Proceedings of the Edinburgh Mathematical Society (2001) **44**, 103–110 ©

ON $\mathbb{Q}$-DERIVED POLYNOMIALS

E. V. FLYNN

Department of Mathematical Sciences, Mathematics and Oceanography Building, University of Liverpool, Peach Street, Liverpool L69 7ZL, UK

(Received 26 July 1999)

Abstract It is known that $\mathbb{Q}$-*derived* univariate polynomials (polynomials defined over $\mathbb{Q}$, with the property that they and all their derivatives have all their roots in $\mathbb{Q}$) can be completely classified subject to two conjectures: that no quartic with four distinct roots is $\mathbb{Q}$-derived, and that no quintic with a triple root and two other distinct roots is $\mathbb{Q}$-derived. We prove the second of these conjectures.

Keywords: genus 2; Jacobians; coverings; $\mathbb{Q}$-derived

AMS 2000 *Mathematics subject classification:* Primary 11G30

1. $\mathbb{Q}$-derived polynomials

If a (univariate) polynomial, defined over $\mathbb{Q}$, and all its derivatives have all of their roots in $\mathbb{Q}$, then we say that the polynomial is $\mathbb{Q}$-*derived*. We say that a polynomial is of type $p_{m_1,\dots,m_r}$ if it has r distinct roots, and each m_i is the multiplicity of the ith root. We further note that the property of being $\mathbb{Q}$-derived is always preserved by replacing $q(x)$ by $rq(sx+t)$ for any constants $r,s,t \in \mathbb{Q}$, with $r,s \neq 0$, and so we can take $q(x)$ to be monic, and can map any two roots to 0 and 1. We say that two $\mathbb{Q}$-derived polynomials $q_1(x)$ and $q_2(x)$ are *equivalent* if $q_2(x) = rq_1(sx+t)$, for some constants $r,s,t \in \mathbb{Q}$, with $r,s \neq 0$, and we shall only consider those polynomials which are distinct modulo any such transformation. In [**1**], the problem of classifying all $\mathbb{Q}$-derived polynomials has been reduced to showing the following two conjectures.

Conjecture 1.1. *No polynomial of type $p_{1,1,1,1}$ is $\mathbb{Q}$-derived.*

Conjecture 1.2. *No polynomial of type $p_{3,1,1}$ is $\mathbb{Q}$-derived.*

Indeed, the following theorem is presented in [**1**].

Theorem 1.3. *If Conjectures 1.1 and 1.2 are true, then all $\mathbb{Q}$-derived polynomials are equivalent to one of*

$$x^n, \quad x^{n-1}(x-1), \quad x(x-1)\left(x - \frac{v(v-2)}{v^2-1}\right), \quad x^2(x-1)\left(x - \frac{9(2w+z-12)(w+2)}{(z-w-18)(8w+z)}\right),$$

for some $n \in \mathbb{Z}^+$, $v \in \mathbb{Q}$, $(w,z) \in \mathcal{E}_0(\mathbb{Q})$, where $\mathcal{E}_0 : z^2 = w(w-6)(w+18)$ is an elliptic curve of rank 1.

https://doi.org/10.1017/S0013091599000760 Published online by Cambridge University Press

For Conjecture 1.2, we let $q(x)$ be a $\mathbb{Q}$-derived polynomial of type $p_{3,1,1}$, which we may take to be in the form $q(x) = x^3(x-1)(x-a)$, for some $a \in \mathbb{Q}$ with $a \neq 0, 1$. Then, as observed in [**1**], the discriminants of the quadratics $q'''(x)$, $q''(x)/x$ and $q'(x)/x^2$, must all be rational squares. This implies that a satisfies

$$b_1^2 = 4a^2 - 2a + 4, \quad b_2^2 = 9a^2 - 12a + 9, \quad b_3^2 = 4a^2 - 7a + 4, \tag{1.1}$$

for some $b_1, b_2, b_3 \in \mathbb{Q}$. Using the transformation $a = (X-3)/(X+3)$, $b_i = Y_i/(X+3)^3$, for $i = 1, 2, 3$, gives the genus 5 curve

$$\mathcal{F}_1 : Y_1^2 = 6(X^2+15),\ Y_2^2 = 6(X^2+45),\ Y_3^2 = X^2 + 135. \tag{1.2}$$

