Journal of Integer Sequences, Vol. 12 (2009),
Article 09.2.8

On a Sequence of Nonsolvable Quintic Polynomials

Jennifer A. Johnstone and Blair K. Spearman[1]
Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC V1V 1V7
Canada
johnstone33@hotmail.com
Blair.Spearman@ubc.ca

Abstract

Aleksandrov, Kolmogorov and Lavrent'ev state that x^5+x-a is nonsolvable for $a = 3, 4, 5, 7, 8, 9, 10, 11, \ldots$. In other words, these polynomials have a nonsolvable Galois group. A full explanation of this sequence requires consideration of both reducible and irreducible solvable quintic polynomials of the form $x^5 + x - a$. All omissions from this sequence due to solvability are characterized. This requires the determination of the rational points on a genus 3 curve.

1 Introduction

Let $f(x)$ be a polynomial with rational coefficients. The polynomial $f(x)$ is solvable if its Galois group is solvable. Equivalently, the zeroes of $f(x)$ can be expressed in radical form. Dummit [6] provides a description of this process for quintic polynomials. Aleksandrov, Kolmogorov and Lavrent'ev [1] state that "the equation $x^5 + x - a = 0$, where a is a positive whole number, in most cases cannot be solved by radicals. For example, it is not solvable in radicals for $a = 3, 4, 5, 7, 8, 9, 10, 11, \ldots$ ". The purpose of this paper is to give a complete explanation of this sequence for all integers. Our main Theorem is

[1] All correspondence should be directed to this author.

Theorem 1. *Let $f(x) = x^5 + x - a$ where a is an integer. Then $f(x)$ is not solvable by radicals unless*

$$a = r^5 + r \text{ for some integer } r,$$
$$\text{or} \quad a = \pm 1, \pm 6.$$

In Section 2 we give some preliminary results we shall need for the proof of our theorem, which is given in Section 3.

2 Preliminary Results

If the polynomial $f(x) = x^5 + x - a$ is reducible over $\mathbb{Q}$ then $f(x)$ is solvable by radicals since the factors have degree at most four. In this section we begin by enumerating the values of the integer a for which $f(x)$ is reducible over $\mathbb{Q}$. The first class of reducibility is the easiest and is described in the following lemma, where the proof is obvious and thus omitted.

Lemma 1. *Let $f(x) = x^5 + x - a$ where a is an integer. If $f(x)$ has a rational zero, say r, then r is an integer and $a = r^5 + r$.*

For the second class of reducible polynomials Rabinowitz [7] provides us with the following result:

Proposition 1. *The only integers a for which $x^5 + x - a$ factors into the product of an irreducible quadratic and an irreducible cubic are $a = \pm 1$ and $a = \pm 6$.*

Now we need a characterization of solvable irreducible quintic trinomials $x^5 + x - a$. This is given by a Theorem of Dummit [6], specialized to our polynomials.

Proposition 2. *The irreducible quintic $x^5 + x - a \in \mathbb{Q}[x]$ is solvable by radicals if and only if the resolvent sextic polynomial*

$$t^6 + 8t^5 + 40t^4 + 160t^3 + 400t^2 + (512 - 3125a^4)t + 256 - 9375a^4 \tag{1}$$

has a rational zero t.

To finish this section we give a determination of the set of rational points on a genus 3 curve. This result will be required in the proof of our theorem.

Lemma 2. *The affine curve $y^2 = (20x^4 - 1)(5x^4 + 1)$ has no rational points.*

Proof. The computational method of proof used here is described in depth, with examples, by Bremner and Tzanakis [3]. We shall work in the number field $K = \mathbb{Q}(\theta)$ where θ is a zero of $z^4 + 3z^2 + 1$. The number field K is a bicyclic quartic field, specifically $K = \mathbb{Q}\left(\sqrt{-1}, \sqrt{5}\right)$. The maximal order O_K of K is $\mathbb{Z}[\theta]$, the class number of O_K is 1, and the fundamental unit of O_K is $\varepsilon = 1 + \theta^2$. Let $(x, y) = (X/Z, Y/Z^4)$ where $X, Y, Z \in \mathbb{Z}$ and $\gcd(X, Z) = 1$ with $Z \neq 0$. This gives us the following equation:

