BULL. AUSTRAL. MATH. SOC. 11D25, 11G05
VOL. 51 (1995) [121–132]

ON RATIONAL-DERIVED QUARTICS

R.H. BUCHHOLZ AND S.M. KELLY

We present a characterisation of all quartic polynomials with exactly three distinct roots and the property that it and all its derivatives have rational roots. It turns out that there are an infinite number of distinct such quartics, each of which corresponds to a point on a related elliptic curve. Furthermore the collection of these points forms a proper subgroup of the group of rational points on the curve.

DEFINITION: A polynomial, $p(x)$, in $\mathbb{Q}[x]$ is a rational-derived quartic if and only if it and all its derivatives have rational roots. Similarly $p(x)$, in $\mathbb{Z}[x]$ is an integer-derived quartic if and only if it and all its derivatives have integer roots.

DEFINITION: We denote by $\mathcal{P}_n(\mathbb{Q})$ the set of all rational-derived polynomials of degree n.

1. INTRODUCTION

A number of authors have considered the problem of finding integer-derived polynomials. See for example [**1**, **2**, **3**, **4**] which contain results completely describing solutions for degrees 1, 2 and 3, and providing two infinite families of integer-derived polynomials for all degrees greater than 1. Carroll, in particular, makes a conjecture that $\mathcal{P}_4(\mathbb{Z})$ contains essentially only one polynomial with three or more distinct roots (apart from translation, rescaling or reflection about the x-axis), namely

$$p(x) = (x + 167)^2(x - 141)(x - 193).$$

This was shown [**5**] to be incorrect by the discovery of two non-equivalent polynomials. (See the discussion above Table 1.) We have found that there are in fact an infinite number of non-equivalent such polynomials which are characterised by the following theorem.

Consider the following elliptic curve and subgroup of rational points:

$$E: \quad Y^2 = X(X - 48)(X + 6),$$
$$E_A(\mathbb{Q}) = \{k(75, 405) : k \in \mathbb{Z}\}.$$

Received 7th April, 1994

THEOREM. *All rational-derived quartics of the form* $y = x^2(x-1)(x-a)$ *for* $a \neq 0, 1$ *are given by* $a = (5X + Y + 30)/9(X + 2)$ *where* $(X, Y) \in E_A(\mathbb{Q})$.

This throws doubt on the conclusions of Carroll that $\mathcal{P}_n(\mathbb{Z})$ contains only 2 infinite families of integer-derived polynomials for $n \geqslant 5$, which was based on his conjecture above.

2. QUARTICS

If we classify all quartics on the basis of the number of distinct roots then only the case of 4 distinct roots remains unsolved. As shown in the references mentioned above, rational-derived quartics with one distinct root are all equivalent to an infinite family, namely $y = (x-a)^4$.

All quartics with two distinct roots fall into two categories: namely the form $y = (x-a)^3(x-b)$ or the form $y = (x-a)^2(x-b)^2$. Only the first gives an infinite family of rational-derived quartics for all $a, b \in \mathbb{Q}$ while the second family provides no rational-derived quartics.

Any quartic with 3 distinct roots must be a translation, reflection or rescaling of

$$y = x^2(x-1)(x-a). \tag{1}$$

Notice that any rational-derived quartic (RDQ) can be rescaled by the least common multiple of the denominators of all the roots to produce an integer-derived quartic (IDQ), and any IDQ is automatically an RDQ so it is sufficient to characterise all RDQ's. Another reason for working over $\mathbb{Q}$ is that the root of the third derivative is always rational for rational a.