The curve $\mathcal{F}_1$, by the map $(X, Y_1, Y_2, Y_3) \mapsto (X, Y_1Y_2Y_3/6)$, covers the genus 2 curve

$$\mathcal{C}_1 : Y^2 = (X^2+15)(X^2+45)(X^2+135). \tag{1.3}$$

In order to find all polynomials of type $p_{3,1,1}$, it is sufficient to find all of $\mathcal{F}_1(\mathbb{Q})$. Indeed, it is sufficient to find all members of $\mathcal{C}_1(\mathbb{Q})$ that are images of the map $(X, Y_1, Y_2, Y_3) \mapsto (X, Y_1Y_2Y_3/6)$ from $\mathcal{F}_1(\mathbb{Q})$ to $\mathcal{C}_1(\mathbb{Q})$. The Jacobian J of $\mathcal{C}_1$ is isogenous over $\mathbb{Q}$ to $\mathcal{E}^a \times \mathcal{E}^b$, where

$$\left.\begin{aligned} \mathcal{E}^a &: Y^2 = (z+15)(z+45)(z+135), \\ \mathcal{E}^b &: \underline{Y}^2 = (15\underline{z}+1)(45\underline{z}+1)(135\underline{z}+1), \end{aligned}\right\} \tag{1.4}$$

both of which have rank 1, so that $J(\mathbb{Q})$ has rank 2. This makes the Chabauty techniques in [**5**] and Chapter 13 of [**2**], based on [**3**], not directly applicable, since they require the rank of $J(\mathbb{Q})$ to be less than the genus of the curve. A natural technique would now be to find the collection of covering curves induced by the isogeny from $\mathcal{E}^a \times \mathcal{E}^b$ to J, as in [**6**] and [**11**]. We find that $\mathcal{F}_1$ is a member of this covering collection, and so we are no closer to finding $\mathcal{F}_1(\mathbb{Q})$.

We shall exploit the fact that $\mathcal{C}_1$ is of the form $Y^2 = (X^2-k)(X^2-rk)(X^2-r^2k)$, which means that, as well as $(X,Y) \mapsto (-X, Y)$, there is also the involution $(X,Y) \mapsto (-rk/X, rk\sqrt{-rk}Y/X^3)$ on the curve, from which we can derive another isogeny to the Jacobian of $\mathcal{C}_1$. In § 2 we will describe how to find equations for a covering collection of curves induced by this isogeny. In § 3 we shall see that the resulting collection of curves for $\mathcal{C}_1$ allows us to find $\mathcal{C}_1(\mathbb{Q})$ and hence prove Conjecture 1.2.

2. Curves of the form $Y^2 = (X^2-k)(X^2-rk)(X^2-r^2k)$

We consider the curve of genus 2

$$\mathcal{C} : Y^2 = F(X) = (X^2-k)(X^2-rk)(X^2-r^2k), \quad r, k \in \mathbb{Q}, \quad k \neq 0, \quad r \neq 0, \pm 1, \tag{2.1}$$

with Jacobian J. We shall assume for simplicity that k, rk and $-rk$ are non-squares. We shall use ∞^+, ∞^- to denote the points on the non-singular curve that lie over the singular point at infinity on $\mathcal{C}$; they correspond to Y/X^3 taking the values 1 and -1, respectively. Both ∞^+ and ∞^- are in $\mathcal{C}(\mathbb{Q})$, since the coefficient of X^6 is a $\mathbb{Q}$-rational square. Following Chapter 1 of [**2**], any member of $J(\mathbb{Q})$ may be represented by a divisor of the form $P_1+P_2-\infty^+-\infty^-$, where P_1, P_2 are points on $\mathcal{C}$ and either P_1 and P_2 are both $\mathbb{Q}$-rational or P_1 and P_2 are quadratic over $\mathbb{Q}$ and conjugate. For convenience, we shall abbreviate such a divisor by $\{P_1, P_2\}$. This representation gives a 1–1 correspondence with $J(\mathbb{Q})$, except that everything of the form $\{(x,y),(x,-y)\}$ must be identified into a single equivalence class $\mathcal{O}$, which serves as the group identity in $J(\mathbb{Q})$.

