PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 12, December 2017, Pages 5179–5190
http://dx.doi.org/10.1090/proc/13677
Article electronically published on June 22, 2017

SPECIALIZATION OF GALOIS GROUPS AND INTEGRAL POINTS ON ELLIPTIC CURVES

SIMAN WONG

(Communicated by Matthew A. Papanikolas)

ABSTRACT. Let $n \neq 0, \pm 4$ be an integer. We show that the Galois group of $x^5 - 10nx^2 - 24n$ is A_5 precisely when $|n|$ appears in the purely periodic continued fraction expansion $[\,|n|, |n|, |n|, \dots\,]$ of odd positive integer powers of $(1+\sqrt{5})/2$; otherwise the Galois group is S_5. This shows that entries A002827 and A135064 of the On-Line Encyclopedia of Integer Sequences agree except for $n = 4$. The proof involves determining all integral points of certain curves of genus 1 and 2. For integral points of an elliptic curve we handle that in two ways: via a computer algebra system and by a method of Tate.

1. INTRODUCTION

Let $\phi = (1+\sqrt{5})/2$ and $\overline{\phi} = (1-\sqrt{5})/2$, so

$$n(k) := \phi^{2k-1} + \overline{\phi}^{2k-1} \tag{1.1}$$

is a positive integer for any positive integer k. Since $\phi\overline{\phi} = -1$, we have

$$\begin{aligned} \phi^{2k-1} &= n(k) - \overline{\phi}^{2k-1} \\ &= n(k) + 1/\phi^{2k-1}. \end{aligned}$$

Apply this inductively and it follows that ϕ^{2k-1} has a purely periodic continued fraction expansion $[n(k), n(k), n(k), \dots]$ from which we can easily derive the recurrence relation

$$n(k) = 3n(k-1) - n(k-2) \tag{1.2}$$

(stated without proof in [11] and attributed to Colin Baker). Here are the first few values of $n(k)$:

k	1	2	3	4	5	6	7	8	9	10
$n(k)$	1	4	11	29	76	199	521	1364	3571	9349

These $n(k)$ constitute the terms of entry A002878 of the On-Line Encyclopedia of Integer Sequences (OEIS) [11]. Brockhaus [11] notes that except for $n(k) = 4$, these terms appear to match those of A135064, which consists of all positive integers n for which the quintic

$$f_n(x) := x^5 - 10nx^2 - 24n$$

Received by the editors September 30, 2016 and, in revised form, January 13, 2017.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11J70, 11R09, 11R32, 14G05.
Key words and phrases. Elliptic curves, Galois groups, integral points, specialization.

has Galois group A_5 (the Galois group of $f_4(x)$ is dihedral of order 10). As Sloane points out in [11], if this agreement is provable we can readily provide recurrences such as (1.2), generating function, etc., for the Galois sequence A135064. In this paper we confirm this agreement.

Theorem 1.1. *Let $n \neq 0, \pm 4$ be an integer. Then the Galois group of $x^5 - 10nx^2 - 24n$ is A_5 if $|n| = n(k)$ for some positive integer $k \neq 2$; otherwise it is S_5.*

Since $f_{-n}(-x) = -f_n(x)$ and $f_0(x) = x^5$, it suffices to consider positive integer values of n. The polynomial discriminant of $f_n(x)$ is $2^{10}3^4 5^5 n^4(n^2+4)$, so $f_n(x)$ has *even* Galois group if and only if

$$n^2 + 4 = 5m^2 \tag{1.3}$$

for some integer $m > 0$. Necessarily $m \equiv n \pmod 2$, so $(n + m\sqrt{5})/2$ belongs to the ring of integers $\mathbf{Z}[\phi]$ of $\mathbf{Q}(\phi) = \mathbf{Q}(\sqrt{5})$, and upon rewriting (1.3) as $(n^2 - 5m^2)/4 = -1$ we see that (1.3) is equivalent to $(n + m\sqrt{5})/2$ being a unit in $\mathbf{Z}[\phi]$ of norm -1. Since m, n are positive, that means $(n + m\sqrt{5})/2 = \phi^{2k-1}$ for some integer $k \geq 1$, whence $n = \phi^{2k-1} + \overline{\phi}^{2k-1}$. Recalling (1.1) we see that the Galois group of $f_n(x)$ is even precisely when $|n| = n(k)$ for some $k \geq 1$. Combining this parity criterion with a special case of a celebrated theorem of Galois [3, Thm. 14.1.1] that says the Galois group of an irreducible quintic either contains A_5 or is solvable, we see that Theorem 1.1 is a consequence of the following two results.

Theorem 1.2. *The quintic $f_n(x)$ is irreducible over $\mathbf{Q}$ for all non-zero integers n.*

Theorem 1.3. *The only rational numbers n for which $f_n(x)$ is irreducible and solvable are $n = \pm 4$.*

Viewed as a $\mathbf{Z}$-polynomial in the variables x and n, the quintic $f_n(x)$ defines an affine plane curve $\mathcal{F}$ over $\mathbf{Q}$. Similarly, the equation (1.3) defines an affine conic $\mathcal{C}$ over $\mathbf{Q}$. Each of these two affine curves has a projection-to-n map, and we can take their fiber product:

$$\begin{array}{ccc} \mathcal{F}_{\mathcal{C}} & \longrightarrow & \mathcal{F} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_{\mathcal{F}}} \\ \mathcal{C} & \xrightarrow{\pi_{\mathcal{C}}} & \mathbf{A}^1 \end{array}$$