The first and second derivatives have rational roots if and only if the discriminants of the quadratic parts are rational squares. Specifically we require that $9a^2 - 14a + 9$ and $9a^2 - 6a + 9$ are simultaneously rational squares. An important observation is that such solutions form a subset of the solution space to the product of these two quadratic forms being a rational square. Consequently we consider the rational points on the curve

$$Y^2 = (9X^2 - 14X + 9)(9X^2 - 6X + 9). \tag{2}$$

Firstly we rescale the quartic using the transformation $X = U/9, Y = V/9$ to give

$$V^2 = U^4 - 20U^3 + 246U^2 - 1620U + 6561.$$

Next we remove the cubic term by setting $U = W + 5$ to give

$$V^2 = W^4 + 96W^2 - 160W + 2736.$$

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

Mordell's bi-rational transformation of a quartic to a cubic [6, p.139], namely $W = (T+40)/2(S+16)$, $V = 2S - W^2 - 16$ leads to

$$T^2 = 4(S+14)(S-34)(S+20).$$

One final rescaling $T = 2y$, $S = x - 14$ gives the elliptic curve in standard form:

$$E: \quad y^2 = x(x-48)(x+6). \tag{3}$$

Rescaling and translating Carroll's IDQ leads to an RDQ of the form of (1) with $a = 90/77$. Hence the point $(X,Y) = (90/77, 291.171/77^2)$ lies on (2). Using the transformations above implies that the point $(x,y) = (75,405) \in E(\mathbb{Q})$. Notice that all rational points on (3) correspond to rational points on (2), but only those which also force $9X^2 - 14X + 9$ to be a rational square (and hence automatically force $9X^2 - 6X + 9 \in \mathbb{Q}^2$) lead to values of a which make (1) an RDQ.

3. Characterising RDQ's from E

3.1 Rational Points on $\mathbf{E}(\mathbb{Q})$. Recall that all RDQ's of the form given by equation (1) correspond to a subset of the rational points on the elliptic curve given by equation (3). Hence we need to characterise all the rational points on E. Standard theory tells us that the rational points form a group, which we denote by $\mathbf{E}(\mathbb{Q})$. It turns out that the group $E(\mathbb{Q})$ has torsion free part isomorphic to $\mathbb{Z}$ and has torsion subgroup isomorphic to the Klein 4-group.

3.1.1 Torsion Subgroup. Let $E_{tors}(\mathbb{Q})$ denote the torsion subgroup of $E(\mathbb{Q})$. The discriminant, Δ, of E is given by $\Delta = 2^{16}3^{10}$ and hence reducing the curve modulo 5 (which does not divide Δ) leads to a non-singular curve. In fact a short calculation shows that

$$E\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}}.$$

By the Nagel-Lutz theorem [7, pp.221-222], the torsion subgroup of $E(\mathbb{Q})$ must be a subgroup of $E(\mathbb{Z}/5\mathbb{Z})$. We now show that there are no points of order 4 and hence $E_{tors}(\mathbb{Q})$ must be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ as the only points of order 2 on E are just $(x,y) = (-6,0), (0,0)$ or $(48,0)$. Suppose there exists a point $P = (x_0, y_0) \in E(\mathbb{Q})$ such that $4P = \mathcal{O}$, where $\mathcal{O}$ denotes the additive identity of the curve E. Then $2P = (x_1, y_1)$ must be one of the order 2 points. The equation of the line through P is $y = \lambda(x - x_0) + y_0$ and intersecting this with E gives a cubic in x:

$$x^3 - (42 + \lambda^2)x^2 + \ldots = 0.$$

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

Since the sum of the roots is the negative of the coefficient of x^2, we obtain $2x_0 + x_1 = 42 + \lambda^2$. Substituting $\lambda = f'(x_0)/2y_0 = (3x_0^2 - 84x_0 - 288)/2y_0$ into this expression leads to a quartic equation in x_0:

$$x_0^4 - 4x_1x_0^3 + (576 + 168x_1)x_0^2 + 1152x_1x_0 + 82944 = 0.$$

Each of the three cases for x_1 results in a contradiction.

i. $x_1 = 0 \Rightarrow x_0^2 = -288$ which has no rational solutions.
ii. $x_1 = -6 \Rightarrow x_0 = 12$, or -24 both of multiplicity 2 but not lying on E.
iii. $x_1 = 48 \Rightarrow x_0 = 48 \pm 36\sqrt{2}$ both of multiplicity 2 but irrational.

Hence there are no points of order 4 and $E_{tors}(\mathbb{Q}) = \{\mathcal{O}, (-6,0), (0,0), (48,0)\}$.