The map $(X,Y)\mapsto(-X,Y)$ is an involution on $\mathcal{C}$, and the function X^2 is invariant under this map. There are then maps $\theta_1:(X,Y)\mapsto(X^2,Y)$ and $\theta_2:(X,Y)\mapsto(1/X^2, Y/X^3)$ from $\mathcal{C}$ to the elliptic curves

$$\left.\begin{aligned}\mathcal{E}^a &: y^2=(x-k)(x-rk)(x-r^2k),\\ \mathcal{E}^b &: \underline{y}^2=(-k\underline{x}+1)(-rk\underline{x}+1)(-r^2k\underline{x}+1),\end{aligned}\right\}\tag{2.2}$$

respectively, generalizing (1.4). As in [**11**], these induce the isogeny $\theta_1^*+\theta_2^*:\mathcal{E}^a\times\mathcal{E}^b\to J$.

The map $(X,Y)\mapsto(-rk/X, rk\sqrt{-rk}Y/X^3)$ is also an involution on $\mathcal{C}$; we first find the quotient of $\mathcal{C}$ by this map. First note that the functions

$$U=\frac{X+\sqrt{-rk}}{-X+\sqrt{-rk}},\qquad V=\frac{8\sqrt{-rk}Y}{(X-\sqrt{-rk})^3},\tag{2.3}$$

are, respectively, negated and left invariant by the involution. They give a $\mathbb{Q}(\sqrt{-rk})$-defined birational transformation between $\mathcal{C}$ and the curve:

$$V^2=-2k(U^2+1)((r+1)^2U^4-2(r^2-6r+1)U^2+(r+1)^2).\tag{2.4}$$

We are now in the same situation as in (2.2) and can use the maps $(U,V)\mapsto(U^2,V)$ and $(U,V)\mapsto(1/U^2,V/U^3)$, both of which map (2.4) to the elliptic curve

$$\mathcal{E}: v^2=-2k(u+1)((r+1)^2u^2-2(r^2-6r+1)u+(r+1)^2),\tag{2.5}$$

defined over $\mathbb{Q}$. Viewing $\mathcal{E}$ as being defined over $\mathbb{Q}(\sqrt{-rk})$, let A be the Weil-restriction of $\mathcal{E}$ over $\mathbb{Q}$. As a group, we can uniquely represent each member of $A(\mathbb{Q})$ as a pair $[P_1,P_2]\in\mathcal{E}(\mathbb{Q}(\sqrt{-rk}))\times\mathcal{E}(\mathbb{Q}(\sqrt{-rk}))$, where P_1 and P_2 are conjugates under $\sqrt{-rk}\mapsto -\sqrt{-rk}$. The maps $\psi_1:(X,Y)\mapsto(U^2,V)$ and $\psi_2:(X,Y)\mapsto(1/U^2,V/U^3)$ from $\mathcal{C}$ to $\mathcal{E}$, induce the isogeny $\phi=\psi_1^*+\psi_2^*:A\longrightarrow J$. This is essentially the same type of isogeny described after (2.2), except composed with the isomorphism of Jacobians induced by the birational transformation between $\mathcal{C}$ and (2.4). Furthermore, one can check directly that ψ_1 and ψ_2 are conjugates under $\sqrt{-rk}\mapsto-\sqrt{-rk}$, so that ϕ is defined over $\mathbb{Q}$. We shall require the injective homomorphism (a special case of [**8**])

$$\left.\begin{aligned}\mu &: J(\mathbb{Q})/\phi(A(\mathbb{Q}))\longrightarrow K^*/(K^*)^2\times\mathbb{Q}^*/(\mathbb{Q}^*)^2\\ &: \{(X_1,Y_1),(X_2,Y_2)\}\\ &\mapsto[(X_1-\sqrt{k})(X_1+r\sqrt{k})(X_2-\sqrt{k})(X_2+r\sqrt{k}),(X_1^2-rk)(X_2^2-rk)],\end{aligned}\right\}\tag{2.6}$$

where $K = \mathbb{Q}(\sqrt{k})$. Now let $(X, Y) \in \mathcal{C}(\mathbb{Q})$, and suppose that we have completely found

$$J(\mathbb{Q})/\phi(A(\mathbb{Q})) = \{D_1, \dots, D_n\} \quad \text{and} \quad \mu(D_i) = [d_i, e_i], \quad \text{for } i = 1, \dots, n. \tag{2.7}$$

