When Newton met Diophantus : A study of rational-derived polynomials and their extension to quadratic fields

Ralph H. Buchholz and James A. MacDougall

January*, 1999

Abstract

We consider the problem of classifying all univariate polynomials, defined over a domain k, with the property that they and all their derivatives have all their roots in k. This leads to a number of interesting sub-problems such as finding k-rational points on a curve of genus 1 and rational points on a curve of genus 2.

Keywords : polynomial, derivative, diophantine, elliptic, jacobian.

1 Introduction

Consider the polynomial $x^3 - 33x^2 + 216x$ and its first two derivatives, namely,

$$\begin{aligned} y &= x^3 - 33x^2 + 216x = x(x-9)(x-24), \\ y' &= 3x^2 - 66x + 216 = 3(x-4)(x-18), \\ y'' &= 6(x-11). \end{aligned}$$

Notice that the roots of y, y', and y'' are all integers. In this paper we generalize this observation and consider the problem of finding such polynomials defined over specific domains.

Definition : Let $\overline{D}(n, l, k)$ denote the set of polynomials of degree n with coefficients in some domain k, such that they and their first l derivatives have all their roots in k.

One can extend the above definition by letting l be an n-long binary vector describing which derivatives are required to have their roots in k. It should be clear from context when this extension is being used. We will also restrict

*Revision : June 21, 2009

ourselves to certain cases in which k is either an integral domain or a field. We call any polynomial in $\overline{D}(n,l,k)$ an (n,l,k)-derived polynomial or just a derived polynomial if the context is clear.

Given an arbitrary derived polynomial we have available a number of transformations (from the group of so-called axial deformation transformations of [22]), which do not produce an essentially different polynomial, namely,

- reflection about the lines $x = t$ or $y = t$ for some $t \in k$, denoted by R_t^x and R_t^y where
$$R_t^x : x \mapsto 2t - x, \quad R_t^y : y \mapsto 2t - y,$$
- scaling the x-axis or y-axis by some $t \in k^* = k\backslash\{0\}$, denoted by S_t^x and S_t^y, where
$$S_t^x : x \mapsto tx, \quad S_t^y : y \mapsto ty,$$
- translation parallel to the x-axis or y-axis by some $t \in k$, denoted by T_t^x and T_t^y where
$$T_t^x : x \mapsto x + t, \quad T_t^y : y \mapsto y + t.$$

Some axial deformations may not preserve the property of being a k-derived polynomial, so a little care is needed. Recall that arbitrary reflections (in lines perpendicular to a given line) can be expressed in terms of a single reflection (in a line perpendicular to the given line) and a translation (parallel to the given line) *e.g.* $R_t^x = T_{2t}^x \circ R_0^x$. Furthermore R_0^x and R_0^y both preserve the k-derived polynomial property. Next, a non-zero scaling of the y-axis does not move any of the roots of $p(x)$ or its derivatives while an x-axis scaling does. If k is a field then $S_t^x(p(x))$ is still k-derived whenever $p(x)$ is k-derived for any $t \in k^*$. But when k is an integral domain the only scalings, S_t^x, which preserve k-derived polynomials are those for which t divides the greatest common divisor of all the roots of $p(x)$ and all its specified derivatives. Finally, any translation parallel to the x-axis leaves a polynomial k-derived, while a translation parallel to the y-axis may or may not. This last translation T_t^y creates the most difficulty.

Accordingly, we define the generating sets

$$X = \{R_0^x, R_0^y\} \cup \{S_t^x \mid t \in k^*, p \in \overline{D} \to S_t^x(p) \in \overline{D}\} \cup \{S_t^y \mid t \in k^*\} \cup \{T_t^x \mid t \in k\}$$

and

$$X^* = X \cup \{T_t^y \mid t \in k, p \in \overline{D} \to T_t^y(p) \in \overline{D}\}.$$

We will consider only those polynomials which are distinct modulo any combination of the transformations in X or X^* and call these sets $D(n,l,k)$ and $D^*(n,l,k)$ respectively. Thus we have

$$D(n,l,k) = \frac{\overline{D}(n,l,k)}{\langle X \rangle} \qquad \text{and} \qquad D^*(n,l,k) = \frac{\overline{D}(n,l,k)}{\langle X^* \rangle}.$$

First, we make a number of elementary observations.

1. All polynomials in $\mathbb{Z}[x]$ are $\overline{\mathbb{Q}}$-derived.
2. The polynomial x^n is k-derived for any number field k.
3. For any polynomial, y say, there exists a number field, k, such that $y \in \overline{D}(n,l,k)$.
4. $\overline{D}(n,l,k) = \overline{D}(n,n-1,k)$ for all $l \geq n-1$.
5. $\overline{D}(n,n-2,k) = \overline{D}(n,n-1,k)$ if k is a field.
6. $\#D(n,l,\mathbb{Z}) \geq 2$ for all $n > l \geq 1$.
7. $\overline{D}(n,l,k) \subseteq \overline{D}(n,l,K)$ for any $k \subseteq K$.
8. $D(n,l,\mathbb{Z}_k) = D(n,l,k)$ for any number field k.

The first three items are really included simply to demonstrate the existence of (n,l,k)-derived polynomials. Note that in item 3, a bound for the degree of the number field would be given by an extension of $\mathbb{Q}$, by the roots of y and all its derivatives, of degree at most $1!2!3!\ldots n!$. The eighth item is a generalisation of an observation, by Don Zagier, that any $\mathbb{Q}$-derived polynomial can be rescaled to produce a $\mathbb{Z}$-derived polynomial.

To simplify the notation somewhat we will write $\overline{D}(n,k)$, $D(n,k)$ and $D^*(n,k)$ whenever $l \geq n-1$ for an integral domain or $l \geq n-2$ for a field. If $k = \mathbb{Q}$ then we will simply write $\overline{D}(n)$, $D(n)$ and $D^*(n)$ respectively in these cases.

2 Rational Derived Polynomials

From a number theoretic perspective, the most interesting cases for this problem are $k = \mathbb{Z}$ or $k = \mathbb{Q}$ and in this section we restrict to the latter since property (5) means we have one less derivative to consider. It is already known (for example see [4], [7], [10], [15], [16], [20], [33]) that

$$
\begin{aligned}
&D(1) = \{x\},\\
&D(2) = \{x^2, x(x-1)\},\\
&D(3) = \{x^3\} \cup \{x(x-1)(x-a) \mid a = \tfrac{w(w-2)}{w^2-1}, w \in \mathbb{Q}\},\\
&D(4) \supseteq \{x^4\} \cup \{x^2(x-1)(x-a) \mid a = \tfrac{9(2w+z-12)(w+2)}{(z-w-18)(8w+z)}, (w,z) \in E(\mathbb{Q})\},\\
&D(n) \supseteq \{x^n, x^{n-1}(x-1)\} \text{ for } n \geq 5,
\end{aligned}
$$

where E denotes the elliptic curve $z^2 = w(w-6)(w+18)$ which has infinitely many rational points. In fact the smallest non-trivial solution was first found by Carroll in 1989.

We note in passing that for $D(3)$ the root $a = \frac{w(w-2)}{w^2-1}$ corresponds (by homogenizing the numerator and denominator) to four consecutive terms of an arbitrary arithmetic progression $W-2Z$, $W-Z$, W, $W+Z$. As far as we can tell this was first observed as early as 1960 by Chapple.