3.1.2 RANK OF $\mathbf{E}$. To determine the rank (that is, the number of linearly independent generators of the torsion-free part) of E we consider the isogeny ϕ, as in [7, p.302], defined by

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(-288 - x^2)}{x^2}\right)$$

which maps E to its 2-isogenous curve, $\overline{E}$ given by

$$\overline{E}: \quad Y^2 = X^3 + 84X^2 + 2916X.$$

We also make use of the usual 2-descent homomorphism, α, given by

$$\begin{aligned} \alpha(\mathcal{O}) &= 1 \qquad \bmod (\mathbb{Q}^*)^2, \\ \alpha((0,0)) &= -288 \bmod (\mathbb{Q}^*)^2, \\ \alpha((x,y)) &= x \qquad \bmod (\mathbb{Q}^*)^2. \end{aligned}$$

The following figure summarises the relationship between the elliptic curves, mappings and groups mentioned above.

$$\begin{array}{ccc} E & \xrightarrow{\ \phi\ } & \overline{E} \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \overline{\alpha}} \\ \mathbb{Q}/(\mathbb{Q}^*)^2 & & \mathbb{Q}/(\mathbb{Q}^*)^2 \end{array}$$

Figure 1.

From Tate's Theorem [8, pp.89–98] we know that the rank of E, denoted by $r(E)$, is given by

$$2^{r(E)} = \frac{|\alpha(E(\mathbb{Q}))|\ |\overline{\alpha}(\overline{E}(\mathbb{Q}))|}{4}.$$

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

For any point $(x,y) \in E(\mathbb{Q})$ we can take $x = dr^2/s^2$, $y = u/v$ where $\gcd(r,s) = 1$, d is squarefree and $\gcd(u,v) = 1$ which substituted into E gives

$$dt^2 = \left(dr^2 - 48s^2\right)\left(dr^2 + 6s^2\right) \tag{4}$$

for some rational t. Since $\alpha((x,y)) = d \bmod (\mathbb{Q}^*)^2$ we see that the number of distinct images of points from the elliptic curve in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is given by the number of distinct d for which (4) has at least one non-trivial solution, that is $r, s \neq 0$. This lets us bound $\left|\alpha(E(\mathbb{Q}))\right|$ and similarly $\left|\overline{\alpha}(\overline{E}(\mathbb{Q}))\right|$ and hence the rank of E.

Now $d \mid -288s^4$ which implies that $d \mid 6$ as d is squarefree. When $d = 1, -2, 3, -6$ we find that there are non-trivial solutions, namely

$$(r,s,t) = (36,3,1080),\ (1,1,10),\ (4,1,0),\ (1,1,0)$$

respectively. The remaining four values of d have no solutions. When $d = -1$ equation (4) becomes

$$-t^2 = r^4 + 42r^2s^2 - 288s^4.$$

Considering this modulo 3 implies that both t and r are divisible by 3. So letting $t = 3T$ and $r = 3R$ leads to

$$-T^2 = 9R^4 + 14.3R^2s^2 - 2^5s^4.$$

But this forces T and s to be divisible by 3 which contradicts $\gcd(r,s) = 1$. Hence there can be no solutions in this case which implies that $-1 \notin \alpha(E(\mathbb{Q}))$. However we already know that $-2, 3, -6 \in \alpha(E(\mathbb{Q}))$. This implies that $2, -3, 6 \notin \alpha(E(\mathbb{Q}))$. Otherwise, for example, $-2 \times 2 = -4 = -1 \bmod (\mathbb{Q}^*)^2$ and so -1 must be in $\alpha(E(\mathbb{Q}))$ which is a contradiction. Hence $|\alpha(E(\mathbb{Q}))| = 4$.