Then, for some i, $\{(X, Y), \infty^+\} = D_i$ in $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ and so

$$\mu(\{(X, Y), \infty^+\}) = [(X - \sqrt{k})(X + r\sqrt{k}), X^2 - rk] = [d_i, e_i].$$

If we now define

$$x = 2X/(X^2 - rk), \tag{2.8}$$

which is invariant under our involution $(X, Y) \mapsto (-rk/X, rk\sqrt{-rk}Y/X^3)$, then

$$\left.\begin{aligned} rkx^2 + 1 &= x^2(X^2 + rk)^2/4X^2 \in (\mathbb{Q}^*)^2, \\ d_i\bar{d}_i(-(r-1)^2kx^2/4 + 1) &= d_i\bar{d}_i x^2(X^2 - k)(X - r^2k)/4X^2 \in (\mathbb{Q}^*)^2, \\ d_ie_i((r-1)\sqrt{k}x/2 + 1) &= d_ie_i x^2(X^2 - rk)(X - \sqrt{k})(X + r\sqrt{k})/4X^2 \in (K^*)^2. \end{aligned}\right\} \tag{2.9}$$

Regarding r, k, d_i, e_i as constants, and setting the first left-hand side to a variable squared, yields a curve of genus 0 over $\mathbb{Q}$. Doing the same with the product of the first two left-hand sides yields a curve of genus 1 over $\mathbb{Q}$, and the product of the first and third left-hand sides yields an elliptic curve over K. We summarize the above in the following lemma.

Lemma 2.1. *Let $\mathcal{C} : Y^2 = (X^2 - k)(X^2 - rk)(X^2 - r^2k)$, $r, k \in \mathbb{Q}$, $k \neq 0$, $r \neq 0, \pm 1$, let J be the Jacobian of $\mathcal{C}$, let $\mathcal{E} : v^2 = -2k(u+1)((r+1)^2u^2 - 2(r^2 - 6r + 1)u + (r+1)^2)$, regarded as defined over $\mathbb{Q}(\sqrt{-rk})$, and let A be the Weil-restriction of $\mathcal{E}$ over $\mathbb{Q}$. Let ϕ be the isogeny from A to J induced by the map (and its conjugate) from $\mathcal{C}$ to $\mathcal{E}$ given by $(X, Y) \mapsto (X + \sqrt{-rk})^2/(-X + \sqrt{-rk})^2, 8\sqrt{-rk}Y/(X - \sqrt{-rk})^3)$, and let μ be the injective homomorphism from $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ to $K^*/(K^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ given by (2.6), where $K = \mathbb{Q}(\alpha)$ and $\alpha = \sqrt{k}$. Suppose that $J(\mathbb{Q})/\phi(A(\mathbb{Q})) = \{D_1, \dots, D_n\}$, and $\mu(D_i) = [d_i, e_i]$ for $i = 1, \dots, n$. Let $(X, Y) \in \mathcal{C}(\mathbb{Q})$ and let $x = 2X/(X^2 - rk) \in \mathbb{Q}$. Then $\{(X, Y), \infty^+\} = D_i$ for some $i \in \{1, \dots, n\}$ and there exist $y, y_1 \in \mathbb{Q}$ and $y_2 \in K$ such that*

$$\left.\begin{aligned} G &: y^2 = rkx^2 + 1, \\ \mathcal{E}_{i,1} &: y_1^2 = d_i\bar{d}_i(rkx^2 + 1)(-(r-1)^2kx^2/4 + 1), \\ \mathcal{E}_{i,2} &: y_2^2 = d_ie_i(rkx^2 + 1)((r-1)\alpha x/2 + 1). \end{aligned}\right\} \tag{2.10}$$

This gives a strategy for trying to find all members of $\mathcal{C}(\mathbb{Q})$. One first performs a Galois descent to try to find a complete set of representatives $D_1, \dots, D_n$ for $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$. Then, for each $i \in \{1, \dots, n\}$, one hopes to find only finitely many $x \in \mathbb{Q}$ which satisfy all of G, $\mathcal{E}_{i,1}$ and $\mathcal{E}_{i,2}$, for some $y, y_1 \in \mathbb{Q}$ and $y_2 \in K$.