We can classify any polynomial on the basis of the multiplicity of each distinct root such that a type $p_{(m_1,m_2,\ldots,m_r)}$ polynomial has r distinct roots where m_i is the multiplicity of the i-th root. Clearly, we have that $m_1 + m_2 + \cdots + m_r$ is just the degree of p. For example, all quartics belong to one of the categories of Table 1, which are in 1-1 correspondence with the partitions of four.

type	representative	$\mathbb{Q}$-derived
$p_{(1,1,1,1)}$	$x(x-1)(x-a)(x-b)$	no - Conjecture 1
$p_{(2,1,1)}$	$x^2(x-1)(x-a)$	yes
$p_{(2,2)}$	$x^2(x-1)^2$	no - $\sqrt{3} \notin \mathbb{Q}$
$p_{(3,1)}$	$x^3(x-1)$	yes
$p_{(4)}$	x^4	yes

Table 1: Quartic polynomial classification

Checking all derivatives shows that type $p_{(4)}$ and type $p_{(3,1)}$ polynomials are both rational-derived while the second derivative alone reveals that the type $p_{(2,2)}$ polynomial is not. With a little more effort (*e.g.*, [4], [20], [33]) one can show that the $p_{(2,1,1)}$ type leads to infinitely many distinct $\mathbb{Q}$-derived polynomials. The only unresolved case for quartic polynomials is the $p_{(1,1,1,1)}$ type. These lead to a pair of elliptic surfaces which we describe in Section 2.2.

Similarly, quintics belong to one of the seven types shown in Table 2. This time the unresolved cases are the $p_{(3,1,1)}$ type and the polynomials obtained by integrating the $p_{(1,1,1,1)}$ type. The $p_{(3,1,1)}$ quintics lead to a genus 2 curve which we explore a little more in Section 2.3. The $p_{(3,2)}$ quintics are fairly easily disposed of while the $p_{(2,2,1)}$ quintics require the following.

Theorem 1 *No $p_{(2,2,1)}$ quintic can be rational derived.*

Proof : Consider the generic type $p_{(2,2,1)}$ quintic and its first three derivatives,

$$\begin{aligned} y &= x^2(x-1)^2(x-a), \\ y' &= x(x-1)(5x^2-(4a+3)x+2a), \\ y'' &= 20x^3-12(a+2)x^2+6(2a+1)x-2a, \\ y''' &= 6(10x^2-4(a+2)x+(2a+1)). \end{aligned}$$

Now, if the first and third derivatives have rational roots then the product of the two discriminants (of the quadratic factors) must be a rational square, namely,

$$(4a^2-4a+6)(16a^2-16a+9) = \square.$$

However, a simple run through `apecs` in Maple reveals that this is birationally equivalent to a rank zero elliptic curve and hence has only one rational solution, $a = 1/2$, which does not lead to a rational-derived quintic. ■

If there are no solutions for either of the $p_{(1,1,1,1)}$ or $p_{(3,1,1)}$ cases then it is possible to classify all rational-derived polynomials. In fact there would turn out to be no new ones to add to the list of already known ones above.

Conjecture 1 *No polynomial of type $p_{(1,1,1,1)}$ is rational derived.*

Conjecture 2 *No polynomial of type $p_{(3,1,1)}$ is rational derived.*

type	representative	$\mathbb{Q}$-derived
$p_{(1,1,1,1,1)}$	$x(x-1)(x-a)(x-b)(x-c)$	no - Conjecture 1
$p_{(2,1,1,1)}$	$x^2(x-1)(x-a)(x-b)$	no - Conjecture 1
$p_{(2,2,1)}$	$x^2(x-1)^2(x-a)$	no - Theorem 1
$p_{(3,1,1)}$	$x^3(x-1)(x-a)$	no - Conjecture 2
$p_{(3,2)}$	$x^3(x-1)^2$	no - $\sqrt{6} \notin \mathbb{Q}$
$p_{(4,1)}$	$x^4(x-1)$	yes
$p_{(5)}$	x^5	yes

Table 2: Quintic polynomial classification

Evidence for Conjecture 1 is admittedly extremely sparse and in fact it is little more than wishful thinking on the part of those of us with a perverse desire to classify everything in sight. It has been shown (see [6]) that symmetric quartic polynomials, which are equivalent to $x(x-1)(x-a)(x-a-1)$, cannot be rational-derived. We provide an example of another infinite set of inequivalent quartics, which are not rational-derived, at the end of section 2.2.2. Furthermore, it seems almost pointless to mention any computational searches done and despite the fact that there are $4+3+2=9$ constraints on such quartics their existence relies on the intersection of two elliptic surfaces.

On the other hand, Conjecture 2 is far more plausible. First we will show that there are at most finitely many such quintics and that one can effectively bound their number. Furthermore, an efficient search has been made which has so far failed to reveal any examples. Based on discussions with Joseph Wetherell it seems likely that a proof of non-existence (using the techniques from [32]) is just around the corner.

Somewhat optimistically, we make the following conclusion which is no more than a slight correction to Carroll's observation [7].

Theorem 2 *If Conjectures 1 and 2 are true then*

$$D(n) = \{x^n, x^{n-1}(x-1)\}$$

for all $n \geq 5$.

Proof : If $n = 5$ we have $\{x^5, x^4(x-1)\} \subseteq D(5)$. Also type $p_{(3,2)} \notin D(5)$ by checking the second derivative while $p_{(3,1,1)} \notin D(5)$ by Conjecture 2. The

$p_{(2,2,1)}$ type is not rational-derived by Theorem 1. The remaining quintics of type $p_{(1,1,1,1,1)}$ and $p_{(2,1,1,1)}$ both have a first derivative of type $p_{(1,1,1,1)}$ and so cannot be rational derived by Conjecture 1. Assume that the theorem holds for $(n-1)$-degree polynomials then all polynomials of degree n with at most an $(n-2)$ multiplicity factor have a first derivative with at most an $(n-3)$ multiplicity factor. But none of these derivatives are rational derived and so we obtain the result by induction. ■

2.1 Cubics with three distinct roots

In this section we make a simple geometric observation about cubic polynomials which we prove algebraically. A similar observation for quartics is true, but by no means obvious—so this proof is used as a stepping stone for the quartic analog.

First recall that the discriminant of any polynomial, f say, provides us with information about the common roots of f and f', or equivalently, information about repeated roots of f. It can be calculated via

$$\begin{aligned}\Delta(f) &= \mathit{Resultant}(f(x), f'(x), x)\\ &= -\prod_{i\neq j}(x_i - x_j)^2.\end{aligned}$$

where the x_i are the roots of $f(x)$.

Now consider an arbitrary rational-derived cubic $f(x) = x(x-1)(x-a)$ with three distinct roots. Since f is rational-derived it is clear that the x-coordinate of the maximum, x_{max} say, is rational and hence the corresponding y-coordinate, $f(x_{max})$, is also rational. If we simply translate this cubic parallel to the y-axis by $f(x_{max})$ then the maximum becomes a (rational) double root and the third root, r say, of the cubic is forced to be rational—since the sum of the roots is rational. In other words, any rational-derived cubic with 3 distinct roots can be transformed into one with a double root by allowing a rational vertical translation (see Figure 1).