Applying the same process to $\overline{E}$ leads to the search for solutions to

$$DT^2 = D^2R^4 + 84DR^2S^2 + 2916S^4. \tag{5}$$

As before $D \mid 6$. For $D = 1, 6$ we have the solutions

$$(R,S,T) = (10,1,146),\ (1,1,24)$$

respectively. The remaining six values of D have no solutions. When $D = -1$ equation (5) becomes

$$-T^2 = \left(R^2 - 54S^2\right)^2 + 24R^2S^2.$$

This has no non-trivial real solutions let alone integer solutions. Similarly for $D = -2, -3, -6$ there are no possible solutions. When $D = 2$ equation (5) becomes

$$T^2 = 2R^4 + 84R^2S^2 + 1458S^4.$$

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

Now $2 \mid T$ so we make the substitution $T = 2\tau$ to give

$$2\tau^2 = R^4 + 42R^2S^2 + 729S^4.$$

Reducing this modulo 3 leads to the conclusion that three divides both R and τ. Using this last fact in the same way lets us remove the powers of three from the coefficient of S^4 and finally show that $3 \mid S$ which contradicts the fact that $\gcd(R,S) = 1$. Hence there are no solutions in this case. Now $3 \notin \overline{\alpha}(\overline{E}(\mathbb{Q}))$ since otherwise for example $3 \times 6 = 2 \bmod (\mathbb{Q}^*)^2$ which implies that $2 \in \overline{\alpha}(\overline{E}(\mathbb{Q}))$. Thus $|\overline{\alpha}(\overline{E}(\mathbb{Q}))| = 2$.

Finally this shows that the rank of E is one. Hence $E(\mathbb{Q}) = \{mP + nQ\}$ where $P \in \{(-6,0),(0,0),(48,0)\}$, $Q = (75,405)$, $m = 0,1$ and $n \in \mathbb{Z}$.

Thus $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

3.2 RDQ'S FORM A SUBGROUP OF $\mathbf{E}(\mathbb{Q})$. Having characterised $E(\mathbb{Q})$ we searched for points in $E(\mathbb{Q})$ which corresponded to RDQ's. We discovered that all small multiples of the point $(75,405)$ did in fact correspond to RDQ's and in addition, $(-6,0)$ added to any of these multiples also gave an RDQ. We call a point on $E(\mathbb{Q})$ which corresponds to an RDQ a rational-derived point (RDP). Using the transformations which convert equation (2) into equation (3) gives us a mapping $a : E(\mathbb{Q}) \mapsto \mathbb{Q}$ defined by

$$a = a(x,y) = \frac{5x + y + 30}{9(x+2)}.$$

Specifically, any $(x,y) \in E(\mathbb{Q})$ which is an RDP corresponds to an $a \in \mathbb{Q}$ for which (1) is an RDQ.

LEMMA 1. *If $(x,y) \in E(\mathbb{Q})$ is any RDP then $-((x,y) + (75,405))$ is also an RDP.*

PROOF: Firstly let $(\overline{x},\overline{y}) = -((x,y) + (75,405))$ and $\overline{a} = a((\overline{x},\overline{y}))$. Notice that if (x,y) is an RDP then there exists $r \in \mathbb{Q}$ such that

$$9a^2 - 14a + 9 = r^2. \tag{6}$$

It is sufficient to show that $\overline{a}$ satisfies

$$9\overline{a}^2 - 14\overline{a} + 9 = \overline{r}^2$$

for some $\overline{r} \in \mathbb{Q}$. Intersecting the line through (x,y) and $(75,405)$ with E gives

$$\overline{x} = \frac{75x^2 - 963x - 21600 - 810y}{(x-75)^2}$$

$$\overline{y} = \frac{-115425y + 10287yx + 8748000 + 2901420x - 405x^3 - 57105x^2}{(x-75)^3}.$$

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

Hence

$$\overline{a} = \frac{693yx + 20925y + 406755x + 465750 - 10755x^2}{(x-75)(77x^2 - 1263x - 810y - 10350)}.$$

If we write $a = n/d$ and $\overline{a} = \overline{n}/\overline{d}$ then

$$n\overline{n} - d\overline{d} = -693x^4 + 8181x^3 + 1078434x^2 + 6026400x + 693y^2x + 20925y^2.$$