By construction, the deck transformation group of the cover π is A_5. The conic $\mathcal{C}$ has a $\mathbf{Q}$-rational point, so $\mathcal{C}$ is $\mathbf{Q}$-birational to $\mathbf{A}^1$. The Hilbert irreducibility theorem [9, Chap. 9] then implies that outside a thin set of points in $\mathcal{C}(\mathbf{Q})$, the fibers of π have A_5 Galois group. That means $f_n(x)$ has A_5 Galois group for infinitely many *rational* n. However, the number of *rational* points in $\mathrm{im}(\pi_{\mathcal{C}}) \subset \mathbf{A}^1$ of (multiplicative) height $\leq M$ is $\asymp M^{1/2}$, whereas by (1.1), the number of height $\leq M$ integers of the form $n(k)$ is $\asymp \log M$. Since the exceptional set in Hilbert irreducibility could be infinite, we cannot conclude by this argument that $f_n(x)$ has A_5 Galois group for infinitely many *integers* n. Since $f_n(x)$ is monic, to say that $f_n(x)$ has a linear factor over $\mathbf{Q}$ for an *integer* n is to say that $\mathcal{F}$ has an *integral point* (with respect to the model $f_n(x) = 0$ for $\mathcal{F}$). More generally, the exceptional n in Hilbert irreducibility correspond to rational points on intermediate covers of

the Galois closure of the extension of the rational function field $\mathbf{Q}(n)$ defined by $f_n(x)$ (cf. [7]). Estimating the genus of these intermediate covers and applying Siegel's theorem, we can quickly deduce that Theorem 1.1 holds for all but finitely many integers n. But this would not allow us to determine the exceptional values. Instead we proceed by explicitly constructing these intermediate covers and then analyzing their arithmetic.

The exceptional values in Theorem 1.3 are parameterized by a genus 2 curve that double covers an elliptic curve over $\mathbf{Q}$ with Mordell-Weil rank 0, so we can determine these exceptional values very easily. The proof of Theorem 1.2 involves finding all integral points of an elliptic curve over $\mathbf{Q}$ with Mordell-Weil rank 1. We handle that in two ways: via a computer algebra system and by a method of Tate (cf. section 3).

Remark 1.4. It is well known that a generic integer polynomial of degree n has S_n Galois group, and we expect that a generic *even* integer polynomial of degree n to have A_n Galois group. However, in practice proving these statements for a given one-parameter family of integer polynomials of fixed degree is a non-trivial task: Since there are degree $n > 3$ integer polynomials with Galois groups strictly smaller than A_n and S_n, that means the aforementioned statements about generic Galois groups have a non-trivial exceptional set, and for n sufficiently large it is conceivable that we can find a one-parameter family of degree n polynomials that lies entirely inside the exceptional set. For a discussion about these exceptional sets from an algebro-geometric point of view, see [7].

Remark 1.5. We are not aware of an exposition of Tate's method for finding integral points in the literature besides an exercise in [12]. We hope that our argument here will help popularize this useful technique.

2. Sextic resolvent

Proof of Theorem 1.3. The Galois group of an irreducible quintic either contains A_5 or is a subgroup of $\mathbf{Z}/5 \rtimes \mathbf{Z}/4$ [3, Thm. 14.1.1]. If the quintic $f_n(x)$ is irreducible over $\mathbf{Q}$, by [5, Thm. 1] it is solvable if and only if the associated sextic resolvent

$$C_{\text{res}}: \quad x^6 - 12000n^2x^4 - 20000n^4x^3 + 36000000n^4x^2 \\ -4800000(29n^2+216)n^4x + 10^8n^8 = 0 \tag{2.1}$$

has a rational root α_0, in which case α_0 would have to be an integer since the sextic (2.1) is monic and has integer coefficients. We set

$$n_1 = n/4, \;\; \alpha_1 = \alpha_0/80 \tag{2.2}$$

and turn this into

$$C_2 : 25\,n_1^8 - 174\,\alpha_1\,n_1^6 - 10\,\alpha_1^3\,n_1^4 + 225\,\alpha_1^2\,n_1^4 - 81\,\alpha_1\,n_1^4 - 30\,\alpha_1^4\,n_1^2 + \alpha_1^6 = 0. \tag{2.3}$$

This equation turns out to define a smooth projective curve of genus 2; cf. Remark 2.1 below. In general it is not easy to determine the rational points of a genus 2 curve (C_2 is not in hyperelliptic form, so e.g. [8] is not immediately applicable). But note that

$$\delta : (\alpha_1, n_1) \mapsto (\alpha_1, n_1^2)$$

defines a non-constant rational map from C_2 to

$$C_1 : 25\,n_2^4 - 174\,\alpha_2\,n_2^3 - 10\,\alpha_2^3\,n_2^2 + 225\,\alpha_2^2\,n_2^2 - 81\,\alpha_2\,n_2^2 - 30\,\alpha_2^4\,n_2 + \alpha_2^6 = 0. \tag{2.4}$$

So we can first look for rational points on[1] C_1 and then pull them back to C_2 (note that this approach does not presuppose the knowledge that C_2 defines a genus 2 curve).