Suppose we translate $f(x)$ by $b \in \mathbb{Q}$ to get

$$F(x) = x^3 - (a+1)x^2 + ax + b.$$

Then $F(x)$ has a repeated root if and only if $\Delta(F) = 0$. So we require

$$\begin{aligned}\Delta(F) &= \mathit{Resultant}(F, F')\\ &= 27b^2 - 2(a-2)(a+1)(2a-1)b - a^2(a-1)^2\\ &= 0\end{aligned}$$

which has rational solutions for a and b only when the discriminant of the quadratic in b is a rational square, i.e.

$$\Delta(\Delta(F)) = 16(a^2 - a + 1)^3 = \square.$$

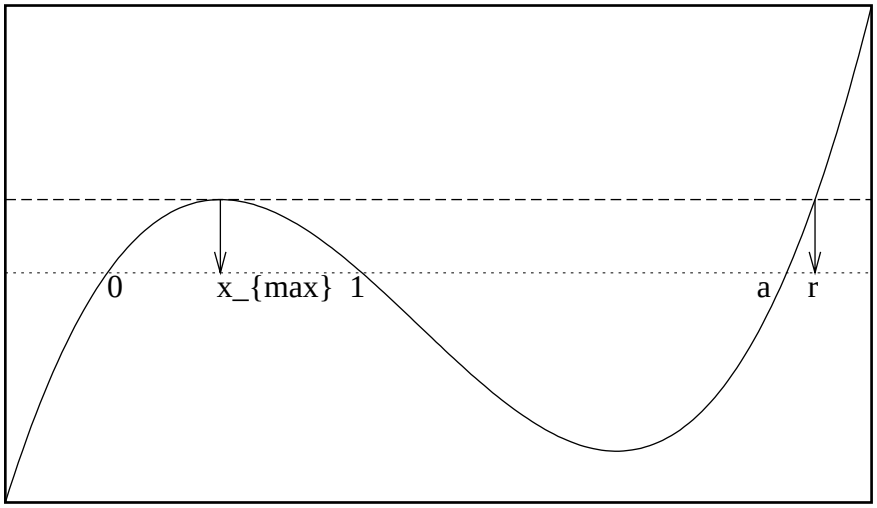

Figure 1: Vertical translate of a cubic

Clearly, this is equivalent to $(a^2-a+1) = \square$. However, recalling that $a = \frac{w(w-2)}{w^2-1}$ where $w \in \mathbb{Q}^*$ for all rational-derived cubics (with three distinct roots) we substitute into this expression to find that

$$a^2 - a + 1 = \left(\frac{w^2 - w + 1}{w^2 - 1}\right)^2$$

namely $\Delta(\Delta(F))$ is identically a square. This proves that all such rational-derived cubics can be transformed into one equivalent to $x^2(x-1)$ and hence $D^*(3) = \{x^3, x^2(x-1)\}$.

2.2 Quartics with four distinct roots

There are at least two possible approaches to the $p_{(1,1,1,1)}$ quartic. One is to force the quartic through the origin while the second (suggested by Scott Sciffer in [28]) is to force the first derivative to pass through the origin. For the former approach we find it convenient to work over the integers while for the latter we work over the rationals.

In the first approach we start with a generic quartic (rescaled to avoid fractions) and consider its first three derivatives

$$\begin{aligned}
y &= x(x-4a)(x-4b)(x-4c), \\
y' &= 4x^3 - 12(a+b+c)x^2 + 32(ab+ac+bc)x - 16abc, \\
y'' &= 12x^2 - 24(a+b+c)x + 32(ab+ac+bc), \\
y''' &= 24x - 24(a+b+c).
\end{aligned}$$

Translating by $x \mapsto x + (a+b+c)$ leaves the quartic with four integer roots and simplifies the conditions $y' = 0 = y''$ by removing the quadratic and linear terms respectively, to produce

$$\begin{aligned} x^3 - px + q &= 0, \\ 3x^2 - p &= 0, \end{aligned} \tag{1}$$

where $p = (-a+b+c)^2 + (a-b+c)^2 + (a+b-c)^2$ and $q = 2(-a+b+c)(a-b+c)(a+b-c)$.

2.2.1 Quartics with just the second derivative

We consider each of the equations in (1) separately before trying to combine the two constraints. For the $D(4, [1,0,1], \mathbb{Q})$ case we make a linear transformation so that

$$A := -a+b+c, \quad B := a-b+c, \quad C := a+b-c,$$

then the second derivative constraint becomes

$$3x^2 = A^2 + B^2 + C^2.$$

Notice that $(A, B, C, x) = (1, 1, 1, 1)$ is a particular solution and since this is a homogeneous quadratic we can use the chord method (mentioned in [12]) to parametrize all solutions as

$$\begin{aligned} dA &= -u^2 + v^2 + w^2 - 2uv - 2uw, \\ dB &= u^2 - v^2 + w^2 - 2uv - 2vw, \\ dC &= u^2 + v^2 - w^2 - 2uw - 2vw, \\ dx &= u^2 + v^2 + w^2. \end{aligned} \tag{2}$$

where $d = \gcd(r.h.s's)$ and $u, v, w \in \mathbb{Z}$. By solving these equations for a, b, c we obtain the following characterization.

Theorem 3 *All integer quartics with four distinct roots such that the second and third derivatives have all their roots in $\mathbb{Z}$ are equivalent to one given by $y = x(x-4a)(x-4b)(x-4c)$ where*

$$\begin{aligned} da &= u(u-v-w) - 2vw, \\ db &= v(-u+v-w) - 2uw, \\ dc &= w(-u-v+w) - 2uv \end{aligned}$$

such that

$$(u-v)(u-w)(v-w)(u+v+w) \neq 0.$$

2.2.2 Quartics with just the first derivative

The more difficult constraint, for the $D(4,[1,1,0],\mathbb{Q})$ case, is the requirement that all the roots of the cubic in (1) lie in $\mathbb{Z}$. From a paper by Schulz, [27], we find the result that

Theorem 4 (Schulz) *A cubic of the form $f(x) = x^3+Px+Q$ has three rational roots if and only if the following two conditions hold*

there exists one rational root, and
$-3((P/3)^3 + (Q/2)^2)$ is a perfect rational square.

Note that, since $\Delta(f) = 108((P/3)^3 + (Q/2)^2)$, Schulz' second condition is clearly equivalent to

$$\Delta(f) = -\square,$$

which we use from now on. For our particular cubic we require a refinement of Schulz' result which removes the first condition and works over the integers. But before stating it we recall a theorem of Mordell, [21], on non-equivalent binary cubics and their covariants which will be needed in the proof of Theorem 6.

Theorem 5 (Mordell) *All the solutions to the equation*

$$X^2 + 27Y^2 = Z^3, \quad (X,Z) = 1$$

are given by $(X,Y,Z) = (\frac{1}{2}G(x,y), \frac{1}{3}f(x,y), H(x,y))$ where

$$\begin{aligned} f(x,y) &= 9x^3 + 147x^2y + 798xy^2 + 1440y^3, \\ G(x,y) &= 20x^3 + 294x^2y + 1428xy^2 + 2288y^3, \\ H(x,y) &= 7x^2 + 74xy + 196y^2 \end{aligned}$$

for arbitrary integers x and y.

