 3p-1 \\ \gcd(j,3p)=1}}\left(1 - \zeta_{3p}^j\right),$$

each $\lambda + \zeta_p^j$ for $1 \leq j \leq p-1$ is λ times a unit in $\mathbb{Z}[\zeta_{3p}]$. Also, λ is a unit in $\mathbb{Z}[\zeta_{3p}]$. It follows that the constant term of $h_p(x-1)$ is a unit in $\mathbb{Z}[\zeta_{3p}]$ times p. Since it is also in $\mathbb{Z}$, we deduce that the constant term is $\pm p$, concluding the proof. □

As indicated earlier, Proposition 4 implies that the polynomials considered there are irreducible over $\mathbb{Q}$. There are alternative approaches to establishing the irreducibility of these polynomials. We describe such a method next which also provides us some additional information, in particular about the polynomials' associated Galois groups.

Observe that if λ is as in Proposition 3 with $m = 1$, then $-\lambda$ is a p^{th} root of ζ_3^2 and, hence, a $(3p)^{\text{th}}$ root of unity. For $p = 3$, these p^{th} roots of ζ_3^2 are *primitive* $(3p)^{\text{th}}$ roots of unity. For $p \geq 5$, one can check directly that ζ_3^{2p} is the only p^{th} root of ζ_3^2 which is not a primitive $(3p)^{\text{th}}$ root of unity. We deduce from Proposition 3 that the splitting field K of $f_{p,1}$ over $\mathbb{Q}$ is precisely the maximal real subfield of $\mathbb{Q}(\zeta_{3p})$. The degree of this extension is $\phi(9)/2 = 3$ in the case of $p = 3$ and is $\phi(3p)/2 = p - 1$ for $p \geq 5$. The irreducibility of the polynomials $f_{3,1}(x)$ and $f_{p,1}(x)/(x+1)$ for $p \geq 5$ follows. Note that the Galois group of the maximal real subfield of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}$ is cyclic. This gives us the following result.

Proposition 5. *Let $p \geq 3$ be prime. Let K be a splitting field of $f_{p,1}(x)$ over $\mathbb{Q}$. If $p = 3$, then the Galois group of $K/\mathbb{Q}$ is cyclic of order 3. If $p \geq 5$, then the Galois group of $K/\mathbb{Q}$ is cyclic of order $p - 1$.*

It is of some interest to describe a generator for these Galois groups. If λ is a p^{th} root of $\zeta_6 = -\zeta_3^2$, then Proposition 3 and

$$(-\lambda - \overline{\lambda})^2 = \lambda^2 + 2 + \overline{\lambda}^2$$

imply that $\sigma(x) = 2 - x^2$ is an automorphism of K over $\mathbb{Q}$. For $p = 3$, one can check directly that σ generates the Galois group of K over $\mathbb{Q}$. For $p \geq 5$, the automorphism σ may or may not generate the Galois group. In particular, if the order of 2 modulo p is even and $< p - 1$, then σ will not be a generator for the Galois group (for example, consider $p = 17$ or $p = 41$). To obtain an automorphism that generates the Galois group for all $p \geq 5$, for each $j \in \{1, 2, \ldots, p-1\}$, we consider an integer $k = k(j)$ satisfying $k \equiv 1 \pmod 3$ and $k \equiv j \pmod p$. The automorphism σ_j of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}$ defined by $\sigma_j(\zeta_{3p}) = \zeta_{3p}^k$ has the property that $\sigma_j(\zeta_3) = \zeta_3$ and $\sigma_j(\zeta_p) = \zeta_p^j$. In other words, the $p - 1$ different σ_j are precisely the automorphisms of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}(\zeta_3)$. We now consider a primitive root g modulo p and fix $\lambda = -\zeta_3^{2p}$. Define $\sigma_g^{(t)}$ to be the composition of t copies of σ_g. Then

$$\sigma_g^{(t)}\big(-\lambda\zeta_p - \overline{\lambda}\zeta_p^{-1}\big) = -\lambda\zeta_p^{g^t} - \overline{\lambda}\zeta_p^{-g^t}.$$

We deduce from Proposition 3 that the restriction of σ_g to K, the maximal real subfield of $\mathbb{Q}(\zeta_{3p})$, is a generator for the Galois group of K over $\mathbb{Q}$.

The above explicit construction of the generator leads naturally to a further conclusion.