Using the `Weierstrassform` command in the computer algebra system `Maple`, we find that

(2.5)
$$\alpha_2 = \frac{5(S-2)^2(8T+S^2+22S+29)}{(S-7)^4},$$
$$n_2 = \frac{(S-2)(15S^3T+235S^2T+505ST-195T+S^5+95S^4+510S^3+3380S^2-635S-1007)}{(S-7)^6}$$

defines a $\mathbf{Q}$-rational *birational* map from the elliptic curve

$$E_1 : T^2+ST+T = S^3+S^2+35S-28$$

to C_1. This is the elliptic curve $15A4$ in the Cremona table [4]. Its $\mathbf{Q}$-rational points, besides the point at infinity $\mathcal{O}$, are

$$(S,T): \ (2,6),(7,-29),(32,171),(3/4,-7/8),(32,-204),(7,21),(2,-9).$$

The birational map (2.5) is not defined at $S=7$. Excluding the points $\mathcal{O},(7,-29)$ and $(7,21)$, by (2.5) and (2.2) the remaining points of $E_1(\mathbf{Q})$ correspond to the following points on C_1:

$$(\alpha_2,n_2): \ (0,0),(36,864/25),(1/5,-1/125),(36/26,54/625),(0,0).$$

None of the non-zero n_2 values above is a square in $\mathbf{Q}$, so none of these points on $C_1(\mathbf{Q})$ with $n_2=0$ is the image of a point in $C_2(\mathbf{Q})$. And if $n_2=0$, then $n=0$, in which case $f_n(x)$ is reducible.

Finally, we look for rational points on $C_1(\mathbf{Q})$ that map to $\mathcal{O}$. Equivalently, we are looking for those points $P\in C_1(\mathbf{Q})$ at which the inverse of the birational map (2.5) is not defined. The `Weierstrassform` command also provides an explicit formula for this inverse birational map; it is of the form

$$S=\frac{S_1(\alpha_2,n_2)}{4(\alpha_2-5)^2(4\alpha_2^2+4\alpha_2-9)}, \ T=\frac{T_1(\alpha_2,n_2)}{4(\alpha_2-5)^2(4\alpha_2^2+4\alpha_2-9)},$$

where S_1,T_1 are (complicated) $\mathbf{Q}$-polynomials in n_2 and α_2. The only $\mathbf{Q}$-rational solution to (3.3) with $\alpha_2=5$ is $n=1$. So the only possible point in $C_1(\mathbf{Q})$ whose image under this inverse birational map is[2] $\mathcal{O}$ is $(\alpha_2,n_2)=(5,1)$. Note that $(\alpha_2,n_2)=(5,1)$ is the image of $(x,n)=(400,\pm4)\in C_{\mathrm{res}}(\mathbf{Q})$ under (2.2) and δ, and we check that $f_n(x)$ is $\mathbf{Q}$-irreducible for $n=\pm4$, so we are done. □

Remark 2.1. Using `Maple`, we find that C_2 is $\mathbf{Q}$-birational to the genus 2 hyperelliptic curve

$$C_2': \ Y^2=\tfrac{5}{12}X^5+\tfrac{51}{4}X^4+1416X^3-13374X^2+40500X-40500. \tag{2.6}$$

[1] An elementary congruence argument shows that if (α_0,n) is an integral point on (2.1), then (α_1,n_1) is an integral point on (2.3). Thus it suffices to focus only on the *integral points* of C_1. But finding integral points on a genus 2 curve in general is not easy, and as we will see below, there is no need to impose this restriction. Instead, we use the transformation (2.2) to simplify the output of the `Maple` computations.

[2] In principle we should check that $(5,1)$ is actually a pole of this inverse birational map; that entails checking that neither S_1 nor T_1 vanishes at $(5,1)$. That is the case, by making use of the actual formula for S_1 and T_1. But this is not necessary for the purpose of determining a finite set of points that *could* go to $\mathcal{O}$.

The existence of the non-constant map $\delta : C_2 \to C_1$ means that the Jacobian of C_2 (and hence of C_2') is $\mathbf{Q}$-isogenous to the product of $E_1/\mathbf{Q}$ with another elliptic curve over $\mathbf{Q}$. While we do not need this for the rest of the paper, it is easy to determine this complementary factor, so we sketch the steps here. The following discussion is inspired by [1, §14.1].

The change of variables $X = 6/(6U+1)$ and $Y = 216V/(6U+1)^3$ takes (2.6) to

$$C_2'' : \ V^2 = -40500U^6 + 3501U^4 - 102U^2 + 1.$$

Then the map $(U, W) \mapsto (U^2, W)$ takes C_2'' to

$$\mathcal{E}_1 : Y^2 = -40500X^3 + 3501X^2 - 102X + 1,$$

while $(U, W) \mapsto (1/U^2, W/U^3)$ sends C_2'' to

$$\mathcal{E}_2 : Y^2 = X^3 - 102X^2 + 3501X^2 - 40500.$$

We readily check that $\mathcal{E}_1$ is $\mathbf{Q}$-isomorphic to our earlier elliptic curve E_1 and that $\mathcal{E}_2$ is $\mathbf{Q}$-isomorphic to the elliptic curve 180A2 in the Cremona table, so $\mathcal{E}_2$ is the desired complementary factor. Each of these elliptic curves has a finite Mordell-Weil group over $\mathbf{Q}$.

3. Irreducibility

Proof of Theorem 1.2. Since $f_n(x)$ is quintic and monic, by Gauss's lemma it is reducible over $\mathbf{Q}$ if and only if it has a monic factor over $\mathbf{Z}$ of degree 1 or 2. We consider these two cases separately.