Now we are in a position to state our refinement of Schulz's result.

Theorem 6 *Any cubic equation of the form $x^3 - px + q$ has three distinct, relatively prime, integer roots if and only if*

$$4p^3 - 27q^2 = r^2, \quad (p,q) = 1, \ \textit{and} \quad 2 \mid q$$

where r is non-zero.

Proof: First we assume the cubic has 3 distinct, relatively prime roots, a', b', c' and then

$$x^3 - px + q = (x-a')(x-b')(x-c')$$

implies that $a'+b'+c'=0$, $p=-({a'}^2+a'b'+{b'}^2)$ and $q=a'b'(a'+b')$. Clearly, we observe that $2 \mid q$ and that a', b', c' are pairwise co-prime. Furthermore

$$(p,q)=({a'}^2+a'b'+{b'}^2, {a'}^2b'+a'{b'}^2) \mid ({a'}^3,{b'}^3) \mid (a',b')^3=1$$

A simple calculation reveals that

$$4p^3-27q^2=[(a'-b')(a'-c')(b'-c')]^2$$

which completes the implication in this direction.

In the reverse direction we require the solutions to

$$4p^3-27q^2=r^2, \quad (p,q)=1, \text{ and } \quad 2 \mid q.$$

Without loss of generality we can set $q=2Q$ and $r=2R$, then this equation becomes

$$p^3=27Q^2+R^2, \quad (p,Q)=1$$

which by Mordell's theorem has the solutions $(p,Q)=(H(u,v),\frac{1}{3}f(u,v))$ for arbitrary integers u and v. Now we find that our cubic factorizes as

$$x^3-H(u,v)x+\frac{2}{3}f(u,v)=[x-(2u+10v)][x-(u+6v)][x+(3u+16v)]$$

and checking the three possible pairwise identifications of the roots leads to $u/v=-4,-5,-6$. Each of these in turn contradict $(p,Q)=1$ which completes the proof in the reverse direction. ■

Finally, we can substitute our values for p and q into Theorem 6 to find that Caldwell's so-called nice quartics, [6], are characterized by the integer points on the surface :

$$\begin{aligned}\square = {} & 9(a^2-ab+b^2)c^4 \\ & -(14a^3-3a^2b-3ab^2+14b^3)c^3 \\ & +3(3a^4+a^3b-a^2b^2+ab^3+3b^4)c^2 \\ & -3(3a^4b-a^3b^2-a^2b^3+3ab^4)c \\ & +(9a^4b^2-14a^3b^3+9a^2b^4). \end{aligned} \tag{3}$$

We can obtain two infinite families of values for a and b such that this multiquartic condition, symmetric in a, b and c, becomes an elliptic surface. If we dehomogenize at $c=1$ (which is equivalent to dividing by c^6 for non-zero c and mapping $(a,b)\mapsto(a/c,b/c)$) then we have an elliptic surface whenever $a^2-a+1=\square$ or $9a^2-14a+9=\square$. Despite this we cannot always reduce it to an elliptic surface. For example, if we set $a=2, c=1$ then we obtain

$$\square=27b^4-108b^3+171b^2-126b+68$$

which has no rational solutions, when considered 3-adically, and so is not an elliptic curve.

2.2.3 Rational-derived quartics

If we combine the parametrization of Theorem 3 and the condition of Theorem 6 we obtain the requirement that

$$A_4(u,v,w)A_6(u,v,w) = B^2.$$

where A_4 and A_6 are homogeneous polynomials of degree 4 and 6 respectively. Hence we can divide by w^{10} and set $U := u/w$, $V := v/w$ to get a degree 10 hyperelliptic surface

$$\overline{A}_4(U,V)\overline{A}_6(U,V) = \overline{B}^2.$$

Rational points on this surface correspond to rational derived quartics.

Now we consider an alternative approach to the $p_{(1,1,1,1)}$ quartic (borrowing heavily from [28]) by letting the quartic have a zero at $x = 1$ and forcing the first derivative through the origin. This time we work exclusively over the rationals to get

$$\begin{aligned} y &= (x-1)(x-a)(x-b)(x-c), \\ &= x^4 - \sigma_1 x^3 + \sigma_2 x^2 - \sigma_3 x + \sigma_4, \\ y' &= 4x^3 - 3\sigma_1 x^2 + 2\sigma_2 x - \sigma_3, \\ y'' &= 12x^2 - 6\sigma_1 x + 2\sigma_2, \end{aligned}$$

where σ_i is the sum of the products of the roots of y taken i at a time. If we set the constant term in y' to zero our problem is simplified to a pair of quadratics. Now $\sigma_3 = 0$ is equivalent to

$$c = \frac{-ab}{ab + a + b}.$$

This identity maintains the rationality of all the roots of the quartic while the first and second derivatives have all rational roots if and only if the two discriminants are rational squares i.e.

$$9\sigma_1^2 - 32\sigma_2 = r^2, \quad \text{and} \quad 9\sigma_1^2 - 24\sigma_2 = s^2.$$

Substituting for σ_1 and σ_2 in terms of a and b and clearing the denominator leads to the two multiquartic equations

$$\begin{aligned} r_4 b^4 - r_3 b^3 + r_2 b^2 + r_1 b + r_0 &= \square, \\ s_4 b^4 - s_3 b^3 + s_2 b^2 + s_1 b + s_0 &= \square, \end{aligned}$$

where

$$\begin{aligned} r_4 &= 9a^2 + 18a + 9, & s_4 &= 9a^2 + 18a + 9, \\ r_3 &= 14a^3 + 10a^2 + 10a + 14, & s_3 &= 6a^3 - 6a^2 - 6a + 6, \\ r_2 &= 9a^4 - 10a^3 - 6a^2 - 10a + 9, & s_2 &= 9a^4 + 6a^3 + 18a^2 + 6a + 9, \\ r_1 &= 18a^4 - 10a^3 - 10a^2 + 18a, & s_1 &= 18a^4 + 6a^3 + 6a^2 + 18a, \\ r_0 &= 9a^4 - 14a^3 + 9a^2, & s_0 &= 9a^4 - 6a^3 + 9a^2. \end{aligned}$$

Since the coefficient of b^4 in both cases is a perfect square we can transform so that the equations become monic. Then we remove the cubic term in b which is followed by Mordell's transformation, [21], into an elliptic curve with coefficients which are polynomials in one parameter, namely a. Both these elliptic curves have an order two point and so we make a final transformation into the form

$$E_r[a] : z^2 = w(w^2 + R_2 w + R_4),$$
$$E_s[a] : Z^2 = W(W^2 + S_2 W + S_4),$$

where the coefficients are given by

$$R_2 = 9(9a^4 + 32a^3 - 18a^2 + 32a + 9), \qquad S_2 = 27(3a^4 + 8a^3 - 6a^2 + 8a + 3),$$
$$R_4 = -2^7 3^4 a^2 (a-1)^2 (a^2 + 4a + 1), \qquad S_4 = -2^5 3^6 a^2 (a^4 + 2a^3 + 2a + 1).$$

Since all these transformations were birational we have shown that any rational points $(w, z) \in E_r[a](\mathbb{Q})$ and $(W, Z) \in E_s[a](\mathbb{Q})$ which correspond to the same value of b provide a rational derived quartic.