Proposition 6. *The polynomial $f_{3,1}(x)$ and the polynomials $f_{p,1}(x)/(x+1)$, for $p \geq 5$, are irreducible over $\mathbb{Q}(\zeta_3)$.*

One checks the above result directly for $p = 3$. For $p \geq 5$, we use that for $2 \leq j \leq p - 1$, the roots of $f_{p,1}(x)/(x+1)$ are images of the root $-\lambda\zeta_p - \overline{\lambda}\zeta_p^{-1}$ under applications of the automorphism σ_g of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}(\zeta_3)$. Since this automorphism fixes the elements of $\mathbb{Q}(\zeta_3)$, the above result follows. The result for $p \geq 5$ also follows from the proof of Proposition 4 (from the fact that $f_{p,1}(x)/(x+1)$ is Eisenstein with respect to a prime which does not ramify in $\mathbb{Q}(\zeta_3)$).

3 The Galois Groups of General $f_{p,m}$

For p a prime ≥ 5 and m an integer ≥ 2, we establish the irreducibility of $f_{p,m}$ over the rationals and compute the Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$. Multiplying the relation $\lambda^p + \overline{\lambda}^p = 1$ of Proposition 3 by λ^p shows that the roots of $f_{p,m}$ are associated with the roots of $p_m(x) = x^{2p} - x^p + m^p$. Our investigations here begin with a closer look at the polynomials $p_m(x)$.

Proposition 7. *Let p be an odd prime and let m be an integer with $m \geq 2$. Then the polynomials $x^{2p} + x^p + m^p$ and $x^{2p} - x^p + m^p$ are irreducible.*

Proof. We prove the result only for the polynomial $p_m(x) = x^{2p} - x^p + m^p$, the remaining case following as $p_m(-x) = x^{2p} + x^p + m^p$. Let $N = 1 - 4m^p$ and $\gamma = (1 + \sqrt{N})/2$. Thus, $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{D})$, where $D < 0$ is a squarefree integer, $D|N$, and N/D is a square. Let λ be a p^{th} root of γ. Thus, λ is a root of $p_m(x)$. We show that $x^p - \gamma$ is irreducible over $\mathbb{Q}(\gamma)$. This will imply $[\mathbb{Q}(\lambda) : \mathbb{Q}(\gamma)] = p$. Since $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2$, we deduce $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2p$ and, hence, that $p_m(x)$ is irreducible.

Assume $x^p - \gamma = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Q}(\gamma)[x]$ with $r = \deg g \in [1, p-1]$. Since the p roots of $x^p - \gamma$ are of the form $\zeta^j\lambda$, where $\zeta = \zeta_p$ and $j \in \{0, 1, \ldots, p-1\}$, we deduce that the constant term of $g(x)$ is of the form $\pm\zeta^k\lambda^r$. Thus, $\zeta^k\lambda^r \in \mathbb{Q}(\gamma)$. Let x and y be integers satisfying $rx + py = 1$. Since $\gamma = \lambda^p$, we deduce

$$\left(\zeta^k\lambda^r\right)^x\gamma^y = \zeta^{kx}\lambda^{rx+py} = \zeta^{kx}\lambda \in \mathbb{Q}(\gamma).$$

Setting $\alpha = \zeta^{kx}\lambda$, we see that α is an algebraic integer in $\mathbb{Q}(\sqrt{N})$ and

$$\alpha^p = \frac{1 + \sqrt{1 - 4m^p}}{2} = \frac{1 + \sqrt{N}}{2}. \tag{2}$$

Observe that α is a root of $x^{2p} - x^p + m^p$. Let β be the conjugate of α. Then

$$\beta^p = \frac{1 - \sqrt{N}}{2}.$$

Since $\alpha\beta$ is a real number satisfying $(\alpha\beta)^p = m^p$, we have $\alpha\beta = m$. Next, we determine $\alpha + \beta$. Note that

$$1 = \alpha^p + \beta^p = (\alpha + \beta)\left(\alpha^{p-1} - \alpha^{p-2}\beta + \cdots - \alpha\beta^{p-2} + \beta^{p-1}\right).$$

Each one of the two factors on the right is an algebraic integer expressed as a symmetric function of α and β. Hence, each of these factors must be a rational integer. We deduce that $\alpha + \beta = \pm 1$. We justify that $\alpha + \beta = 1$. Writing $\alpha = (a + b\sqrt{D})/2$, it suffices to show that $a \neq -1$ (i.e., that $\alpha + \beta \neq -1$). Observe that

$$2^{p-1} + 2^{p-1}\sqrt{N} = 2^p\alpha^p = (a + b\sqrt{D})^p = A + B\sqrt{D},$$

where $A \equiv a^p \pmod{p}$. Hence,

$$a^p \equiv 2^{p-1} \equiv 1 \pmod{p}.$$

As p is odd, $a \neq -1$. Thus, $\alpha + \beta = 1$. It follows that α and β are both roots of $x^2 - x + m$.