3. Solution of the case $p_{3,1,1}$

Recall from § 1 that it is sufficient to find $\mathcal{F}_1(\mathbb{Q})$, where $\mathcal{F}_1$ is as in (1.2). We first find $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$, where, as usual, J is Jacobian of $\mathcal{C}_1$, the curve (1.3) covered by $\mathcal{F}_1$.

Lemma 3.1. *Let $\mathcal{C}_1$ be the curve $Y^2 = (X^2+15)(X^2+45)(X^2+135)$ with Jacobian J and A, ϕ, μ as in Lemma 2.1, and let $\alpha = \sqrt{-15}$. Then $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ is given by*

$$D_1 = \mathcal{O}, \quad D_2 = \{(\alpha,0),(-\alpha,0)\}, \quad D_3 = \{(\sqrt{-45},0),(-\sqrt{-45},0)\}, \quad D_4 = D_2 + D_3,$$
$$D_5 = \{(3,432),\infty^+\}, \quad D_6 = D_5 + D_2, \quad D_7 = D_5 + D_3, \quad D_8 = D_5 + D_4,$$

whose images under μ are

$$\left.\begin{gathered} [d_1,e_1] = [1,1], \quad [d_2,e_2] = [30,1], \quad [d_3,e_3] = [-3,1], \\ [d_4,e_4] = [-10,1], \quad [d_5,e_5] = [54+6\alpha,6], \quad [d_6,e_6] = [45+5\alpha,6], \\ [d_7,e_7] = [-18-2\alpha,6], \quad [d_8,e_8] = [9+\alpha,6]. \end{gathered}\right\} \tag{3.1}$$

Proof. The images in (3.1) were obtained by applying the definition of μ in (2.6); they are all distinct members of $K^*/(K^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$. It was shown in [**1**] that $J(\mathbb{Q})$ has torsion group generated by D_2, D_3 and has rank 2 (the latter being immediate from the fact that each of $\mathcal{E}^a(\mathbb{Q})$, $\mathcal{E}^b(\mathbb{Q})$ in (1.4) has rank 1). Thus, $J(\mathbb{Q})/2J(\mathbb{Q})$ is generated by D_2, D_3, D_5 and one further generator. Recall also from [**7**] that if for some c, we let $\theta_1,\dots,\theta_6$ be the roots of $H(X) = F(X+c)$, and find that

$$h(X) = \prod (X - \theta_i\theta_j\theta_k - \theta_\ell\theta_m\theta_n)$$

is square-free and has no $\mathbb{Q}$-rational root, then $\{\infty^+,\infty^+\} \notin 2J(\mathbb{Q})$. The product in the definition of $h(X)$ is taken over the 10 unordered partitions of the six roots $\theta_1,\dots,\theta_6$ of $H(X)$ into two sets of three. Applying this to $H(X) = F(X+1)$ gives $h(X)$ of degree 10 with factors:

$$x^2 - 176x - 35\,456, \quad x^2 + 184x - 2336, \quad x^2 + 124x + 125\,344,$$
$$x^2 + 364x + 154\,624, \quad x^2 + 304x + 671\,104,$$

and so $\{\infty^+,\infty^+\} \notin 2J(\mathbb{Q})$. Hence D_2, D_3, D_5, $\{\infty^+,\infty^+\}$ generate $J(\mathbb{Q})/2J(\mathbb{Q})$, with $\{\infty^+,\infty^+\} = \mathcal{O}$ in $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$. Hence D_2, D_3, D_5 generate $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$, as required. Note that $D_1,\dots,D_8$ are simply the eight elements of the Boolean group $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ generated by D_2, D_3, D_5. □

We are now in a position to apply Lemma 2.1 and determine all of $\mathcal{F}_1(\mathbb{Q})$.