2.2.4 Vertical translation of a quartic

If we now allow our rational-derived quartics to undergo a vertical translate by a rational distance, so that the (highest) local minimum, x_{min} say, is moved up to become a double root, then the remaining two roots, r and s say, of the quartic could possibly lie in a quadratic extension of $\mathbb{Q}$. Certainly, we have no *a priori* reason to expect the extra roots to be rational (see Figure 2). None-the-less, in this section we show that the latter is precisely the case.

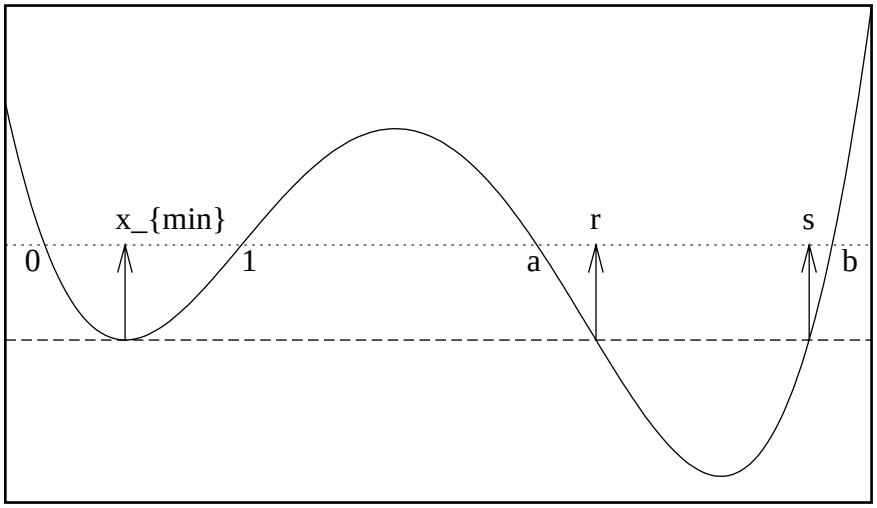

Figure 2: Vertical translate of a quartic

Consider a rational-derived quartic, $f(x)$ say, given by

$$f(x) = x(x-1)(x-a)(x-b),$$

which is to be translated by a rational amount, c say, parallel to the y-axis. We assume that the resulting quartic, $F(x)$ say, given by

$$F(x) = x(x-1)(x-a)(x-b) + c \tag{4}$$

is rational-derived and has a double root. As before, we require $\Delta(F) = 0$ so we calculate

$$\begin{aligned}\Delta(F) &= Resultant(F, F') \\ &= 256c^3 + p_4(a,b)c^2 + p_5(a,b)c + p_6(a,b) \\ &= 0.\end{aligned}$$

The number of real roots of this cubic is determined by its discriminant, so in this case we have

$$\Delta(\Delta(F)) = -2^{12}(a-b-1)^2(a-b+1)^2(a+b-1)^2 D_6(a,b)^3$$

where $D_6(a,b)$ is a multisextic polynomial in a and b given by

$$\begin{aligned}D_6(a,b) = {} & 9a^4b^2 - 14a^3b^3 + 9a^2b^4 \\ & - (9a^4b - 3a^3b^2 - 3a^2b^3 + 9ab^4) \\ & + 9a^4 + 3a^3b - 3a^2b^2 + 3ab^3 + 9b^4 \\ & - (14a^3 - 3a^2b - 3ab^2 + 14b^3) \\ & + 9a^2 - 9ab + 9b^2.\end{aligned}$$

Note that we will define $\Delta_F := \Delta(\Delta(F))$ to ease notation. Now the number of real roots of the equation $\Delta(F) = 0$ is precisely 1, 2, or 3 according as the discriminant is $\Delta_F > 0$, $\Delta_F = 0$, or $\Delta_F < 0$ respectively.

A routine analysis of the surface defined by $z = D_6(a,b)$ reveals that it has three stationary points shown in Table 3. Since $D_6(0,0) = D_6(1,1) = 0$, and

(a,b)	$\partial^2 z/\partial a^2$	$\partial^2 z/\partial a \partial b$	$\partial^2 z/\partial b^2$	type
$(0,0)$	18	-9	18	minimum
$(1/2,1/2)$	9/8	-39/8	9/8	saddle
$(1,1)$	18	-9	18	minimum

Table 3: Stationary points of $z = D_6(a,b)$

$D_6(1/2,1/2) = 1/2$ it is clear that $D_6(a,b) \geq 0$ which implies that $\Delta_F \leq 0$ and so Eq. (4) can never have precisely 1 real root.

In the case that $\Delta_F = 0$ we have one of

- $a - b - 1 = 0$,
- $a - b + 1 = 0$,
- $a + b - 1 = 0$, or
- $D_6(a, b) = 0$.

The first three cases immediately lead to a symmetric quartic which cannot be rational-derived. To deal with the fourth condition, we note the somewhat surprising result that $D_6(a, b)$ is related to the discriminant of $f'(x)$, *c.f.*, Eq. (3). In particular we find that

$$\Delta(f') = -16D_6(a, b)$$

so if $D_6(a, b) = 0$ then $\Delta(f') = 0$ which implies that $f'(x)$ would have a double root. This is impossible since we are assuming that $f(x)$ has four distinct roots.

The only remaining case occurs when $\Delta_F < 0$ which can only occur when $D_6(a, b) > 0$. We appeal to the same observation used above, namely that

$$\Delta_F = 2^8(a - b - 1)^2(a - b + 1)^2(a + b - 1)^2\Delta(f')^3.$$

If $\Delta_F \neq -\square$ then $\Delta(f') \neq -\square$ and hence $f'(x)$ will not have three rational roots by Theorem 4. Conversely, if $\Delta_F = -\square$ then $\Delta(f') = -\square$ leading to three distinct roots for f' as expected.

Previously one may have thought that the class of rational derived quartics with four distinct roots split into two types: those obtainable by a rational vertical translate from a $p_{(2,1,1)}$ quartic and those not so obtainable. The result of all the previous work shows that the latter class is empty and so any rational-derived quartic with four distinct roots can be vertically translated into a rational-derived quartic with a double root. Hence these are equivalent to one of the $p_{(2,1,1)}$ quartics for which we already have a complete description. In other words we can see that we have proven

Theorem 7 *All rational-derived quartics are equivalent, modulo $\langle X^* \rangle$, to one of the polynomials in the set*

$$D^*(4) = \{x^4\} \cup \{x^2(x-1)(x-a) \mid a = \tfrac{9(2w+z-12)(w+2)}{(z-w-18)(8w+z)}, (w, z) \in E(\mathbb{Q})\}.$$

where E denotes the curve $z^2 = w(w - 6)(w + 18)$.