Now using E to eliminate y^2 leads to $n\overline{n} - d\overline{d} = 0$ and hence $a\overline{a} = 1$. Replacing a by $1/\overline{a}$ in (6) gives

$$9 - 14\overline{a} + 9\overline{a}^2 = (r\overline{a})^2$$

as required. □

COROLLARY. *If $X = (x,y) \in E(\mathbb{Q})$ is any RDP and $Q = (75, 405)$ then*

$$a(X) = \frac{1}{a(-X-Q)}.$$

LEMMA 2. *If $(x,y) \in E(\mathbb{Q})$ is any RDP then $(x,-y)$ is also an RDP.*

PROOF: Again let $(\overline{x},\overline{y}) = (x,-y)$ then $\overline{a} = (5x - y + 30)/(9(x+2))$. As before it is sufficient to show that $\overline{a}$ satisfies

$$9\overline{a}^2 - 14\overline{a} + 9 = \overline{r}^2$$

for some $\overline{r} \in \mathbb{Q}$. Solving the equations for $a, \overline{a}$ in terms of x, y leads to

$$x = \frac{60 - 18a - 18\overline{a}}{9a + 9\overline{a} - 10}$$
$$y = \frac{180(a + \overline{a})}{9a + 9\overline{a} - 10}.$$

Substituting this into the elliptic curve gives a quadratic in a, namely

$$(90\overline{a} - 77)a^2 + \big(90\overline{a}^2 - 254\overline{a} + 90\big)a + \overline{a}(90 - 77\overline{a}) = 0.$$

Solving this for a and substituting into equation (6) we obtain

$$4(90\overline{a} - 77)^2 r^2 = p_1 - 10p_2^{1/2}p_3$$

where

$$p_1 = 36450\overline{a}^4 - 86670\overline{a}^3 + 101331\overline{a}^2 - 74504\overline{a} + 41301$$
$$p_2 = \big(9\overline{a}^2 - 14\overline{a} + 9\big)\big(9\overline{a}^2 - 6\overline{a} + 9\big)$$
$$p_3 = 405\overline{a}^2 - 513\overline{a} - 134.$$

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

Squaring and then completing the square where appropriate results in

$$(90\bar{a}-77)^2\left[\left\{(513\bar{a}^2-542\bar{a}+513)+4r^2(90\bar{a}-77)\right\}^2-400r^2(9\bar{a}^2-14\bar{a}+9)(9\bar{a}+2)^2\right]$$

being identically zero. If $\bar{a} \neq 77/90$ then we have

$$9\bar{a}^2-14\bar{a}+9=\left[\frac{(513\bar{a}^2-542\bar{a}+513)+4r^2(90\bar{a}-77)}{20r(9\bar{a}+2)}\right]^2.$$

Since $x,y \in \mathbb{Q}$ we have $\bar{a},r \in \mathbb{Q}$ and hence the right hand side above is a rational square. □

From these two lemmata we can conclude that addition of points and negation of points on E preserves the property of being an RDP.

THEOREM 1. *The set of all rational-derived points forms a subgroup $E_S(\mathbb{Q})$ of $E(\mathbb{Q})$ where $E_S(\mathbb{Q}) = \{\, m(-6,0)+n(75,405)\,\}$, $m=0,1$ and $n \in \mathbb{Z}$.*

PROOF: Recall that $(x,y)=(-6,0)$ is an RDP hence any element of $E_S(\mathbb{Q})$ is an RDP. So we just need to show that any RDP is an element of $E_S(\mathbb{Q})$. Suppose not, then there exists an RDP $(x,y) \in E(\mathbb{Q})\backslash E_S(\mathbb{Q})$ such that (x,y) can be expressed in the form

$$(x,y)=\begin{cases}(48,0)+n(75,405) & \text{or}\\ (0,0)\ +n(75,405).\end{cases}$$

If any such (x,y) is an RDP then by repeated application of Lemmata 1 and 2 we see that $(x,y)-n(75,405)$ must also be an RDP. This implies that either $(0,0)$ or $(48,0)$ must be an RDP. Now $a((0,0))=5/3$ and $a((48,0))=3/5$ neither of which satisfy $9a^2-14a+9 \in \mathbb{Q}^2$ and hence $(0,0)$ and $(48,0)$ are not RDP's, which contradicts our premise. □