Writing $\alpha = se^{\mathrm{i}\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$, we have $\beta = se^{-\mathrm{i}\theta}$ and $\cos\theta = 1/(2\sqrt{m})$. On the other hand, (2) and $\alpha^p = s^p e^{\mathrm{i}p\theta}$ imply $\cos(p\theta) = 1/(2m^{p/2})$. Using that $\cos(p\theta) = T_p(\cos\theta)$, where T_p is the p^{th} Chebyshev polynomial, we get that

$$\cos(p\theta) = 2^{p-1}(\cos\theta)^p - 2^{p-3}p(\cos\theta)^{p-2} + \cdots, \tag{3}$$

where what remains on the right is a sum of smaller odd powers of $\cos\theta$ times p times rational integers (see, for example, (1.10) and (1.96) in [Ri]). Furthermore, the coefficient of each term $(\cos\theta)^j$ on the right is divisible by 2^{j-1} (an immediate consequence of Exercise 1.4.45 in [Ri]). Given that $\cos\theta = 1/(2\sqrt{m})$ and $\cos(p\theta) = 1/(2m^{p/2})$, we see that the expression on the left of (3) equals the first term on the right of (3). Thus, the remaining terms on the right must sum to zero. After factoring out the common factor of $p\cos\theta$ in each term and multiplying through by -1, we deduce $w_1(\cos^2\theta) = 0$ where $w_1(x) \in \mathbb{Z}[x]$ and $\deg w_1(x) = (p-3)/2$. Further, the leading coefficient of $w_1(x)$ is 2^{p-3} and 2^{2j} divides the coefficient of x^j for each j. We deduce that $w_2(x) = w_1(x/4)$ is a monic polynomial with integer coefficients that has $4\cos^2\theta$ as a root. Since rational roots of monic polynomials with integer coefficients are rational integers and since $4\cos^2\theta = 1/m$, we obtain a contradiction to $m \geq 2$. □

Before continuing, we note that one can replace the argument leading to (2) by an application of Capelli's theorem (see [Sc1] and Lemma 28 of [Sc2]). The second part of the argument above (as well as the end of our next proof) is similar to an approach of Lebesgue [Le].

As in the proof of Proposition 7, we set $\gamma = (1 + \sqrt{1 - 4m^p})/2$ and fix λ to be a p^{th} root of γ. By Proposition 7, we have $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2p$. We consider the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$ which is irreducible over $\mathbb{Q}$. We show that it is also irreducible over $\mathbb{Q}(\lambda)$.

Proposition 8. *Let p be a prime ≥ 5, and let m be an integer ≥ 2. Then $\Phi_p(x)$ is irreducible over $\mathbb{Q}(\lambda)$.*

Proof. By way of contradiction, assume $\Phi_p(x)$ is reducible over $\mathbb{Q}(\lambda)$. Then $\mathbb{Q}(\zeta)$ contains a subfield of $\mathbb{Q}(\lambda)$ of degree 2, p or $2p$ over $\mathbb{Q}$. The latter two are not possible since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$. Thus, $\mathbb{Q}(\zeta)$ contains $\mathbb{Q}(\gamma)$ which is the subfield of $\mathbb{Q}(\lambda)$ of degree 2 over $\mathbb{Q}$. Recall that the quadratic subfield in $\mathbb{Q}(\zeta)$ is $\mathbb{Q}\big(\sqrt{(-1)^{(p-1)/2}p}\big)$. Thus, $\mathbb{Q}(\gamma) = \mathbb{Q}\big(\sqrt{(-1)^{(p-1)/2}p}\big)$. Since γ is imaginary, the quadratic field $\mathbb{Q}\big(\sqrt{(-1)^{(p-1)/2}p}\big)$ must contain imaginary numbers. We deduce that $p \equiv 3 \pmod 4$. Since $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{1-4m^p})$, the equality of $\mathbb{Q}(\gamma)$ and $\mathbb{Q}(\sqrt{-p})$ implies that there is a solution to the Diophantine equation

$$px^2 = 4m^p - 1,$$

where m is an integer ≥ 2, p is a prime $\equiv 3 \pmod 4$ that is ≥ 5, and x is an integer. We conclude the proof by showing that this is impossible.