2.3 Quintics with a triple root

Consider the generic $p_{(3,1,1)}$ quintic polynomial and its first three derivatives

$$\begin{aligned} y &= x^3(x-1)(x-a), \\ y' &= x^2(5x^2 - 4(a+1)x + 3a), \\ y'' &= 2x(10x^2 - 6(a+1)x + 3a), \\ y''' &= 6(10x^2 - 4(a+1)x + a). \end{aligned}$$

Now the first three derivatives have rational roots if and only if the discriminant of each quadratic factor is a rational square. Clearly, it is sufficient to find all values of $a \in \mathbb{Q}$ such that $\Delta(y')\Delta(y'')\Delta(y''') \in \mathbb{Q}^2$. In other words we require the rational solutions of

$$(4a^2 - 7a + 4)(9a^2 - 12a + 9)(4a^2 - 2a + 4) = b^2. \tag{5}$$

Using the transformation $a := (w-1)/(w+1), b := 2z/(w+1)^3$ we find it is equivalent to searching for rational points on the hyperelliptic curve

$$C : z^2 = 9w^6 + 195w^4 + 975w^2 + 1125.$$

By Faltings' theorem this curve contains only finitely many rational points (which had already been observed by Zagier in [33]). In fact, Bombieri showed (see [2]), that we can effectively bound their number by the rank of the Jacobian, $J(\mathbb{Q})$, and the size of the torsion subgroup. Thus there are at most finitely many $p_{(3,1,1)}$ type rational-derived quintics.

It turns out that the Jacobian is degenerate since the three discriminants are linearly dependent. This implies (as observed by Flynn, [14]) that the Jacobian $J(\mathbb{Q})$ is isogenous to the direct product of two elliptic curves given by

$$\begin{aligned} E_1 &: z^2 = 9w^3 + 195w^2 + 975w + 1125, \\ E_2 &: z^2 = 1125w^3 + 975w^2 + 195w + 9. \end{aligned}$$

Rescaling to make both cubics monic, translating to remove the constant and rescaling again to remove redundant factors leads to

$$\begin{aligned} E_1 &: z^2 = w(w+30)(w+120), \\ E_2 &: z^2 = w(w-150)(w+450). \end{aligned}$$

Applying Tate's Theorem, [29], to these shows that they both have rank 1 and their torsion is just the Klein 4 group. Thus

$$J(\mathbb{Q})/J_{tors}(\mathbb{Q}) \cong \mathbb{Z}^2.$$

Unfortunately, since the rank of the Jacobian is greater than one, we are not in a position to apply Chabauty's theorem, as suggested in [9], which provides an effective method for finding all rational points on the curve C.

As for the torsion subgroup of the Jacobian we first transform our curve C, via $(w, z) = (x/3, y/9)$, into the curve

$$D : y^2 = (x^2 + 15)(x^2 + 45)(x^2 + 135) = f(x)$$

with discriminant $2^{26} \cdot 3^{22} \cdot 5^{15}$. A short search revealed the rational points $(\pm 3, \pm 432)$ on the curve. Now the Weierstraß points of D are just given by

the roots of the three quadratics which gives us the divisors comprising the full 2-torsion of $J(\mathbb{Q})$, namely

$$\begin{aligned}\mathfrak{A} &= \{(\sqrt{-15},0),(-\sqrt{-15},0)\},\\ \mathfrak{B} &= \{(\sqrt{-45},0),(-\sqrt{-45},0)\},\\ \mathfrak{C} &= \{(\sqrt{-135},0),(-\sqrt{-135},0)\}.\end{aligned}$$

Next we use the injective homomorphism of reduction by a prime not dividing twice the discriminant of $f(x)$. With $p=7$ and $p=41$ we get $\#\tilde{J}(\mathbb{F}_7)=64$ and $\#\tilde{J}(\mathbb{F}_{41})=1296$ respectively. Thus we conclude that $J_{tors}(\mathbb{Q})$ injects into a group of order 16. At this point we know that

$$\{\mathfrak{O},\mathfrak{A},\mathfrak{B},\mathfrak{C}\}\subseteq J_{tors}(\mathbb{Q}) \quad \text{and} \quad \#J_{tors}(\mathbb{Q}) \mid 16.$$

To pin this down we search for an order 4 element of the Jacobian. Now $\mathfrak{D}\in J_{tors}(\mathbb{Q})$ has order 4 if and only if $2\mathfrak{D}$ is one of the order 2 divisors, $\mathfrak{A},\mathfrak{B},\mathfrak{C}$. Equivalently, $J_{tors}(\mathbb{Q})$ has order 4 elements if and only if one of $\mathfrak{A}$, $\mathfrak{B}$ or $\mathfrak{C}$ lie in $2J(\mathbb{Q})$.

The original approach we used, to prove that this could never happen, was essentially to attempt to halve each of $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$ by brute force. We assumed that $2\mathfrak{D}=\mathfrak{A}$ where $\mathfrak{D}=\{(w_1,z_1),(w_2,z_2)\}$ and $w_1\neq w_2$ and then intersected the curve D with the unique cubic defined by the points in $\mathfrak{D}$ and those in $\mathfrak{A}$. This led, via resultants, to a degree 5448 polynomial in a single variable (amongst other conditions) which provided no new divisors. We then had to check the case of $w_1=w_2$ and finally repeat the whole process for the other 2 divisors.

The following approach was suggested by a referee and borrows heavily from correspondence with E. V. Flynn. Consider the Cassels map, defined in [9], specialised to a curve of the form $y^2=(x^2-a)(x^2-b)(x^2-c)$ for which[1]

$$\mu : J(\mathbb{Q}) \longrightarrow \frac{K_1^*/(K_1^*)^2 \times K_2^*/(K_2^*)^2 \times K_3^*/(K_3^*)^2}{\mathbb{Q}^*}$$

where $K_1=\mathbb{Q}(\sqrt{a})$, $K_2=\mathbb{Q}(\sqrt{b})$, and $K_3=\mathbb{Q}(\sqrt{c})$. Furthermore μ acts on $J(\mathbb{Q})$ via

$$\mathfrak{D}\mapsto[(x_1-\sqrt{a})(x_2-\sqrt{a}),(x_1-\sqrt{b})(x_2-\sqrt{b}),(x_1-\sqrt{c})(x_2-\sqrt{c})]$$

where $\mathfrak{D}=\{(x_1,y_1),(x_2,y_2)\}$. Now since $2J(\mathbb{Q})\subseteq ker(\mu)$ it is sufficient to show that none of $\mathfrak{A}$, $\mathfrak{B}$ or $\mathfrak{C}$ lie in $ker(\mu)$. Picking on $\mathfrak{A}$ first one finds that

$$\begin{aligned}\mathfrak{A}\in ker(\mu) \leftrightarrow\ & [(a-b)(c-a),b-a,c-a]=[1,1,1]\\ \leftrightarrow\ & [a-b,(a-b)(a-c),1]=[1,1,1]\\ \leftrightarrow\ & a-b\in(K_1^*)^2 \quad \text{and} \quad (a-b)(a-c)\in(K_2^*)^2 \quad \text{OR}\\ & c(a-b)\in(K_1^*)^2 \quad \text{and} \quad c(a-b)(a-c)\in(K_2^*)^2.\end{aligned}$$

[1] Of course we are secretly thinking of a, b and c as corresponding to the divisors $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$ respectively.

