THE FACTORIZATION OF $x^5 + ax^m + 1$.

Paul D. Lee and Blair K. Spearman

Received March 9, 2011

Abstract. We consider trinomials of the form $x^5 + ax^m + 1$ where a is a rational number and determine those trinomials that factor over the rational numbers as the product of an irreducible quadratic and an irreducible cubic. The solution requires the calculation of the rational points on a pair of genus 2 curves.

1 Introduction Let $f(x)$ be a polynomial with rational coefficients. The determination of those polynomials $f(x)$ with a specific form and a prescribed factorization often leads to interesting Diophantine problems. A general source of information on this type of problem is Schinzel [4]. In a paper by Rabinowitz [3] the factorization of $x^5 \pm x + n$, for n an integer, into the product of an irreducible quadratic and an irreducible cubic over the rational numbers $\mathbb{Q}$ was studied and a finite number of polynomials was determined. This type of result was extended by Spearman and Williams [5] to polynomials of the form $x^5 \pm x^m + n$, for $1 \leq m \leq 4$. The purpose of this paper is to study in a similar manner to [3] and [5] the particular class of quintic polynomials $f(x)$ given by

$$f(x) = x^5 + ax^m + 1,$$

where a is a rational number and $1 \leq m \leq 4$. We shall determine those rational values of a for which $f(x)$ is equal to the product of an irreducible quadratic and an irreducible cubic over $\mathbb{Q}$. In doing so, we take full advantage of a recent theoretical result of Stoll, described in Section 2, on rational points on certain genus 2 curves. We also take advantage of the computer algebra system Magma [1]. We note that such a factorization for $f(x) = x^5 + ax^m + 1$ immediately yields a factorization for the polynomial $x^5 + ax^{5-m} + 1$, by using the reverse polynomial $x^5 f\,(1/x)$. We state all of the factorizations of $f(x)$ for m satisfying $1 \leq m \leq 4$, for completeness. Finally, a factorization of $x^5 + ax^m + 1$ immediately yields a factorization for $x^5 + ax^m - 1$ if m is odd and $x^5 - ax^m - 1$ if m is even by scaling with $x \to -x$. Therefore we only treat the case where the constant term of $f(x)$ is equal to positive 1. We prove the following theorem.

Theorem 1. *Let $f(x) = x^5 + ax^m + 1$ where a is a rational number and m is an integer with $1 \leq m \leq 4$. Then $f(x)$ factors into the product of an irreducible quadratic and an irreducible cubic if and only if a and m assume the values listed in the following table. In each case the factorization is given.*

(a, m)	*factorization of* $x^5 + ax^m + 1$
$(1, 1)$	$x^5 + x + 1 = (x^2 + x + 1)(x^3 - x^2 + 1)$
$(-11/4, 1)$	$x^5 - 11/4x + 1 = (x^2 + x - 1/2)(x^3 - x^2 + 3/2x - 2)$
$(1, 4)$	$x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 - x + 1)$
$(-11/4, 4)$	$x^5 - 11/4x^4 + 1 = (x^2 - 2x - 2)(x^3 - 3/4x^2 + 1/2x - 1/2)$

2000 *Mathematics Subject Classification.* Primary 12E05, Secondary 14G05.
Key words and phrases. Reducible polynomial, genus 2 curve.

In Section 2 we give some preliminary results concerning rational points on specific genus 2 curves. In Section 3 we give the proof of our theorem.

2 Some Lemmas on Rational Points. In this section we give two lemmas which determine the set of rational points on two genus 2 curves. We refer the reader to Cassels and Flynn [2] as a reference for these types of algebraic curves. We will use a theorem of Stoll [6] which bounds the number of rational points on $C_k : y^2 = x^5 + k$ where k is a tenth-power-free integer. This theorem states that if the rank of the Jacobian of this curve is at most one then the number of rational points is bounded above by 7 and this bound is achieved only for $k = 324$. Assuming that C_k has no rational point of the form $(x, 0)$ for $k \neq 324$, the bound is 5. Magma will be used to determine the rank of the Jacobian for our curves using the command `RankBounds`. Additionally we use the fact that if the Jacobian of a genus 2 curve has a rank of zero, then one can enumerate all points in the Jacobian and consequently find all rational points on C_k. The Magma command that does this is `Chabauty0`. Now we analyze the rational points on two relevant genus 2 curves.

Lemma 1. *The only finite rational points on the genus 2 curve* $y^2 = x^5+4$ *are* $(0, \pm 2), (2, \pm 6)$.

Proof. We observe the four given points $(0, \pm 2), (2, \pm 6)$ on the curve. Magma confirms, using `RankBounds` that the rank of the Jacobian of this curve is equal to 1. Consequently the theorem of Stoll applies. The bound in this case, including the point at infinity, is 5 so that all of them are determined. □

Lemma 2. *The only finite rational points on the genus 2 curve* $y^2 = x^5 + 256$ *are* $(0, \pm 16)$.