The Diophantine equation leads to

$$\frac{1 + x\sqrt{-p}}{2} \cdot \frac{1 - x\sqrt{-p}}{2} = m^p.$$

Let $\omega = (1 + x\sqrt{-p})/2$, and let $\overline{\omega}$ be its conjugate. We work in the ring of algebraic integers in $\mathbb{Q}(\sqrt{-p})$. Since $\omega + \overline{\omega} = 1$, the principal ideals (ω) and $(\overline{\omega})$ are coprime. Therefore, each of these ideals is a p^{th} power of some ideal. Let A be an ideal for which $(\omega) = A^p$. The class number h of $\mathbb{Q}(\sqrt{-p})$ is less than p (see, for example, [BS]) and, hence, not divisible by p. Thus, there is an integer p' such that $pp' \equiv 1 \pmod{h}$. We deduce the fractional ideal equation

$$\left(\omega^{p'}\right) = (\omega)^{p'} = A^{pp'} = A(\beta),$$

for some $\beta \in \mathbb{Q}(\sqrt{-p})$. It follows that $\beta' = \omega^{p'}/\beta$ is an algebraic integer in $\mathbb{Q}(\sqrt{-p})$ and that $A = (\beta')$. Since $(\omega) = (\beta')^p$ and since the only units in the ring of algebraic integers in $\mathbb{Q}(\sqrt{-p})$ are ± 1, we obtain $(1 + x\sqrt{-p})/2 = \alpha^p$ where either $\alpha = \beta'$ or $\alpha = -\beta'$.

Let a and b be integers, necessarily of the same parity, such that $\alpha = (a + b\sqrt{-p})/2$. Comparing real parts of the equation $(1 + x\sqrt{-p})/2 = \alpha^p$, we deduce

$$2^{p-1} = a^p - \binom{p}{2} p a^{p-2} b^2 + \binom{p}{4} p^2 a^{p-4} b^4 - \cdots - \binom{p}{p-1} p^{(p-1)/2} a b^{p-1}. \tag{4}$$

As a and b have the same parity, if a is even, then b is even and the right-hand side of (4) is divisible by 2^p. As the left-hand side is not divisible by 2^p, we deduce that a and b are odd. Since a divides the right-hand side of (4), a divides 2^{p-1} so that $a = \pm 1$. Also, (4) implies $a^p \equiv 2^{p-1} \equiv 1 \pmod{p}$. Therefore, $a = 1$. Clearly, $b \neq 0$. We complete the proof by showing that with $a = 1$, (4) has no solutions in nonzero integers b.

Assume (4) has a solution with p a prime ≥ 5, $a = 1$ and b a nonzero integer. The right-hand side of (4) corresponds to the real part of $(2\alpha)^p$ where $\alpha = (a + b\sqrt{-p})/2 = (1 + b\sqrt{-p})/2$. It follows that

$$2^p = (1 + b\sqrt{-p})^p + (1 - b\sqrt{-p})^p.$$

We divide each term in this equation by $(1 + b^2 p)^{p/2}$. With θ satisfying

$$\cos\theta = \frac{1}{\sqrt{1 + b^2 p}} \quad \text{and} \quad \sin\theta = \frac{b\sqrt{p}}{\sqrt{1 + b^2 p}},$$

we deduce

$$\frac{2^p}{(1 + b^2 p)^{p/2}} = (\cos\theta + \mathrm{i}\sin\theta)^p + (\cos\theta - \mathrm{i}\sin\theta)^p = e^{\mathrm{i}p\theta} + e^{-\mathrm{i}p\theta} = 2\cos(p\theta).$$

Thus,

$$\cos(p\theta) = \frac{2^{p-1}}{(1 + b^2 p)^{p/2}}.$$

With p and θ as above, we appeal to (3) and follow the argument after (3) in the proof of Proposition 7. We deduce that $4\cos^2\theta = 4/(1 + b^2 p)$ is a rational integer. Since $b \neq 0$ and $p \geq 5$, this is a contradiction. □