Translating this last condition from the quadratic extensions to the rationals leads to the requirement that at least one of the following eight elements

$$\begin{aligned} [a-b, a-c], \quad & [a(a-b), a(a-c)], \\ [b(a-c), a-b], \quad & [ab(a-c), a(a-b)], \\ [c(a-b), a-c], \quad & [ac(a-b), a(a-c)], \\ [b(a-c), c(a-b)], \quad & [ab(a-c), ac(a-b)] \end{aligned}$$

lie in $(\mathbb{Q}^*)^2 \times (\mathbb{Q}^*)^2$. A simple check now shows that this fails for $a = -15$, $b = -45$ and $c = -135$ and hence that $\mathfrak{A} \notin ker(\mu)$.

This proves that $\mathfrak{A} \notin 2J(\mathbb{Q})$. A similar argument shows that $\mathfrak{B}, \mathfrak{C} \notin 2J(\mathbb{Q})$ and so the torsion subgroup is just the Klein 4 group. So we have

$$J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2.$$

Using the notation of [2] we find that either the height of the rational points on D is less than $\gamma(D)$ or the number of rational points on D is bounded by

$$\#D(\mathbb{Q}) < 4 \cdot 7^2 \cdot (1 + \log_2 \gamma(D))$$

where $\gamma(D)$ is an effectively computable constant.

3 UFD-derived quartics

When we try to extend the results to quadratic fields we automatically inherit all $\mathbb{Q}$-derived polynomials by property (7). So the type $p_{(4)}$ and $p_{(3,1)}$ quartics are k-derived for all $k = \mathbb{Q}(\sqrt{m})$. Next a check of the first two derivatives of the $p_{(2,2)}$ polynomial shows that it is $\mathbb{Q}(\sqrt{3})$-derived.

Now we consider the case of quartics with three distinct roots contained in $D(4, \mathbb{Q}(\sqrt{m}))$. Let $k = \mathbb{Q}(\sqrt{m})$, then we denote the ring of integers of k by $\mathbb{Z}_k = \mathbb{Z}[\alpha]$ where

$$\alpha = \begin{cases} \sqrt{m} & \text{if } m \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4. \end{cases} \tag{6}$$

As in [4], [20] and [33] we require that the discriminants of the first and second derivatives of such a quartic be squares over k. Thus, given the quartic

$$y = x^2(x-1)(x-a),$$

we require that $9a^2 - 6a + 9 = c^2$ and $9a^2 - 14a + 9 = d^2$ for some integers c and d. Using the chord method to solve the first constraint leads to $a = \frac{2(p^2-3pq)}{3(p^2-q^2)}$ for arbitrary integers p and q of $\mathbb{Z}_k$. Substituting this into the second discriminant condition and clearing denominators gives us

$$81q^4 - 252q^3p + 246q^2p^2 + 36qp^3 + 33p^4 = \square.$$

Now we dehomogenize the left hand side and then use Mordell's transformation to obtain the elliptic curve

$$E : z^2 = w(w-6)(w+18).$$

The transformation $a : E(k) \longrightarrow k$ given by

$$a((w,z)) = \frac{9(2w+z-12)(w+2)}{(z-w-18)(8w+z)}$$

provides the correspondence between all k-rational points on the curve E and all k-derived quartics. Finding all k-rational points on E in turn requires the determination of the rank of E over such number fields. Since the curve E has an order 2 point we initially used the usual technique of searching for solutions to the corresponding homogeneous spaces of $E(k)$ and its 2-isogenous curve, $\overline{E}(k)$, given by

$$\overline{E} : Z^2 = W(W^2 - 24W + 576).$$

We were able to resolve the rank for all fields except those with a radicand of -67, -163, 57 and 73. Fortunately, Andrew Bremner suggested using the method first mentioned by Birch (see [26]). This involves calculating the $\mathbb{Q}$-rank of E and its twist by the radicand of the quadratic field.

So, in particular, we let

$$E_m : mz^2 = w(w-6)(w+18)$$

denote the various twists of E. Then by Birch's result we have

$$\mathrm{rk}[E/\mathbb{Q}(\sqrt{m})] = \mathrm{rk}[E_m/\mathbb{Q}] + \mathrm{rk}[E_1/\mathbb{Q}].$$

Since we already know that $\mathrm{rk}[E_1/\mathbb{Q}] = 1$ it is sufficient to calculate the ranks of $E_m/\mathbb{Q}$ for each quadratic field. By a number of applications of `apecs` we were able to complete the unruly number fields (see Table 4). Note that we

m	2	3	U/U^2	$\mathrm{rk}[E/\mathbb{Q}(\sqrt{m})]$
-1	$u(1+\alpha)^2$	3	$\langle\alpha\rangle$	1
-2	$-\alpha^2$	$(1+\alpha)(1-\alpha)$	$\langle -1\rangle$	1
-3	2	$-(-1+2\alpha)^2$	$\langle -1\rangle$	1
-7	$\alpha\overline{\alpha}$	3	$\langle -1\rangle$	1
-11	2	$\alpha\overline{\alpha}$	$\langle -1\rangle$	3
-19	2	3	$\langle -1\rangle$	3
-43	2	3	$\langle -1\rangle$	3
-67	2	3	$\langle -1\rangle$	1
-163	2	3	$\langle -1\rangle$	1

Table 4: Rank of E over complex quadratic fields with class number 1

have included the factorization properties of 2 an 3 as well as the unit group

modulo squared units (U/U^2), since these provide a measure of the number of homogeneous spaces associated to E. It seems likely, (see [11]), that there are infinitely many real quadratic fields with class number 1 and so we restrict our attention to just the finite list of euclidean fields. Using the same notation as that for the complex quadratic fields we find (again using `apecs`) the ranks of E over real euclidean fields (see Table 5). We illustrate the previous work

m	2	3	U/U^2	$\mathrm{rk}[E/\mathbb{Q}(\sqrt{m})]$
2	α^2	3	$\langle -1, 1+\alpha\rangle$	1
3	$\overline{u}(1+\alpha)^2$	α^2	$\langle -1, 2+\alpha\rangle$	1
5	2	3	$\langle -1, \alpha\rangle$	2
6	$\overline{u}(2+\alpha)^2$	$\overline{u}(3+\alpha)^2$	$\langle -1, 5+2\alpha\rangle$	1
7	$\overline{u}(3+\alpha)^2$	$-(2+\alpha)(2-\alpha)$	$\langle -1, 8+3\alpha\rangle$	2
11	$\overline{u}(3+\alpha)^2$	3	$\langle -1, 10+3\alpha\rangle$	2
13	2	$-\alpha\overline{\alpha}$	$\langle -1, 1+w\rangle$	2
17	$-(1+\alpha)\overline{(1+\alpha)}$	3	$\langle -1, 3+2\alpha\rangle$	2
19	$\overline{u}(13+3\alpha)^2$	$-(4+\alpha)(4-\alpha)$	$\langle -1, 170+39\alpha\rangle$	2
21	2	$\overline{u}(1+\alpha)^2$	$\langle -1, 2+\alpha\rangle$	1
29	2	3	$\langle -1, 2+\alpha\rangle$	2
33	$-(2+\alpha)\overline{(2+\alpha)}$	$\overline{u}(5+2\alpha)^2$	$\langle -1, 19+8\alpha\rangle$	2
37	2	$-(2+\alpha)\overline{(2+\alpha)}$	$\langle -1, 5+2\alpha\rangle$	2
41	$(3+\alpha)\overline{(3+\alpha)}$	3	$\langle -1, 27+10\alpha\rangle$	2
57	$-(3+\alpha)\overline{(3+\alpha)}$	$\overline{u}(13+4\alpha)^2$	$\langle -1, 131+40\alpha\rangle$	1
73	$(4+\alpha)\overline{(4+\alpha)}$	$-(15+4\alpha)\overline{(15+4\alpha)}$	$\langle -1, 943+250\alpha\rangle$	2