$$Y^2 = (20X^4 - Z^4)(5X^4 + Z^4). \tag{2}$$

If X and Z are both odd then (2) reduces to $Y^2 \equiv 2 \pmod 4$, which is impossible. If X is even and Z is odd then (2) reduces to $Y^2 \equiv 3 \pmod 4$, which is also impossible. Therefore, we may assume throughout the remainder of this proof that X is odd and Z is even. We also observe that $X \neq 0$. Factoring (2) over K gives

$$F_1 F_2 = 25Y^2.$$

where

$$\begin{aligned} F_1 &= (10X^2 + (2\theta^2+3)Z^2)(5X^2 + (\theta^3+4\theta)Z^2), \\ F_2 &= (10X^2 - (2\theta^2+3)Z^2)(5X^2 - (\theta^3+4\theta)Z^2). \end{aligned} \tag{3}$$

Now we have the following factorization of ideals in O_K

$$\langle 2 \rangle = \wp_2^2, \qquad \langle 5 \rangle = \wp_{51}^2 \wp_{52}^2.$$

We also have the identities

$$\begin{aligned} &(-10X^2 + (2\theta^3 + 2\theta^2 + 8\theta + 3)Z^2)F_1 + (10X^2 + (2\theta^3 + 2\theta^2 + 8\theta + 3)Z^2)F_2 \\ &= 10Z^6(\theta^3 - 4\theta^2 + 4\theta - 6), \end{aligned}$$

and

$$\begin{aligned} &((10\theta^3 + 10\theta^2 + 40\theta + 15)X^2 - (5\theta^3 + 10\theta)Z^2)F_1 \\ &+((10\theta^3 + 10\theta^2 + 40\theta + 15)X^2 + (5\theta^3 + 10\theta)Z^2)F_2 \\ &= 500X^6(2\theta^3 + 2\theta^2 + 8\theta + 3). \end{aligned}$$

Then since X and Z are relatively prime and the norms of the elements $(\theta^3 - 4\theta^2 + 4\theta - 6)$ and $(2\theta^3 + 2\theta^2 + 8\theta + 3)$ from K to $\mathbb{Q}$ are both equal to 5^4 we see that the gcd ideal of F_1 and F_2 involves only prime ideals dividing 2 and 5. Recalling the observation stated just after equation (2) that X is odd and Z is even, we see from equation (3) that $\wp_2^4 \parallel F_1F_2$, $\wp_2^2 \parallel F_1$ and $\wp_2^2 \parallel F_2$. Furthermore, if $5 \nmid Z$ then as ideals, $\langle 2\theta^2 + 3 \rangle = \langle \theta^3 + 4\theta \rangle = \wp_{51}\wp_{52}$, so that (3) implies $\wp_{51}^4\wp_{52}^4 \parallel F_1F_2$, $\wp_{51}^2\wp_{52}^2 \parallel F_1$, and $\wp_{51}^2\wp_{52}^2 \parallel F_2$. Finally, if $5 \mid Z$ then $5 \nmid X$ so that (3) gives $\wp_{51}^8\wp_{52}^8 \parallel F_1F_2$, $\wp_{51}^4\wp_{52}^4 \parallel F_1$ and $\wp_{51}^4\wp_{52}^4 \parallel F_2$. We conclude that modulo squares the gcd ideal of F_1 and F_2 is $\langle 1 \rangle$. We now deduce equations

$$F_1 = gU^2 \quad \text{and} \quad F_2 = gV^2, \tag{4}$$

with $5Y = gUV$ and $g = (-1)^{i_0}\varepsilon^{i_1}$, $i_0, i_1 = 0, 1$. Using the first of these two equations, a K-rational solution (X, Z, U) to this equation would yield a K-rational point (x, y) on the elliptic curve