Lemma 3.2. *Let $\mathcal{F}_1 : Y_1^2 = 6(X^2+15)$, $Y_2^2 = 6(X^2+45)$, $Y_3^2 = X^2+135$, and let (X,Y_1,Y_2,Y_3) be an affine member of $\mathcal{F}_1(\mathbb{Q})$. Then $(X,Y_1,Y_2,Y_3) = (\pm 3, \pm 12, \pm 18, \pm 12)$.*

Proof. We can apply Lemma 2.1 with $r = 3$, $k = -15$, $\alpha = \sqrt{-15}$, $K = \mathbb{Q}(\alpha)$ and $[d_1,e_1],\dots,[d_8,e_8]$ as in (3.1). Let $(X,Y) \in \mathcal{C}_1(\mathbb{Q})$ be in the image of the map $(X,Y_1,Y_2,Y_3) \mapsto (X, Y_1Y_2Y_3/6)$ from $\mathcal{F}_1(\mathbb{Q})$ to $\mathcal{C}_1(\mathbb{Q})$, and let $x = 2X/(X^2 - rk) \in \mathbb{Q}$.

Then $\{(X,Y),\infty^+\} = D_i$ in $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ for some $i \in \{1,\dots,8\}$. First note that we can dismiss the cases $i = 1,2,3,4$, since then $X^2+45 = e_i = 1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, contradicting $Y_2^2 = 6(X^2+45)$.

For each of $i = 5,6,7,8$, the curve $\mathcal{E}_{i,1}$ of (2.10) is a rank 1 elliptic curve over $\mathbb{Q}$, and so is of no help. For $i = 6$, it is sufficient to find all $x \in \mathbb{Q}$ and $y_2 \in K$ such that (x, y_2) is a point on $\mathcal{E}_{6,2} : y_2^2 = 6(45+5\alpha)(-45x^2+1)(\alpha x+1)$. The 5-adic norm $|\cdot|_5$ has a unique extension to K; note that $|\alpha|_5 = 5^{-1/2}$ and any $w \in K^*$ satisfies $|w|_5 = 5^{r/2}$ for some $r \in \mathbb{Z}$. If $|x|_5 > 1$, then $|x|_5 = 5^s$ for some $s \in \mathbb{Z}^+$, since $x \in \mathbb{Q}$, giving $|x|_5 \geqslant 5$; therefore $6(45+5\alpha)(-45x^2+1)(\alpha x+1)$ has 5-adic norm $5^{-5/2}|x|_5^3 = 5^{(6s-5)/2}$, and so cannot be a square in K. If $|x|_5 \leqslant 1$, then $6(45+5\alpha)(-45x^2+1)(\alpha x+1) \equiv 6\cdot 45 \equiv -3\alpha^2 \pmod{\alpha^3}$. This is also a non-square in K, since -3 is not a quadratic residue mod α. We can similarly discard the case $i = 7$.

For $i = 5$, it is sufficient to find all $x \in \mathbb{Q}$ and $y_2 \in K$ such that (x, y_2) is a point on

$$\mathcal{E}_{5,2} : y_2^2 = 6(54+6\alpha)(-45x^2+1)(\alpha x+1). \tag{3.2}$$

Applying standard descent techniques [**4**, **8**–**10**], we find that $\mathcal{E}_{5,2}(K)$ has rank 1 and is generated by the 2-torsion point $(-1/\alpha, 0)$ and the point $P_1 = (1/6+\alpha/30, 24)$ of infinite order. Since the rank of $\mathcal{E}_{5,2}(K)$ is less than the degree of K, we can apply the technique in [**6**] as follows. First note that $5P_1$ is in the kernel of reduction mod 11, so we define

$$\left.\begin{aligned} Q_1 = 5P_1, \quad \text{where } P_1 = (1/6+\alpha/30, 24),\\ \mathcal{S} = \{\infty, (-1/\alpha,0), \pm P_1, (-1/\alpha,0)\pm P_1, \pm 2P_1, (-1/\alpha,0)\pm 2P_1\},\end{aligned}\right\} \tag{3.3}$$

so that

$$\text{every } P \in \mathcal{E}_{5,2}(K) \text{ can be written as } P = S + nQ_1, \text{ for some } S \in \mathcal{S},\ n \in \mathbb{Z}. \tag{3.4}$$

Since Q_1 is in the kernel of $\tilde{\ }$, the reduction map mod 11, we must have $\tilde{P} = \tilde{S}$. So, if P has $\mathbb{Q}$-rational x-coordinate, then $\tilde{S}$ must have $\mathbb{F}_{11}$-rational x-coordinate. Computing the members of $\mathcal{S}$ mod 11, we find that this is true only for

$$S = \infty, \quad (-1/\alpha,0)\pm P_1 = \pm(-1/3, 12+12\alpha), \quad (-1/\alpha,0)\pm 2P_1 = \pm(1/9, -12-4\alpha/3),$$

and so these are the only $S \in \mathcal{S}$ we need to consider. We make the following five claims.

