On Q-Derived Polynomials

E.V. Flynn, Mathematical Institute, University of Oxford

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. A.M.S. Classification: 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 $p_{m_1,\ldots,m_r}$ if it has r distinct roots, and each m_i is the multiplicity of the i-th 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 is shown in [1].

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

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

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.

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

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

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 $\mathcal{C}_1(\mathbb{Q})$ which 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

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

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 [7] 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 Section 2 we shall describe how to find equations for a covering collection of curves induced by this isogeny. In Section 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

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

with Jacobian J. We shall assume for simplicity that k, rk and $-rk$ are nonsquares. 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, P_2 are both $\mathbb{Q}$-rational or P_1, 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

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

respectively, generalising (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

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

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:

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

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

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

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]):

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

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

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

Then, for some i, $\{(X,Y),\infty^+\} = D_i$ in $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ and so $\mu\big(\{(X,Y),\infty^+\}\big) = [(X-\sqrt{k})(X+r\sqrt{k}),X^2-rk]=[d_i,e_i]$. If we now define

$$x = \frac{2X}{X^2-rk}, \tag{2.8}$$

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

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

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 summarise the above in the following Lemma.

Lemma 2.1. *Let $\mathcal{C}: Y^2=(X^2-k)(X^2-rk)(X^2-r^2k)$, $r,k\in\mathbb{Q}$, $k\neq 0, r\neq 0,\pm1$, 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 $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ 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 $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)=\{D_1,\dots,D_n\}$, 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*

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

□

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 $D_1, \ldots, D_n$ for $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$. Then, for each $i \in \{1, \ldots n\}$, 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 Section 1 that it is sufficient to find $\mathcal{F}_1(\mathbb{Q})$, where $\mathcal{F}_1$ is as in (1.2). We first find $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ 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 $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ is given by:*
$D_1 = \mathcal{O}, D_2 = \{(\alpha, 0), (-\alpha, 0)\}, D_3 = \{(\sqrt{-45}, 0), (-\sqrt{-45}, 0)\}, D_4 = D_2 + D_3,$
$D_5 = \{(3, 432), \infty^+\}, D_6 = D_5 + D_2, D_7 = D_5 + D_3, D_8 = D_5 + D_4,$
whose images under μ are

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

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 [6] that if for some c, we let $\theta_1, \ldots, \theta_6$ 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 ten unordered partitions of the six roots $\theta_1, \ldots, \theta_6$ of $H(X)$ into two sets of three. Applying this to $H(X) = F(X + 1)$ gives $h(X)$ of degree 10 with factors:

$$x^2 - 176x - 35456,\ x^2 + 184x - 2336,\ x^2 + 124x + 125344,$$
$$x^2 + 364x + 154624,\ x^2 + 304x + 671104,$$

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 $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$. Hence D_2, D_3, D_5 generate $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$, as required. Note that $D_1, \ldots, D_8$ are simply the 8 elements of the Boolean group $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ generated by D_2, D_3, D_5. $\square$

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 $[d_1, e_1], \ldots [d_8, e_8]$ 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 $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ for some $i \in \{1, \ldots 8\}$. 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 $|\ |_5$ 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 $|x|_5 \geq 5$; 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 $|x|_5 \leq 1$ 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 nonsquare 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 [4,8,9,10], 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 [7] as follows. First note that $5P_1$ is in the kernel of reduction mod 11, so we define

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

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

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

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 $k = 1, \ldots, 5$, 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 [7]. 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 [7] 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 equations in [7], and are as follows.

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

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 $\pm\sqrt{-45}$, $-3\pm6i$, 3 and 15. Of these, only $3, 15 \in \mathbb{Q}$. Substituting $X = 3$ into the equation of $\mathcal{C}_1$, we see that $Y^2 = (3^2+15)(3^2+45)(3^2+135) = 186624$, which has solutions $Y = \pm432$. Substituting $X = 15$ gives $Y^2 = 23328000$, which does not have a $\mathbb{Q}$-rational solution for Y. It follows that $(X, Y) = (3, \pm432)$ 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 $(X, Y) = (-3, \pm432)$ are the only two points on $\mathcal{C}_1$ corresponding to the case $i = 8$.

Having considered all cases $i = 1, \ldots, 8$, 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 $\infty^+, \infty^-, (\pm3, \pm432)$. Therefore, all affine $(X, Y_1, Y_2, Y_3) \in \mathcal{F}_1(\mathbb{Q})$ have $X = \pm3$, 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 Section 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 $\pm3, \infty$; these correspond to $a = 0, \infty, 1$, which are precisely the degenerate values of a for which $q(x)$ is not of type $p_{3,1,1}$. $\square$

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 www.maths.ox.ac.uk/~flynn/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 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 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] Buchholz, R.H. and MacDougall, J.A. *When Newton met Diophantus: A study of rational-derived polynomials and their extension to quadratic fields.* To appear in J. Number Theory.

[2] Cassels, J.W.S. and Flynn, E.V. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Cambridge University Press, 1996.

[3] Chabauty C. *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] Djabri, Z., Schaefer, E.F. and Smart, N.P. *Computing the p-Selmer group of an elliptic curve.* Manuscript (1999). To appear in Trans. Amer. Math. Soc.

[5] Flynn, E.V. *A Flexible Method for Applying Chabauty's Theorem.* Compositio Math. **105** (1997), 79–94.

[6] Flynn, E.V., Poonen, B. and Schaefer, E.F. *Cycles of quadratic polynomials and rational points on a genus-two curve.* Duke Math. J. **90** (1997), 435-463.

[7] Flynn, E.V. and Wetherell, J.L. *Finding Rational Points on Bielliptic Genus 2 Curves.* To appear in Manuscripta Math.

[8] Schaefer, E.F. *Computing a Selmer Group of a Jacobian using functions on the curve.* Math. Ann. **310** (1998), 447–471.

[9] Siksek, S. *Infinite descent on elliptic curves.* Rocky Mountain J. Math. **25 No. 4** (1995), 1501–1538.

[10] Silverman, J.H. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York (1986).

[11] Wetherell, J.L. *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD Dissertation (1997), University of California at Berkeley.