First, suppose $f_n(x)$ has a monic linear factor over $\mathbf{Z}$; i.e. suppose it has an integer root α. Then $n = \alpha^5/(10\alpha^2 + 24)$. Both n and α are integers, so the denominator $10\alpha^2 + 24$ is not divisible by any prime > 3. If $3|(10\alpha^2 + 24)$, then $3||(10\alpha^2 + 24)$. Now, suppose $2|(10\alpha^2 + 24)$. Then either $2^2|\alpha$, in which case $2^3||(10\alpha^2 + 24)$, or $2||\alpha$, in which case $2^5||\alpha^5$ so $2^i||(10\alpha^2 + 24)$ with $3 \le i \le 5$. Clearly $10\alpha^2 + 24$ is positive, so

$$10\alpha^2 + 24 = 2^i 3^j \quad \text{with } 3 \le i \le 5 \text{ and } 0 \le j \le 1.$$

We check that the only solution is $(i, j) = (3, 1)$, corresponding to $\alpha = n = 0$. Of course $f_0(x) = x^5$ is reducible. Thus $f_n(x)$ has no $\mathbf{Q}$-linear factor for any non-zero integer n.

Now, suppose $f_n(x)$ has a $\mathbf{Q}$-irreducible, monic quadratic factor. That means $f_n(\frac{a+b\sqrt{d}}{2})$ and $f_n(\frac{a-b\sqrt{d}}{2})$ are zero for some $a, b, d \in \mathbf{Z}$ with $b \neq 0$ and d not a square. Then both $f_n(\frac{a+b\sqrt{d}}{2}) \pm f_n(\frac{a-b\sqrt{d}}{2})$ are zero, whence

$$80b^2dn + 80a^2n + 768n - 5ab^4d^2 - 10a^3b^2d - a^5 = 0, \tag{3.1}$$

$$b(160an - b^4d^2 - 10a^2b^2d - 5a^4) = 0. \tag{3.2}$$

Eliminating d from the two equalities we get

$$1024b^8(1000an^3 + (-100a^4 + 1680a^2 - 576)n^2 + (264a^5 - 10a^7)n + a^{10}) = 0.$$

Recall that $b \neq 0$, so

$$1000an^3 + (-100a^4 + 1680a^2 - 576)n^2 + (264a^5 - 10a^7)n + a^{10} = 0. \tag{3.3}$$

For future reference, note that any integral point (a, n) on (3.3) must satisfy

$$a \equiv 0 \pmod 4. \tag{3.4}$$

Using `Maple`, we find that (3.3) is $\mathbf{Q}$-birational to the elliptic curve

$$y^2 + x^3 - \frac{11620583473152}{9765625}x + \frac{10482448033680195584}{30517578125} = 0.$$

The change of variables $x \mapsto -(992/125)^2 X, y \mapsto (992/125)^3 Y$ then turns this into

$$E_2 : Y^2 = X^3 - 300X - 1375. \tag{3.5}$$

Denote by φ_1 the birational map taking (3.5) to (3.3). Its a-coordinate is given by

$$a(X,Y) = \frac{X^3 - 30X^2 + 2325X + 26000 - Y(31X + 2120)}{(X - 20)(X^2 + 115X + 4150)}. \tag{3.6}$$

The equation (3.5) defines the elliptic curve 900E1 in the Cremona table [4]. Its Mordell-Weil group over $\mathbf{Q}$ is $\mathbf{Z} \times (\mathbf{Z}/2)$. So, unlike the proof of Theorem 1.3, additional work is needed to determine the integral points of (3.3). For future reference, note that although E_2 is $\mathbf{Q}$-birational to (3.3) and $E_2(\mathbf{Q})$ is infinite, it does not automatically mean that $f_n(x)$ has a $\mathbf{Q}$-irreducible quadratic factor for infinitely many $n \in \mathbf{Q}$; cf. Remark 3.2 below.

By [12, Cor. 9.3.2.2], there exists a finite set of primes S such that the set of points $(X,Y) \in E_2(\mathbf{Q})$ with $a(X,Y) \in \mathbf{Z}$ is contained in the set of S-integral points of $E_2(\mathbf{Q})$. To determine all n for which $f_n(x)$ has a monic quadratic factor over $\mathbf{Q}$, we will make explicit the argument[3] in [12, Cor. 9.3.2.2].

First, note that $P_1 := (20, -25)$ is a rational point of $E_2(\mathbf{Q})$ and that the numerator of $a(X,Y)$ does not vanish at P_1, so $a(X,Y)$ has a pole at P_1. It is interesting to note that $(20, 25)$ is also a rational point on $E_2(\mathbf{Q})$, but the numerator of $a(X,Y)$ vanishes at this point, so $(20, 25)$ is not a pole of $a(X,Y)$.