Claim *k*. *$n = 0$ is the only $n \in \mathbb{Z}$ for which $R_k + nQ_1$ has $\mathbb{Q}$-rational x-coordinate,* where $k = 1,\dots,5$, and $R_1 = \infty$, $R_2 = (-1/3, 12+12\alpha)$, $R_3 = (-1/3, -12-12\alpha)$, $R_4 = (1/9, -12-4\alpha/3)$, $R_5 = (1/9, 12+4\alpha/3)$. We shall give only a sketch for proving these five claims, since the detailed steps are similar to those in [**6**]. Letting $\phi_{R_k}(n)$ denote the x-coordinate of $R_k + nQ_1$ for $k = 2,3,4,5$ and the reciprocal of the x-coordinate of $R_k + nQ_1$ for $k = 1$, we know from [**6**] that $\phi_{R_k}(n)$ can be written as a power series in n defined over $\mathbb{Z}_{11}[\alpha]$. For each k, write $\phi_{R_k}(n) = \phi^{(0)}_{R_k}(n) + \phi^{(1)}_{R_k}(n)\alpha$, where each of $\phi^{(0)}_{R_k}$, $\phi^{(1)}_{R_k}$ is in $\mathbb{Z}_{11}[\![n]\!]$. The resulting power series $\phi^{(1)}_{R_k}$ may be computed mod 11^3 using the

https://doi.org/10.1017/S0013091599000760 Published online by Cambridge University Press

equations in [**6**], and are as follows:

$$\left.\begin{aligned}
&\phi^{(1)}_{R_1}(n) = O(n^2) \in \mathbb{Z}_{11}[\![n]\!], \quad \phi^{(1)}_{R_k}(n) = O(n) \in \mathbb{Z}_{11}[\![n]\!], \quad \text{for } k = 2,3,4,5;\\
&\phi^{(1)}_{R_1}(n) \equiv 9 \cdot 11^2 n^2 \pmod{11^3},\\
&\phi^{(1)}_{R_2}(n) \equiv 68 \cdot 11n + 5 \cdot 11^2 n^2 \pmod{11^3},\\
&\phi^{(1)}_{R_3}(n) \equiv 53 \cdot 11n + 5 \cdot 11^2 n^2 \pmod{11^3},\\
&\phi^{(1)}_{R_4}(n) \equiv 35 \cdot 11n + 8 \cdot 11^2 n^2 \pmod{11^3},\\
&\phi^{(1)}_{R_5}(n) \equiv 86 \cdot 11n + 8 \cdot 11^2 n^2 \pmod{11^3}.
\end{aligned}\right\} \tag{3.5}$$

For each k, if $R_k + nP_1$ has $\mathbb{Q}$-rational x-coordinate, then $\phi^{(1)}_{R_k}(n) = 0$. Since the leading coefficient of each power series has 11-adic norm strictly greater than all subsequent coefficients, it is clear that $n = 0$ is the only solution in each case, which proves all five claims, and so $x = \infty, -1/3, 1/9$ are the only possibilities. Since $x = 2X/(X^2 - rk) = 2X/(X^2 + 45)$, the corresponding values of X are $\pm\sqrt{-45}$, $-3 \pm 6i$, 3 and 15. Of these, only $3, 15 \in \mathbb{Q}$. Substituting $X = 3$ into the equation of $\mathcal{C}_1$, we see that $Y^2 = (3^2+15)(3^2+45)(3^2+135) = 186\,624$, which has solutions $Y = \pm 432$. Substituting $X = 15$ gives $Y^2 = 23\,328\,000$, which does not have a $\mathbb{Q}$-rational solution for Y. It follows that $(X, Y) = (3, \pm 432)$ are the only two points on $\mathcal{C}_1$ corresponding to the case $i = 5$. Note that, had we wished, we could have used curve G in (2.10) mod 11 as an alternative way of eliminating R_2 and R_3. An almost identical argument, also 11-adic, shows that $(X, Y) = (-3, \pm 432)$ are the only two points on $\mathcal{C}_1$ corresponding to the case $i = 8$.