Table 5: Rank of E over real euclidean quadratic fields

by giving an example of a $\mathbb{Q}(\sqrt{3})$-derived quartic which is not $\mathbb{Q}$-derived. Let $k = \mathbb{Q}(\sqrt{3})$. During the search of the homogeneous spaces we found the point $P = (w, z) = (18 - 12\alpha, 144 - 72\alpha)$ on the curve $E(k)$. We note that $a(P) = 1$ which corresponds to a degenerate k-derived quartic. However, since P is an infinite order point on $E(k)$ we can map any multiple of it. For instance,

$$a(-1 * P) = a((w, -z)) = \frac{37 - 20\alpha}{13}.$$

This implies that the quartic

$$y = x^2(x-1)\left(x - \frac{37 - 20\alpha}{13}\right)$$

is a non-trivial $\mathbb{Q}(\sqrt{3})$-derived polynomial, as is easily verified.

4 Conclusion

While we have not settled the classification problem our work shows that its solution is intimately bound to the case of the quartic with four distinct roots.

Any progress in this area presumably requires either a new insight into elliptic surfaces, to determine all their rational points, or an efficient computational procedure to possibly uncover the existence of such a rational derived quartic.

Note Added in Proof : The authors have recently received (June 1999) a manuscript from E. V. Flynn which claims to prove Conjecture 2.

5 References

1. P.A. Batnik, *Problem E3221*, American Mathematical Monthly, vol. 94, (1987), p. 681.
2. Enrico Bombieri, *The Mordell Conjecture Revisited* Annali Scuola Normale Sup. Pisa, Cl. Sci., S. IV, 17, (1990), pp. 615-640.
3. T. Bruggeman and T. Gush, *Nice cubic polynomials for curve sketching*, Mathematics Magazine, vol. 53, (1980), p. 233-234.
4. R. H. Buchholz and S. M. Ke11y, *Rational Derived Quartics*, Bulletin Aust. Math. Soc., (1995), vol. 51, no. 1, pp. 121-132.
5. Jim Buddenhagen, Charles Ford, and Mike May, *Nice Cubic polynomials, pythagorean triples, and the law of cosines*, Mathematics Magazine, (Oct. 1992), vol. 65, no. 4, pp. 244-249.
6. Chris K. Caldwell, *Nice polynomials of degree 4*, Mathematical Spectrum, (1990), vol. 23, no. 22, pp. 36-38.
7. C. E. Carroll, *Polynomials all of whose derivatives have integer roots*, American Mathematical Monthly, vol. 96, no. 2, (Feb. 1989), pp. 129-130.
8. Carroll, Kloke, Plethö *Solutions of 86-5*, Mathematical Intelligencer, vol. 9, no. 3, (1987), p. 43.
9. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series 230, Cambridge University Press, (1996).
10. M. Chapple, *A cubic equation with rational roots such that it and its derived equation also has rational roots*, A Mathematics Bulletin for Teachers in Secondary Schools, no. 11, (1960), pp. 5-7. (recently re-published in Aust. Senior Math. Journal, vol. 4, no. 1, (1990), pp. 57-60.)
11. T. J. Dekker, *Prime Numbers in Quadratic Fields*, CWI Quarterly, vol. 7, no. 4, Amsterdam, (Dec. 1994), pp. 367-394.
12. L. E. Dickson, *History of the Theory of Numbers*, vol. 2, Chelsea, (1952).
13. E. V. Flynn, *Descent via isogeny in dimension 2*, Acta Arithmetica, LXVI.1, (1994), pp. 23-43.
14. E. V. Flynn, *Private correspondence*, (Dec. 1995).
15. Bill Galvin, *'Nice' Cubic Polynomials with 'Nice' derivatives*, Aust. Senior Math. Journal, vol. 4, no. 1, (1990), pp. 17-21.
16. W. P. Galvin and J. A. MacDougall, *'Nice' Quartic Polynomials - The Sequel*, Australian Senior Mathematics Journal, vol. 8, no. 1, (1994), pp. 23-27.
17. G. Graham and C. Roberts, *A diophantine equation from calculus*, Mathematics Magazine, vol. 62, no. 2, (1989), pp. 97-101.
18. H. B. Griffiths and A. E. Hirst, *Cubic equations, or Where did the Examination question come from?*, American Mathematical Monthly, vol. 101, no. 2, (Feb. 1994), pp. 151-161.

19. Richard Guy, *Unsolved problems come of age*, American Mathematical Monthly, vol. 96, no. 10, (Dec 1989), pp. 907-908.

20. ———— *Unpublished manuscript*, (Dec. 1989), 9 pages.

21. L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

22. Nitsa Movshovitz-Hadar and Alla Shmukler, *Infinitely many different quartic polynomial curves*, The College Mathematics Journal, vol. 23, no. 3, (May 1992), pp. 186-195.

23. A. N. Parshin and I. R. Shafarevich, *Number Theory I*, Encyclopedia of Mathematical Science, vol. 49, Springer, Berlin, (1995).

24. F. Schmidt, *Problem 86-5*, Mathematical Intelligencer, vol. 8, no. 2, (1986), p. 48.

25. ———— *Problem 87-9*, Mathematical Intelligencer, vol. 9, no. 3, (1987), p. 40.

26. U. Schneider and H. G. Zimmer, *The rank of elliptic curves upon quadratic extension*, Computational Number Theory, Debrecen, (1989), de Gruyter, Berlin.

27. William C. Schulz, *Cubics with a rational root*, Mathematics Magazine, vol. 64, no. 3, (June 1991), pp. 172-175.

28. Scott Sciffer, *Private Correspondence*, (Dec. 1994).

29. J. H. Silverman and J. Tate, *Rational points on Elliptic curves*, Springer, New York, (1992).

30. B. M. M. de Weger, *A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number 2*, J. reine angew. Math., vol. 427, (1992), pp. 137-156.

31. S. H. Weintraub, *Partial solution to problem 87-9*, Mathematical Intelligencer, vol. 10, no. 2, (1988), p.55.

32. Joseph Loebach Wetherell, *Bounding the number of rational points on certain curves of high rank*, PhD manuscript, (1997), University of California at Berkeley.

33. Don Zagier, *Quartic polynomials all of whose derivatives have integer roots*, unpublished manuscript, (1989), 3 pages.

34. K. Zuser, *Uber eine gewisse Klasse von ganzen rationalen Funktionen 3. Grades*, Elemente der Mathematik, vol. 18, (1963), p. 101-104.

R. H. Buchholz
Department of Defence
Locked Bag 5076
Kingston, ACT 2605
AUSTRALIA
ralph@defcen.gov.au

J. A. MacDougall
Department of Mathematics
University of Newcastle
NSW 2308
AUSTRALIA
mmjam@cc.newcastle.edu.au