Apply the algorithm of Nagell ([10], cf. [13]) and we find that

$$(X_1, Y_1) \mapsto \Big(\frac{10(710Y_1 + 264X_1^2 + 545X_1 - 134250)}{25Y_1 + 132X_1^2 - 5730X_1 + 61175}, \frac{25(4777Y_1 + 132X_1^2 + 11010X_1 + 85275)}{-25Y_1 - 132X_1^2 + 5730X_1 - 61175} \Big)$$

defines a $\mathbf{Q}$-rational morphism φ_2 from[4]

$$Y_1^2 = X_1^3 - 300X_1 - 1375 \tag{3.7}$$

to E_2, taking the origin[5] of (3.7) to $P_1 \in E_2(\mathbf{Q})$. Using the explicit formula for φ_2 and $a(X,Y)$, we find that the composition function $a_1 := a \circ \varphi_2$ is equal to

$$a_1(X_1, Y_1) = 2Y_1/(5X_1 - 50).$$

Squaring both sides and using the relation (3.7), we get

$$X_1^3 - \tfrac{25}{4} a_1(X_1,Y_1) X_1^2 + X_1(125a_1(X_1,Y_1) - 300) - (625a_1(X_1,Y_1) + 1375) = 0. \tag{3.8}$$

Consequently, if (X_1, Y_1) is a $\mathbf{Q}$-rational point on (3.7) such that $a_1(X_1, Y_1) \in \mathbf{Z}$, then X_1 would satisfy a monic polynomial with coefficients that are 2-integral.

[3]We can also apply the powerful algorithm of Stroeker and Tzanakis [14] for finding all integer solutions of a general genus 1 equation. There are already many examples in the literature that take the linear forms in elliptic logarithms approach, and the delicate diophantine estimates involved make it challenging to give a self-contained exposition. Tate's method, when applicable, only involves basic arithmetic and geometry of the curve. Thus we opt for this 'classical' approach here.

[4]The reason for introducing the equation (3.7) — which of course is the same as (3.5) — is to help distinguish the (X_1, Y_1)-coordinates from the (X, Y)-coordinates.

[5]Since φ_2 does not preserve the origin, it is not an isogeny; in particular, it is not an endomorphism of E_2 (which does not have complex multiplication).

Furthermore, recall that we have the divisibility condition (3.4), so in fact X_1 is an integer, and hence (X_1, Y_1) is an integral point.

Claim. The integral points on (3.7) are $(-14, \pm 9), (-10, \pm 25), (-5, 0), (20, \pm 25)$, $(40, \pm 225)$ and $(284, \pm 4777)$.

Assuming this statement for now, we can then compute the values of a_1 at each of these points and then determine those rational n so that $(a_1, n) \in C_{\mathrm{res}}(\mathbf{Q})$. Note that if (X_1, Y_1) is integral, then so is $(X_1, -Y_1)$, and $a_1(X_1, -Y_1) = -a_1(X_1, Y_1)$. Since (a, n) is a solution to (3.3) if and only if $(-a, -n)$ is a solution, it suffices to work with just one of $(X_1, \pm Y_1)$. Here are the values of (a_1, n) for these integral points:

(X_1, Y_1)	$(-14, 9)$	$(-10, 25)$	$(-5, 0)$	$(20, 25)$	$(40, 225)$	$(284, 4777)$
$a_1(X_1, Y_1)$	$-3/20$	$-1/2$	0	1	3	$\frac{17 \cdot 281}{5 \cdot 137}$
n	$-3/80000$	$-1/16$	0	$\frac{-1}{2}, \frac{-1}{250}$	$-3/2$	$\frac{-281^5}{2 \cdot 5^4 \cdot 17 \cdot 137^3}$

It follows from this calculation that $(a, n) = (0, 0)$ is the only integral point of (3.3) at which the birational maps φ_1 and φ_2 are defined. To complete the proof of Theorem 1.2, it remains to consider those integral points (a, n) on (3.3) at which φ_1 and φ_2 are not defined.

We begin with φ_1. By `Maple`, the inverse birational map of φ_1 is given by

$$X = \frac{F(a, n)}{a^5(a-1)(a+1)^2}, \; Y = \frac{G(a, n)}{a^5(a-1)(a+1)^3}$$

for some $\mathbf{Q}$-polynomials F, G in a, n. Thus the only $\mathbf{Q}$-rational points on (3.3) not in the image of φ_1 are $(a, n) \in \{(1, -1/2), (1, -1/250), (0, 0)\}$. In particular, none of these correspond to integer n values. Next, we turn to φ_2. The inverse to φ_2 is

$$(X, Y) \mapsto \Big(-\frac{10(2Y + 31X + 750)}{335 - Y - 18X}, \; \frac{25(Y^2 - 852X^2 - 9554Y + 600X + 89325)}{(335 - Y - 18X)^2} \Big).$$

Thus the only integral points not in the image of φ_2 are from those points (X, Y) on $E_2(\mathbf{Q})$ with $335 - Y - 18X = 0$. The only such points are $(20, \pm 25)$ and $(284, \pm 4777)$. Among these four points, the function $a(X, Y)$ is defined and integral only for $(284, 4777)$. We check that $a(284, 4777) = -1$, and the corresponding n values are $1/2$ and $1/250$, which are not integral. Combine everything and it follows that $f_n(x)$ is $\mathbf{Q}$-irreducible for all integers $n \neq 0$.

It remains to verify the Claim. Each of the computer algebra systems `Magma` and `Sage` has independent implementation of the standard algorithms for computing S-integral points on elliptic curves. Using these packages it took less than one second of CPU time to verify the Claim. Alternatively, note that the curve (3.7) has Mordell-Weil rank 1. For such curves we can often apply a method of Tate to find all of its integral points; cf. [12, Exer. 9.12, 9.13]. We now explain how to do that. The following exercise provides the key tool [12, Exer. 9.12].