3.3 FURTHER REFINEMENT OF $E_S(\mathbb{Q})$. We now notice that $E_S(\mathbb{Q})$ is degenerate in the sense that four different points correspond to the same rational derived quartic. In fact, the mapping $a : E_S(\mathbb{Q}) \mapsto \mathbb{Q}$ is two-to-one while the RDQ's corresponding to a and $1/a$ are equivalent. We require the following two technical lemmata, the first of which is analogous to Lemma 1, and the second showing that the mapping a is one-to-one when restricted to a subgroup of $E_S(\mathbb{Q})$.

LEMMA 3. *If $X=(x,y) \in E(\mathbb{Q})$ is any RDP and $P=(-6,0)$ then*

$$a(X)=\frac{1}{a(P+X)}.$$

PROOF: Firstly let $(\bar{x},\bar{y})=(-6,0)+(x,y)$ and $\bar{a}=a((\bar{x},\bar{y}))$ Following the line of reasoning used in Lemma 1, we intersect the line through (x,y) and $(-6,0)$ with E

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

and negate the y coordinate to give

$$\overline{x} = \frac{6(48-x)}{x+6} \qquad \overline{y} = \frac{-324y}{(x+6)^2}.$$

Hence

$$\overline{a} = \frac{-9(5x-y+30)}{(x+6)(x-75)}.$$

Again writing $a = n/d$ and $\overline{a} = \overline{n}/\overline{d}$ then

$$n\overline{n} - d\overline{d} = 9\left(x^3 - 42x^2 - 288x - y^2\right) = 0.$$

Clearly this leads to $a\overline{a} = 1$ as required. □

LEMMA 4. *If we define a proper subgroup $E_A(\mathbb{Q})$ of $E_S(\mathbb{Q})$ where $E_A(\mathbb{Q}) = \{n(75,405)\}, n \in \mathbb{Z}$ then $a : E_A(\mathbb{Q}) \mapsto \mathbb{Q}$ is one-to-one.*

PROOF: Consider two points $(x,y),(\overline{x},\overline{y}) \in E_A(\mathbb{Q})$. Now $a((x,y)) = a((\overline{x},\overline{y}))$ if and only if

$$\frac{5x+y+30}{9(x+2)} = \frac{5\overline{x}+\overline{y}+30}{9(\overline{x}+2)}$$

and hence

$$\overline{y}(x+2) - y(\overline{x}+2) = 20(\overline{x}-x).$$

Squaring this and using E leads to

$$2\overline{y}y(x+2)(\overline{x}+2) = (x+2)(\overline{x}+2)\left(\overline{x}^2x + \overline{x}x^2 + 2\overline{x}^2 - 88\overline{x}x + 2x^2 - 288\overline{x} - 288x\right).$$

Again squaring and using E we obtain

$$(x+2)(\overline{x}+2)(\overline{x}-x)^2\left[\left\{(x+2)\overline{x} + (2x-288)\right\}^2 + 800x\overline{x}\right] = 0.$$

Hence we have one of the following four cases:

i. $x = -2$
ii. $\overline{x} = -2$,
iii. $\overline{x} = x$, or
iv. $\left\{(x+2)\overline{x} + (2x-288)\right\}^2 = -800x\overline{x}$.

Notice that for any point $(x,y) \in E_A(\mathbb{Q})$ we must have $x \geqslant 48$ as $n(75,405)$ remains on the unbounded component of E by Bezout's Theorem. Case (iv) implies that x and $\overline{x}$ must have opposite sign unless $x\overline{x} = 0$ in which case the only possible solutions are $(x,\overline{x}) = (0,144),\ (144,0)$ again contradicting the result of Bezout's Theorem. Similarly cases (i) and (ii) can never occur. So the only remaining case is $\overline{x} = x$ which

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

when substituted back into the expression for $a((x,y)) = a((\overline{x},\overline{y}))$ gives $\overline{y} = y$. Thus a is one-to-one. □

THEOREM 2. *The set of all rational-derived quartics with exactly three distinct roots is generated by* $E_A(\mathbb{Q})$.