Proposition 9. *If p is a prime ≥ 5 and m an integer ≥ 2, then $f_{p,m}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By Proposition 7, the polynomial $p_m(x) = x^{2p} - x^p + m^p$ is irreducible. We show now that we have the identity

$$-x^p f_{p,m}\left(-x - \frac{m}{x}\right) = p_m(x). \tag{5}$$

Both polynomials are monic and have the same degree, namely $2p$. Therefore it suffices to show that the roots of p_m are also roots of $-x^p f_{p,m}\left(-x - \frac{m}{x}\right)$. Take a root $\lambda\zeta^j$ of p_m where $\zeta = \zeta_p$ and $\lambda = \gamma^{1/p}$ denotes an arbitrary p^{th} root of $(1 + \sqrt{1 - 4m^p})/2$. Note that $m\lambda^{-1}\zeta^{-j}$ is the conjugate of $\lambda\zeta^j$. Proposition 3 implies

$$-\lambda^p \zeta^{pj} f_{p,m}(-\lambda\zeta^j - m\lambda^{-1}\zeta^{-j}) = 0.$$

Thus, $\lambda\zeta^j$ is a root of the left-hand side of (5). Since $\lambda\zeta^j$ is a root of the left-hand side of (5) if and only if its conjugate $m\lambda^{-1}\zeta^{-j}$ is, (5) follows.

Now, assume that there exist two polynomials f_1 and f_2 in $\mathbb{Q}[x]$ of degrees d_1 and d_2, respectively, such that each $d_j < p$ and

$$f_{p,m}(x) = f_1(x) f_2(x).$$

It follows that

$$x^p f_{p,m}\left(x + \frac{m}{x}\right) = x^p f_1\left(x + \frac{m}{x}\right) f_2\left(x + \frac{m}{x}\right).$$

Since $p = d_1 + d_2$, each

$$x^{d_j} f_j\left(x + \frac{m}{x}\right)$$

is a nonconstant polynomial in $\mathbb{Z}[x]$ dividing $p_m(-x)$ of degree $< 2p$. This contradicts the fact that $p_m(x)$ is irreducible, and the result follows. □

Let γ, λ and ζ be as above. Since $f_{p,m}$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\lambda + \overline{\lambda}) : \mathbb{Q}] = p$. Also, $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = (p-1)/2$. Hence,

$$[\mathbb{Q}(\lambda + \overline{\lambda}, \zeta + \zeta^{-1}) : \mathbb{Q}] = p(p-1)/2. \tag{6}$$

Observe that $-\lambda\zeta - \overline{\lambda}\zeta^{-1}$ satisfies the quadratic polynomial

$$q(x) = x^2 + x(\lambda + \overline{\lambda})(\zeta + \zeta^{-1}) + (\lambda + \overline{\lambda})^2 - 4m + m(\zeta + \zeta^{-1})^2,$$

over $\mathbb{Q}(\lambda + \overline{\lambda}, \zeta + \zeta^{-1})$.

Proposition 10. *The polynomial $q(x)$ is irreducible over $\mathbb{Q}(\lambda + \overline{\lambda}, \zeta + \zeta^{-1})$.*

Proof. By way of contradiction, assume that

$$r = -\lambda\zeta - \overline{\lambda}\zeta^{-1} = \sum_{j=0}^{(p-3)/2} a_j(\zeta + \zeta^{-1})^j,$$

where each $a_j \in \mathbb{Q}(\lambda + \overline{\lambda})$. By Proposition 8, the mapping taking ζ to ζ^{-1} is an automorphism of $\mathbb{Q}(\lambda, \zeta)$ over $\mathbb{Q}(\lambda)$. Under this automorphism, r is mapped to $-\lambda\zeta^{-1} - \overline{\lambda}\zeta \neq -\lambda\zeta - \overline{\lambda}\zeta^{-1}$ while the right-hand side above remains fixed, which is impossible. □

By Proposition 8, $\Phi_p(x)$ is irreducible over $\mathbb{Q}(\lambda)$. Thus, the extension field $\mathbb{Q}(\lambda, \zeta)$ has degree $2p(p-1)$ over $\mathbb{Q}$. Its maximal real subfield must therefore have degree $\leq p(p-1)$.