Lemma 3.1. *Let $\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be the Weierstrass equation of an elliptic curve over $\mathbf{Q}$ with $a_i \in \mathbf{Z}$. Let $P \in \mathcal{E}(\mathbf{Q})$ be a point of infinite order. If the x-coordinate $x([m]P)$ is an integer for some integer $m \geq 1$, then $x(P)$ is an integer.* □

We now return to our specific elliptic curve (3.7). According to the Cremona table, its Mordell-Weil group over $\mathbf{Q}$ is generated by the non-torsion point $Q_1 = (-10, 25)$ and the 2-torsion point $Q_0 = (-5, 0)$.

Let P be an integer point on (3.7). First, suppose $P = [m]Q_1$ for some integer m. Replacing P by $-P$ if necessary, we can assume that $m \geq 1$. Write $m = 2^c m_1$ with $c \geq 0$ and m_1 odd. Lemma 3.1 says that Q_1 is also integral. Since m_1 is odd and Q_1 is not in the identity component of (3.7), $[m_1]Q_1$ is also not in the identity component of (3.7). The roots of $x^3 - 300x - 1375$ are $-14.27, -5$, and 19.27, so the x-coordinate of any integral point in the non-identity component lies between -14 and -5. We check that

$$[\pm 1]Q_1 = (-10, \pm 25), \;\; Q_0 = (-5, 0), \;\; [\pm 2]Q_1 + Q_0 = (-14, \mp 9)$$

are the only such points. It remains to find all $c \geq 1$ so that $[2^c]$ multiples of these points are also integral.

From the duplication law we see that for any point R on (3.7),

$$x([2]R) = \frac{9(x(R)^2 - 100)^2}{4y(R)^2} - 2x(R). \tag{3.9}$$

If $[2]R$ is integral, then Lemma 3.1 says that R is also integral, and (3.9) implies that the integer $y(R)$ must divide the integer $x(R)^2 - 100$, whence $x(R)^3 \equiv 100x(R) \pmod{y(R)}$. Substituting this back into (3.7) we see that

$$\begin{array}{rcll} 0 & \equiv & y(R)^2 & \pmod{y(R)} \\ & \equiv & x(R)^3 - 300x(R) - 1375 & \pmod{y(R)} \\ & \equiv & -25\,(\,8x(R) + 55\,) & \pmod{y(R)}. \end{array}$$

In particular,

$$y(R)^2 \leq 625(8x(R) + 55)^2. \tag{3.10}$$

On the other hand,

$$y(R)^2 = |x(R)^3 - 300x(R) - 1375| \geq |x(R)|^3 - 300|x(R)| - 1375.$$

Combine the two inequalities and it follows that

$$x(R) \leq 40013.$$

We already found all integral points on the non-identity component, so we can assume that R is on the identity components, whence

$$x(R) > 19.$$

We can now perform a brute force search to find all such integral points. In the end we find that the only multiples of Q_1 that are integral are

$$[\pm 1]Q_1, \;\; [\pm 2]Q_1 = (20, \mp 25), \;\; [\pm 4]Q_1 = (284, \pm 4777).$$

Next, suppose P is not a multiple of Q_1, so $P = [m]Q_1 + Q_0$ for some integer m. Using the addition law, we check that for any point R on (3.7),

$$x(R + Q_0) = \frac{y(R)^2}{(x(R) + 5)^2} - x(R) + 5. \tag{3.11}$$

Suppose R is in fact a $\mathbf{Q}$-rational point, and let p be a prime that divides the denominator of $x(R)$. From (3.7) it then follows that $p^{2i} || x(R)$ and $p^{3i} || y(R)$ for some integer $i > 0$. Recalling (3.11) it follows that if $P = [m]Q_1 + Q_0$ is integral,

then $[m]Q_1$ is also integral. Apply the earlier argument and we see that the only integral points of the form $P = [m]Q_1 + Q_0$ are

$$[\pm 1]Q_1 + Q_0 = (40, \pm 225), \ \ [\pm 2]Q_1 + Q_0 = (-14, \mp 9).$$

Combining these two cases we recover the claim. This completes the proof of Theorem 1.2. □

Remark 3.2. As a sanity check, here are the **Q**-rational factorizations of $f_n(x)$ for each of the n values corresponding to the integral points on (3.7) (for the points $(-1, \frac{1}{2}), (-1, \frac{1}{250})$ found at the end of the proof, the factorization of $f_n(x)$ is already given by the table below since $f_{-n}(-a) = -f_n(a)$):

a	n	$f_n(x)$
$-3/20$	$-3/8000$	$\frac{1}{2^6 5^4}(100\,x^2 + 15\,x + 6)(400\,x^3 - 60\,x^2 - 15\,x + 6)$
$-1/2$	$-1/16$	$(2\,x^2 + x + 2)(4\,x^3 - 2\,x^2 - 3\,x + 6)/8$
0	0	x^5
1	$-1/2$	$(x + 2)(x^4 - 2x^3 + 4x^2 - 3x + 6)$
1	$-1/250$	$\frac{1}{5^3}(5\,x^2 + 5\,x + 2)(25\,x^3 - 25\,x^2 + 15\,x - 6)$
3	$-3/2$	$(x^2 - 3x + 6)(x^3 + 3x^2 + 3x + 6)$
$\frac{17\cdot 281}{5\cdot 137}$	$\frac{-281^5}{2\cdot 5^4\cdot 17\cdot 137^3}$	$\frac{1}{5^4\cdot 17\cdot 137^3}(3425\,x^2 - 23885\,x + 157922)$ $\times(7976825\,x^3 + 55628165\,x^2 + 20135055\,x + 133128246)$