Having considered all cases $i = 1, \dots, 8$, we conclude that the only members of $\mathcal{C}_1(\mathbb{Q})$ in the image of the map $(X, Y_1, Y_2, Y_3) \mapsto (X, Y_1Y_2Y_3/6)$ from $\mathcal{F}_1(\mathbb{Q})$ to $\mathcal{C}_1(\mathbb{Q})$ are ∞^+, ∞^-, $(\pm 3, \pm 432)$. Therefore, all affine $(X, Y_1, Y_2, Y_3) \in \mathcal{F}_1(\mathbb{Q})$ have $X = \pm 3$, as claimed. □

We can now achieve our aim of proving Conjecture 1.2.

Theorem 3.3. *No polynomial of type $p_{3,1,1}$ is $\mathbb{Q}$-derived.*

Proof. Recall from § 1 that we can take our polynomial to be of the form $q(x) = x^3(x-1)(x-a)$, for some $a \in \mathbb{Q}$ with $a \neq 0, 1$, satisfying (1.1) for some $b_1, b_2, b_3 \in \mathbb{Q}$. The map from (1.1) to $\mathcal{F}_1$ is $a = (X-3)/(X+3)$, $b_i = Y_i/(X+3)^3$, for $i = 1, 2, 3$. We have shown in Lemma 3.2 that the only possible values of X are $\pm 3, \infty$; these correspond to $a = 0, \infty, 1$, which are precisely the degenerate values of a for which $q(x)$ is not of type $p_{3,1,1}$. □

Note that we have not determined $\mathcal{C}_1(\mathbb{Q})$, since this was not required for proving Conjecture 1.2. In fact, it is straightforward to add to the above arguments, using the isogeny defined after (2.2), to show that $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-, (\pm 3, \pm 432)\}$. The short postscript file at ftp://ftp.liv.ac.uk/pub/genus2/qderived/appendix.ps gives the proof.

We finally observe that, if we were to imitate the above approach to Conjecture 1.1, we would first take our polynomial of type $p_{1,1,1,1}$ to be of the form $x(x-1)(x-a_1)(x-a_2)$. The equations analogous to (1.1) would be of the form in $r_i(a_1, a_2) = b_i^2$, where each r_i is

https://doi.org/10.1017/S0013091599000760 Published online by Cambridge University Press

a polynomial over $\mathbb{Q}$. We would therefore need to find all $\mathbb{Q}$-rational points on a surface, and the techniques used here would not be applicable.

References

1. R. H. Buchholz and J. A. MacDougall, When Newton met Diophantus: a study of rational-derived polynomials and their extension to quadratic fields, *J. Number Theory* **81**(2) (2000), 210–233.
2. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2* (Cambridge University Press, 1996).
3. C. Chabauty, Sur les points rationels des variétés algébriques dont l'irregularité et supérieur á la dimension, *C. R. Acad. Sci. Paris Sér. I Math.* **212** (1941), 882–885.
4. Z. Djabri, E. F. Schaefer and N. P. Smart, Computing the p-Selmer group of an elliptic curve, *Trans. Am. Math. Soc.* **352** (2000), 5583–5597.
5. E. V. Flynn, A flexible method for applying Chabauty's theorem, *Compositio Math.* **105** (1997), 79–94.
6. E. V. Flynn and J. L. Wetherell, Finding rational points on bielliptic genus 2 curves, *Manuscripta Math.* **100** (1999), 519–533.
7. E. V. Flynn, B. Poonen and E. F. Schaefer, Cycles of quadratic polynomials and rational points on a genus-two curve, *Duke Math. J.* **90** (1997), 435–463.
8. E. F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, *Math. Ann.* **310** (1998), 447–471.
9. S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.* **25** (1995), 1501–1538.
10. J. H. Silverman, *The arithmetic of elliptic curves* (Springer, New York, 1986).
11. J. L. Wetherell, Bounding the number of rational points on certain curves of high rank, PhD thesis (University of California at Berkeley, 1997).