Proposition 11. *Let p be a prime ≥ 5, and let m be an integer ≥ 2. The splitting field of $f_{p,m}$ is the maximal real subfield of $\mathbb{Q}(\lambda, \zeta)$ and can be written as*

$$K = \mathbb{Q}(\lambda + \overline{\lambda}, \zeta + \zeta^{-1}, \lambda\zeta + \overline{\lambda}\zeta^{-1}).$$

Proof. Observe that K is a real subfield of $\mathbb{Q}(\lambda, \zeta)$ and that all the roots of $f_{p,m}$ are real numbers in $\mathbb{Q}(\lambda, \zeta)$. From (6) and Proposition 10, $[K : \mathbb{Q}] = p(p-1)$. Since K is a real field of degree $p(p-1)$ over $\mathbb{Q}$, it is the maximal real subfield of $\mathbb{Q}(\lambda, \zeta)$, and consequently $f_{p,m}$ splits in K. If L is the splitting field of $f_{p,m}$, it follows that $L \subseteq K$. Note that $\lambda + \overline{\lambda}$, $\lambda\zeta + \overline{\lambda}\zeta^{-1}$ as well as $\lambda\zeta^{-1} + \overline{\lambda}\zeta$ are roots of $f_{p,m}$ and, hence, in L. To show then that $L = K$ it suffices to show that $\zeta + \zeta^{-1} \in L$, and this follows from

$$\zeta + \zeta^{-1} = \frac{(\lambda\zeta + \overline{\lambda}\zeta^{-1}) + (\lambda\zeta^{-1} + \overline{\lambda}\zeta)}{\lambda + \overline{\lambda}}.$$

This completes the proof. □

We are now ready to describe the Galois group of the splitting field K of $f_{p,m}$ over $\mathbb{Q}$. As $K \subseteq \mathbb{Q}(\lambda, \zeta)$, an automorphism of K can be described by its actions on λ and ζ.

Proposition 12. *Let p be a prime ≥ 5, and let m be an integer ≥ 2. Let g be a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. The Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$ is the subgroup of the symmetric group S_p generated by the automorphisms σ and γ, where $\sigma(\lambda) = \lambda\zeta$, $\sigma(\zeta) = \zeta$, $\tau(\lambda) = \lambda$, and $\tau(\zeta) = \zeta^g$.*

Proof. One has that σ is an automorphism of K which fixes $\mathbb{Q}$, whose order is p. Moreover, τ is an automorphism of K which fixes $\mathbb{Q}$ of order $p-1$. Since $[K : \mathbb{Q}] = p(p-1)$, we deduce that $\mathrm{Gal}(K/\mathbb{Q})$ is as claimed. □

4 A Ubiquitous Trinomial

In the previous section, we encountered the trinomial $p_m(x) = x^{2p} \pm x^p + m^p$, which we proved to be irreducible. In this section, we describe an alternative approach to establishing the irreducibility of many of the more general 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}, 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 $t_p(x) = x^{2p} - bx^p + c$. 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 $\zeta_6^{\pm 1} u$).

(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 $\sqrt{2}\zeta_8^{\pm 1} u$) or $x^2 + 2ux + 2u^2$ (with roots $\sqrt{2}\zeta_8^{\pm 3} u$) depending on whether $p \equiv \pm 1 \pmod 8$ or $p \equiv \pm 3 \pmod 8$, respectively.

(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 $\sqrt{3}\zeta_{12}^{\pm 1} u$) or $x^2 + 3ux + 3u^2$ (with roots $\sqrt{3}\zeta_{12}^{\pm 5} u$) 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 $t_p(x)$. In this section, we establish a result implying that if $b^2 - 4c$ is not a square and p is sufficiently large depending on b, then $t_p(x)$ is irreducible.

Our approach in this section takes 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 non-negative integers n by

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

and

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

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]. 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. 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 establish the following.

Proposition 13. *Let p be a prime and b and c be 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*

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

Proof. We consider p not dividing the above product. In particular, $p \notin \{2,3,5,7,13\}$. Initially, we begin along the lines of the proof of Proposition 7. Let $\gamma = (b+\sqrt{N})/2$ where $N = b^2 - 4c$, and let λ be a p^{th} root of γ. Following the proof of Proposition 7, it suffices to show that $x^p - \gamma$ is irreducible over $\mathbb{Q}(\gamma)$. Assuming $x^p - \gamma = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Q}(\gamma)[x]$ with $r = \deg g \in [1, p-1]$, we deduce

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

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 nonzero rational coprime integers. As $\alpha'/\beta' = -\alpha/\beta$, we also 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].