Proof. The `RankBounds` command in Magma confirms that the rank of the Jacobian of the given curve is equal to 0. `Chabauty0` shows that the the finite points on this curve are indeed those listed in the statement of this lemma. □

3 Proofs of Theorems

Proof. As mentioned in the introduction we need only treat the cases $m = 1, 2$. Suppose that x^5+ax+1 is divisible by a quadratic polynomial x^2+ux+v where $a, u, v \in \mathbb{Q}$. Division of these two polynomials leads to

$$\begin{aligned} x^5 + ax + 1 = (x^2 + ux + v)(x^3 - x^2u + (-v + u^2)x + 2uv - u^3) \\ + (v^2 - 3vu^2 + a + u^4)x + 1 + vu^3 - 2uv^2 \end{aligned} \tag{1}$$

In equation (1) we equate the coefficients of x and 1 in the remainder to zero yieldng the pair of equations

$$\begin{aligned} v^2 - 3vu^2 + a + u^4 = 0, \\ 1 + vu^3 - 2uv^2 = 0. \end{aligned} \tag{2}$$

The second equation in (2) shows that $u \neq 0$ and $v \neq 0$. Eliminating v from (2), using a resultant, produces the equation

$$-11u^5 + 1 + 4ua - u^{10} + 3u^6a + 4u^2a^2 = 0. \tag{3}$$

The discriminant of (3), viewed as quadratic equation in a is equal to

$$25u^7(8 + u^5). \tag{4}$$

If (3) has a rational root a then (4) must be equal to a square in $\mathbb{Q}$, so that

$$25u^7(8 + u^5) = w^2, \tag{5}$$

for some rational number w. Since $u \neq 0$, it follows from (5) that $\left(\frac{2}{u}, \frac{2w}{5u^6}\right)$ is a point on

$$y^2 = x^5 + 4. \tag{6}$$

From Lemma 1, we know that $x = 2$, so that $u = 1$. Substituting $u = 1$ into (3) and factoring gives

$$(4a + 11)(a - 1) = 0.$$

The two choices of $a = 1, a = -11/4$ produce the factorizations given in the table in the theorem.

In this case, suppose similarily to the first case, that $f(x) = x^5 + ax^2 + 1$ is divisible by a quadratic polynomial $x^2 + ux + v$ where $a, u, v \in \mathbb{Q}$. Division of these two polynomials leads to

$$\begin{aligned} x^5 + ax^2 + 1 = (x^2 + ux + v)(x^3 - ux^2 + (-v + u^2)x + a + 2uv - u^3) \\ + (v^2 - ua - 3vu^2 + u^4)x + 1 + vu^3 - 2uv^2 - va. \end{aligned} \tag{7}$$

In equation (7) we equate the coefficients of x and 1 in the remainder to zero yielding the pair of equations

$$\begin{aligned} v^2 - 3vu^2 - ua + u^4 = 0, \\ 1 + vu^3 - 2uv^2 - va = 0. \end{aligned} \tag{8}$$

If there exists a solution to this pair of equations with $u = 0$, then the first equation simplifies to

$$v^2 = 0$$

so that $v = 0$. It would then follow that the irreducible quadratic factor of $f(x)$ is $x^2 + ux + v = x^2$ which violates irreducibility of the quadratic factor. Then since $u \neq 0$, we may solve the first equation in (8) to give

$$a = \frac{u^4 + v^2 - 3u^2v}{u}. \tag{9}$$

Substituting the value of a given in (9) into the second equation in (8) yields

$$\frac{u - v^3 + u^2v^2}{u} = 0$$

so that

$$u - v^3 + u^2v^2 = 0. \tag{10}$$

The existence of a rational solution u to (10) requires the discriminant of this quadratic in u to be equal to a square in $\mathbb{Q}$. That is

$$1 + 4v^5 = z^2 \tag{11}$$

for some rational number z. From (11) we see that $(x, y) = (4v, 16z)$ is a rational point on the genus 2 curve

$$y^2 = x^5 + 256. \tag{12}$$

Lemma 2 tells us that the only rational solution to (12) has $x = 0$ and since $x = 4v$ we must have $v = 0$. However this contradicts the assumption that $x^2 + ux + v$ is irreducible over $\mathbb{Q}$. Thus $f(x) = x^5 + ax^2 + 1$ cannot factor over $\mathbb{Q}$ as the product of an irreducible quadratic and an irreducible cubic. □

References

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

[2] J. W. S. Cassels and E. V. Flynn, Prolegomena To A Middlebrow Arithmetic Of Curves Of Genus 2, Cambridge University Press, 1996.

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

[4] A. Schinzel, On reducible trinomials, *Dissertationes Math. (Rozprawy Mat.)* **329** (1993), 1-83.

[5] B. K. Spearman and K. S. Williams, The factorization of $x^5 \pm x^a + n$, *Fibonacci Quart.* **36** (1998), 158-170.

[6] M. Stoll, On the Number of Rational Squares at Fixed Distance from a Fifth Power, *Acta Arith.* **125:1** (2006), 79-88.

Department of Mathematics, University of British Columbia, Okangan, 3333 University Way, Kelowna B.C. Canada V1V 1V7

E-mail : blair.spearman@ubc.ca