$$y^2 g = x(10x + 2\theta^2 + 3)(5x + \theta^3 + 4\theta). \tag{5}$$

This elliptic curve arises by multiplying the first equation in (4) by X^2/Z^6 and defining $y = XU/Z^3$ and $x = X^2/Z^2$. We wish to determine the Mordell-Weil group of each of these elliptic curves over the number field K. To do this we appeal to Magma and the routine `PseudoMordellWeilGroup`. This routine uses a *2-isogeny descent* when available, returning *true* in the output when the rank is determined. Bruin [4] gives detailed information on this routine. For all four choices of g in (5), using `PseudoMordellWeilGroup,` we found that the group of K-rational points is isomorphic to $\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$. Thus the only K-rational points on (5) are the obvious 2-torsion points $(0,0)$, $\left(-\frac{2\theta^2+3}{10}, 0\right)$ and $\left(-\frac{\theta^3+4\theta}{5}, 0\right)$. If these points were to yield integer pairs (X, Z) with $X, Z \neq 0$, satisfying (2), then one of the nonzero x coordinates would have to be equal to the square of a nonzero rational number, which is impossible as they are not even in $\mathbb{Q}$. Hence there are no rational points on the curve $y^2 = (20x^4 - 1)(5x^4 + 1)$ except the two points at infinity. Equally well, for the last part of this proof, the Magma command `IsLocallySolvable` can be used to show that the curves $F_1 = gU^2$, given in (4), have no finite rational points.

□

3 Proof of Theorem

Proof. Suppose that $f(x) = x^5 + x - a$ is solvable by radicals. If $f(x)$ is reducible then either $f(x)$ has a rational root or $f(x)$ factors into the product of and irreducible quadratic and an irreducible cubic polynomial over $\mathbb{Q}$. The case of reducible quintics was covered by Lemma 1 and Proposition 1, in Section 2 . This gives us the exceptional values of a which are stated in our theorem. Now we search for integral values of a where the polynomials $x^5 + x - a$ are solvable and irreducible. By Proposition 2, this leads to a consideration of the rational solutions (t, a) satisfying (1). The curve (1) is birationally equivalent to the genus 3 curve

$$y^2 = (3125x^4 - 4)(3125x^4 + 16), \tag{6}$$

using the transformations

$$\begin{aligned} x &= \frac{a}{t+2}, \quad y = \frac{t^2+6t-16}{t+3}, \\ t &= \frac{3125x^4 + y}{2}, \quad a = 2x + \frac{3125x^5 + xy}{2}, \end{aligned} \tag{7}$$

and after scaling (6) becomes

$$y^2 = (20x^4 - 1)(5x^4 + 1).$$

As shown in Lemma 2, there are no rational points on this curve. We conclude from the birational transformations given in (7) that there are no finite rational points (t, a) satisfying (1) so that the determination of the integral values of a is complete.

□

Remark 1. In the proof of Theorem 1 we actually showed that there were no rational values of a such that $f(x) = x^5 + x - a$ is solvable and irreducible. An analog of Theorem 1 for sextic trinomials $x^6 + x - a$ would be an interesting calculation since for these sextics there exist rational values of a for which $x^6 + x - a$ is irreducible and solvable over $\mathbb{Q}$. The sextic trinomial $x^6 + x + \frac{41}{8}$ is irreducible and solvable with Galois group $6T13$ in Maple which is isomorphic to $C_3^2 \rtimes D_4$ [5].

4 Acknowledgements

Both authors received funding from the Natural Sciences and Engineering Research Council of Canada and wish to thank them for their support.

References

[1] A. D. Aleksandrov, A. N. Kolmogorov and M. A. Lavrent'ev, *Mathematics: Its Content, Methods and Meaning*, MIT Press, 1963.

[2] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: the user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[3] A. Bremner and N. Tzanakis, On squares in Lucas sequences, *J. Number Theory* **124** (2007), 511–520.

[4] N. Bruin, Some ternary diophantine equations of signature $(n, n, 2)$, in W. Bosma and J. Cannon, eds., *Discovering Mathematics with Magma: Reducing the Abstract to Concrete*, Springer, 2006, pp. 63–91.

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 2000.

[6] D. S. Dummit, Solving solvable quintics, *Math. Comput.* **57** (1991), 387–401.

[7] S. Rabinowitz, The factorization of $x^5 \pm x + n$, *Math. Mag.* **61** (1988), 191–193.

2000 *Mathematics Subject Classification*: Primary 12E05; Secondary 14G05.
Keywords: Nonsolvable polynomial, Galois group.

Received November 11 2008; revised version received February 13 2009. Published in *Journal of Integer Sequences*, February 15 2009.

Return to Journal of Integer Sequences home page.