PROOF: Let $P = (-6,0)$, $Q = (75,405)$ and $X = (x,y)$ be any RDP. Since $X \in E_S(\mathbb{Q})$ we can write $X = mP + nQ \quad m = 0,1$. Now if $m = 1$ we get by Lemma 3

$$a(P + nQ) = \frac{1}{a(nQ)}$$

as $2P = \mathcal{O}$. Observe that the quartic $y = x^2(x-1)(x-1/a)$ is equivalent, under rescaling, to $y = x^2(x-1)(x-a)$ and so does not provide a new RDQ. Hence when $X = P + nQ$ we obtain the same RDQ as when $X = nQ$. Thus it is sufficient to consider the case $m = 0$. Now let $n = -r$ for $r \geqslant 1$. Then

$$a(-rQ) = \frac{1}{a((r-1)Q)}$$

by the Corollary to Lemma 1. This implies that it is sufficient to consider the positive multiples of Q as any negative multiple of Q will not provide us with any new RDQ's. Now by Lemma 4 we have $| Im(a) | = | E_A(\mathbb{Q}) |$. Since Q is a point of infinite order, every (positive) multiple of Q on E is distinct and consequently #RDQ's $= |Im(a)|/2 = \aleph_0$. □

By way of illustration, the table on the following page lists the first four elements of $E_A(\mathbb{Q})$, the resulting a value under the bijection from Lemma 4 and the non-zero roots of the corresponding integer-derived quartic. Note that the first example is equivalent to Carroll's IDQ and the second and third examples had been previously found by Galvin and MacDougall.

4. CONCLUSION

This completely determines all rational-derived quartics with exactly three distinct roots. The remaining unsolved degree 4 case is that with four distinct roots and at

https://doi.org/10.1017/S0004972700013940 Published online by Cambridge University Press

present a computer search has not found any examples.

n	$n(75,405)$	a	non-zero roots of IDQ
1	(75,405)	90/77	308,360
2	$\left(\frac{5329}{100}, -\frac{129283}{1000}\right)$	$\frac{167167}{497610}$	668668, 1990440
3	$\left(\frac{2447877675}{4713241}, -\frac{116043549439635}{10232446211}\right)$	$-\frac{128665027260}{69283212011}$	-514660109040, 277132848044
4	$\left(\frac{978328360054081}{6685637635600}, \frac{25593591021206391940079}{17286785808865496000}\right)$	$\frac{7010366636418797651}{4173952380480465660}$	16695809521921862640, 28041466545675190604

Correspondence between elements of $E_A(Q)$ and IDQ's

ADDED IN PROOF. Recent correspondence has revealed that both Richard Guy and Don Zagier had similar results, in unpublished form, as far back as 1989.

REFERENCES

[1] C.K. Caldwell, *Nice polynomials of degree 4*, Mathematical Spectrum, 1989.

[2] C.E. Carroll, 'Polynomials all of whose derivatives have integer roots', *Amer. Math. Monthly* **26** (1989), 129–130.

[3] M. Chapple, 'A cubic equation with rational roots such that its derived equation also has rational roots', *A Mathematics Bulletin for Teachers in Secondary Schools* **11** (1960), 5–7.

[4] B. Galvin, "Nice' cubic polynomials with 'nice' derivatives', in *Australian Senior Mathematics Journal* **4**, 1990, pp. 17–21.

[5] B. Galvin and J. MacDougall, Private Communication.

[6] L.J. Mordell, *Diophantine equations* (Academic Press, New York, 1969).

[7] J.H. Silverman, *The arithmetic of elliptic curves* (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

[8] J.H. Silverman and J. Tate, *Rational points on elliptic curves* (Springer-Verlag, New York, 1992).

Department of Defence
PO Box 4924
Kingston, ACT 2604
Australia
e-mail: ralph@defcen.gov.au