Before ending this section, we note that the condition in Proposition 13 that p not divide the product appears too strong as typically the trinomial $t_p(x)$ 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 above implies $t_p(x)$ is irreducible whenever c is not a p^{th} power, so examples of reducible $t_p(x)$ should take this into consideration. Among the more interesting examples of reducible $t_p(x)$ we found are

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

5 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 of the irreducibility of the trinomial $p_m(x) = x^{2p} \pm x^p + m^p$ 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.

Recall that we showed in the proof of Proposition 7 that 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 a quadratic x^2-x+m. The discriminant of this 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 the following result.

Proposition 14. *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

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

Proof. The above equation implies that there exist positive integers u and v satisfying

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

with d 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 of the Pell equation

$$AX^2 - BY^2 = 1. \tag{7}$$

Define

$$\alpha_0 = X_1\sqrt{A} + Y_1\sqrt{B} \quad \text{and} \quad \beta_0 = X_1\sqrt{A} - Y_1\sqrt{B}. \tag{8}$$

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 (7) 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 (7). 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 (7) with A and B as above (both X and Y are larger for any other solution in positive integers to (7)); thus, $X_1 = 1$ and $Y_1 = u$. We deduce that there is an odd positive integer t for which

$$\begin{aligned} x^\ell = X_t &= \frac{(\sqrt{du^2+1} + u\sqrt{d})^t + (\sqrt{du^2+1} - u\sqrt{d})^t}{2\sqrt{du^2+1}} \\ &= \frac{(\sqrt{ax^n} + \sqrt{ax^n - 1})^t + (\sqrt{ax^n} - \sqrt{ax^n - 1})^t}{2\sqrt{ax^n}}. \end{aligned} \tag{9}$$

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, (9) 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 (9) 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 (9), 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 14. 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 solutions in positive integers (x, y).*

The application we have in mind of Bennett's theorem is the following.

Proposition 15. *Let $m \geq 3$, and consider the Diophantine equation*

$$\frac{ax^r - 1}{ax^n - 1} = y^m. \tag{10}$$

(i) Suppose r and n are integers with $r > n > 0$ and $m|(r-n)$. Then there are no solutions to (10) in integers a, x, and y with $a > 0$ and $x > 1$.

(ii) Suppose r and n are integers with $r > n > 0$. Then there are no solutions to (10) in integers a, x, and y with $a > 0$ and $x > 1$ if also $x^{r-n} = z^m$ for some integer z.

Proof. (i) Assume (10) holds with the variables satisfying the conditions in (i). We have $r = n + m\ell$ for some positive integer ℓ. Then

$$ax^{n+m\ell} - 1 = (ax^n - 1)y^m \;\Rightarrow\; ax^n(x^\ell)^m - (ax^n - 1)y^m = 1. \tag{11}$$

Therefore, (x^ℓ, y) is a solution of the Diophantine equation

$$AX^m - BY^m = 1, \tag{12}$$

where $A = ax^n$ and $B = ax^n - 1$. But $(1, 1)$ is also a solution of the above equation. Observe that the conditions in (i) imply $ax^n > 1$, $x^\ell > 1$, and $y > 0$ (where we have used (11)

for this last inequality). In particular, $(x^\ell, y) \neq (1,1)$. By Bennett's theorem, we obtain a contradiction.

(ii) Assume (10) holds with the variables satisfying the conditions in (ii). Then (10) can be written as

$$ax^n z^m - (ax^n - 1)y^m = 1.$$

Thus, (z, y) is a solution of (12), together with $(1, 1)$. Using Bennett's theorem, we again obtain a contradiction. □

References

[ACZ] S. S. Abhyankar, S. D. Cohen, M. E. Zieve, *Bivariate factorizations connecting Dickson polynomials and Galois theory*, Trans. Amer. Math. Soc. **352** (2000), 2871–2887.

[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.

[BS] Z. I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, New York, 1986.

[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.

[O] O. Ore, *Some studies on cyclic determinants*, Duke Math. Journal, (1951), 343–354.

[Ri] T. J. Rivlin, The Chebyshev Polynomials, John Wiley and Sons, New York, 1974.

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

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

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

[Wae] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.

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