Note that the points $(0, 0), (1, -1/2)$ (as well as $(-1, 1/2)$, as we explained earlier) do not give rise to **Q**-irreducible quadratic factors of $f_n(x)$. This is not an error: Starting with a quadratic root $\frac{a+b\sqrt{d}}{2}$ of $f_n(x)$, we arrive at the equation (3.3) by eliminating d from (3.1) and (3.2). Thus **Q**-irreducible quadratic factors of $f_n(x)$ give rise to **Q**-rational points on (3.3), but the converse need not be true. More precisely, if we subtract (3.1) from $5a$ times (3.2), we get

$$d \times 5b^2(2n + a^3) = 3(30a^2n - 32n - a^5). \tag{3.12}$$

So every solution (a, n) to (3.3) does give rise to a solution to (3.12) provided that $2n + a^3 \neq 0$ (we can simply set $b = 1$). This excludes precisely the points $(0, 0), (1, -1/2), (-1, 1/2)$ on (3.3). However, we still cannot conclude that all remaining rational solutions to (3.3) give rise to a **Q**-irreducible quadratic factor of $f_n(x)$ since we need d to be *not* a perfect square in **Q**. To find these exceptional solutions, we eliminate n from (3.3) and

$$5z^2(2n + a^3) = 3(30a^2n - 32n - a^5)$$

and we end up with

$$\begin{aligned} C_6 : {} & 16000a^4z^6 - 32000a^2z^6 + 16000z^6 + 26800a^6z^4 - 18800a^4z^4 \\ & -161600a^2z^4 + 153600z^4 + 12880a^8z^2 + 70600a^6z^2 - 715520a^4z^2 \\ & +1536000a^2z^2 + 1911a^{10} + 35016a^8 - 321600a^6 + 768000a^4 = 0. \end{aligned}$$

Using `Maple`, we check that C_6 has genus 6. In particular, all but finitely many rational points on (3.3) give rise to **Q**-irreducible quadratic factors of $f_n(x)$.

Note that $(a,z) \mapsto (a,z^2)$ defines a rational map from C_6 to

$$\begin{aligned}\mathcal{E}' : 16000a^4Z^3 - 32000a^2Z^3 + 16000Z^3 + 26800a^6Z^2 - 18800a^4Z^2 \\ -161600a^2Z^2 + 153600Z^2 + 12880a^8Z + 70600a^6Z - 715520a^4Z \\ +1536000a^2Z + 1911a^{10} + 35016a^8 - 321600a^6 + 768000a^4 = 0.\end{aligned}$$

Using `Maple`, we find that $\mathcal{E}'$ is $\mathbf{Q}$-birational to E_2, which as we saw earlier has Mordell-Weil rank 1 over $\mathbf{Q}$. It seems difficult to recover the finitely many rational points on C_6 via $\mathcal{E}'$. We also have a rational map $(a,z) \mapsto (a^2,z)$ sending C_6 to a curve X_3 of genus 3 and a rational map $(a,z) \mapsto (a^2,z^2)$ sending C_6 to a curve of genus 0 with a $\mathbf{Q}$-rational point. Again we do not know how to exploit these two maps to determine the rational points of C_6.

Appendix: Continued fraction expansion of powers of ϕ

In this appendix we prove the recurrence relation (1.2). This relation is not used anywhere else in the paper; we include the elementary argument for completeness.

For any integer $\ell \geq 1$, define the integer

$$n_1(\ell) := \begin{cases} \phi^\ell + \overline{\phi}^\ell & \text{if } \ell \text{ is odd,} \\ \phi^\ell + \overline{\phi}^\ell - 1 & \text{if } \ell \text{ is even.} \end{cases} \tag{A.1}$$

Lemma A.1. *For any positive integer ℓ, the continued fraction expansion of ϕ^ℓ is given by*

$$\phi^\ell = \begin{cases} [\,n_1(\ell), n_1(\ell), n_1(\ell), \ldots] & \textit{if } \ell \textit{ is odd,} \\ [\,n_1(\ell), 1, n_1(\ell)-1, 1, n_1(\ell)-1, 1, \ldots] & \textit{if } \ell \textit{ is even.} \end{cases}$$

Proof. By definition, the first term of the continued fraction of the irrational number ϕ^ℓ is the largest integer less than ϕ^ℓ. Since $\phi^\ell + \overline{\phi}^\ell$ is an integer and $-1 < \overline{\phi} < 0$, this first term is exactly $n_1(\ell)$.

First, suppose ℓ is odd. Then $\phi^\ell \overline{\phi}^\ell = -1$, whence by (A.1),

$$\phi^\ell = n_1(\ell) + (-\overline{\phi}^\ell) = n_1(\ell) + 1/\phi^\ell.$$

Appling this inductively we get the lemma for odd $\ell \geq 1$. Next, suppose $\ell \geq 2$ is even. Then $\phi^\ell \overline{\phi}^\ell = 1$, whence by (A.1),

$$\phi^\ell = n_1(\ell) + 1 - \overline{\phi}^\ell = n_1(\ell) + \frac{1}{1 - \overline{\phi}^\ell} = n_1(\ell) + \frac{1}{\frac{\phi^\ell}{\phi^\ell - 1}} = n_1(\ell) + \frac{1}{1 + \frac{1}{\phi^\ell - 1}}.$$

Again by (A.1),

$$\begin{aligned}\phi^\ell - 1 &= (n_1(\ell) - 1) + (1 - \overline{\phi}^\ell) = n_1(\ell) - 1 + \frac{1}{1 - \overline{\phi}^\ell} = n_1(\ell) - 1 + \frac{1}{\frac{\phi^\ell}{\phi^\ell - 1}} \\ &= n_1(\ell) - 1 + \frac{1}{1 + \frac{1}{\phi^\ell - 1}}.\end{aligned}$$

Combine these two and we get the lemma for even $\ell \geq 2$. □

We now give the recursion for $n_1(\ell)$. For odd ℓ this is stated without proof in [11] and is attributed to Colin Baker.

Lemma A.2. *Denote by $n_1(\ell)$ the first term of the continued fraction expansion of ϕ^ℓ. Then we have the linear recurrence relation*

$$n_1(\ell+4) = \begin{cases} 3n_1(\ell+2) - n_1(\ell) & \text{if } \ell \geq 1 \text{ is odd,} \\ 3n_1(\ell+2) - n_1(\ell) + 1 & \text{if } \ell \geq 2 \text{ is even.} \end{cases}$$

Proof. By standard linear algebra argument (or direct computation) we find that

$$\begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \phi^2 & \overline{\phi}^2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \phi^2 & 0 \\ 0 & \overline{\phi}^2 \end{pmatrix} \begin{pmatrix} \phi^2 & \overline{\phi}^2 \\ 1 & 1 \end{pmatrix}^{-1}.$$

On both sides of this equality, multiply on the right of the matrix by the vector

$$\begin{pmatrix} n_1(2k+1) \\ n_1(2k-1) \end{pmatrix} = \begin{pmatrix} \phi^{2k+1} + \overline{\phi}^{2k+1} \\ \phi^{2k-1} + \overline{\phi}^{2k-1} \end{pmatrix},$$

and the lemma follows by induction for odd positive $\ell = 2k-1$. Multiply instead by the vector

$$\begin{pmatrix} n_1(2k+2) \\ n_1(2k) \end{pmatrix} = \begin{pmatrix} \phi^{2k+2} + \overline{\phi}^{2k+2} - 1 \\ \phi^{2k} + \overline{\phi}^{2k} - 1 \end{pmatrix}$$

and we get the lemma for even $\ell = 2k \geq 2$. □

Note added in proof. After we submitted the paper, we found using `Magma` that the genus 3 curve X_3 mentioned at the end of Remark 3.2 is $\mathbf{Q}$-birational to the smooth projective hyperelliptic curve Y_3 given by the affine model

$$AY_3 : y^2 = -6x(x^2+x-1)(x^2+x+4)(40x^3 - 71x^2 + 49x - 39).$$

Moreover, under the Generalized Riemann Hypothesis the 2-Selmer group of $J_3(\mathbf{Q})$, the Jacobian of Y_3 over $\mathbf{Q}$, is $(\mathbf{Z}/2)^4$, and the Mordell-Weil rank of $J_3(\mathbf{Q})$ is ≤ 2, so the method of Chabauty and Coleman [2] is applicable. We check that Y_3 has good reduction at 7 and that $\#Y_3(\mathbf{F}_7) = 496$, so $\#Y_3(\mathbf{Q}) \leq 496 + 6 - 2 = 500$. Unwind the birational map from X_3 to Y_3 and we get a conditional bound for $\#X_3(\mathbf{Q})$, and hence for $\#C_6(\mathbf{Q})$. However, this argument does not explicitly determine the rational points of C_6, so we still do not know the set of *rational* n for which $f_n(x)$ is reducible over $\mathbf{Q}$. That said, the conditional bound $\#Y_3(\mathbf{Q}) \leq 500$ is likely to be far from optimal; the `Magma` command `Points(AY3: Bound:=500000)` finds just one rational point $x = y = 0$ on Y_3.

Acknowledgement

The author would like to thank Professor Gunnells for bringing this question to his attention [6], and Professors Hajir and Silverman for useful discussions.

References

[1] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090

[2] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103

[3] David A. Cox, *Galois theory*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2012. MR2919975

[4] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992. MR1201151

[5] D. S. Dummit, *Solving solvable quintics*, Math. Comp. **57** (1991), no. 195, 387–401, DOI 10.2307/2938681. MR1079014
[6] P. Gunnells, email communication, February 19, 2015.
[7] Farshid Hajir and Siman Wong, *Specializations of one-parameter families of polynomials* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **56** (2006), no. 4, 1127–1163. MR2266886
[8] Homero R. Gallegos-Ruiz, *S-integral points on hyperelliptic curves*, Int. J. Number Theory **7** (2011), no. 3, 803–824, DOI 10.1142/S1793042111004435. MR2805581
[9] Serge Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983. MR715605
[10] Trygve Nagell, *Sur les propriétés arithmétiques des cubiques planes du premier genre* (French), Acta Math. **52** (1929), no. 1, 93–126, DOI 10.1007/BF02547402. MR1555271
[11] On-line Encyclopedia of Integer Sequences, entry #A135064. `https://oeis.org/A135064`
[12] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210
[13] Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR3363545
[14] R. J. Stroeker and N. Tzanakis, *Computing all integer solutions of a genus 1 equation*, Math. Comp. **72** (2003), no. 244, 1917–1933, DOI 10.1090/S0025-5718-03-01497-2. MR1986812

Department of Mathematics and Statistics, University of Massachusetts, Amherst, Massachusetts 01003-9305

E-mail address: `siman@math.umass.edu`