J. Aust. Math. Soc. **108** (2020), 245–261
doi:10.1017/S1446788718000320

SMOOTH VALUES OF POLYNOMIALS

J. W. BOBER✉, D. FRETWELL, G. MARTIN and T. D. WOOLEY

(Received 5 October 2017; accepted 12 September 2018; first published online 1 February 2019)

Communicated by I. E. Shparlinski

Abstract

Given $f \in \mathbb{Z}[t]$ of positive degree, we investigate the existence of auxiliary polynomials $g \in \mathbb{Z}[t]$ for which $f(g(t))$ factors as a product of polynomials of small relative degree. One consequence of this work shows that for any quadratic polynomial $f \in \mathbb{Z}[t]$ and any $\varepsilon > 0$, there are infinitely many $n \in \mathbb{N}$ for which the largest prime factor of $f(n)$ is no larger than n^{ε}.

2010 *Mathematics subject classification*: primary 11N32; secondary 11N25, 12E05.

Keywords and phrases: Smooth numbers, polynomials, small degree irreducible factors.

1. Introduction

In this paper we study the smoothness of polynomials. Recall that an integer is called *y-smooth* (or *y-friable*) when each of its prime divisors is less than or equal to y. Given a polynomial $f \in \mathbb{Z}[t]$ of positive degree and a nonnegative number θ, we say that f *admits smoothness* θ when there are infinitely many integers n for which the polynomial value $N = |f(n)|$ is N^{θ}-smooth. Similarly, we say that f *admits polysmoothness* θ when there exists a nonconstant polynomial $g \in \mathbb{Z}[t]$ having the property that each irreducible factor of $f(g(t))$ has degree at most $\theta(\deg f)(\deg g)$. In the latter circumstances, by inspecting the values $f(g(m))$ for large integers m, it is apparent that when f admits polysmoothness θ, then it admits smoothness η for any $\eta > \theta$. Motivated by the widely held conjecture that for each $\varepsilon > 0$, every $f \in \mathbb{Z}[t]$ of positive degree should admit smoothness ε, the latter considerations prompt the following question.

QUESTION. *Given $f \in \mathbb{Z}[t]$ of positive degree d, is it the case that f admits polysmoothness ε for every $\varepsilon > 0$? In other words, for each $\varepsilon > 0$, does there exist*

The third author's work is partially supported by a National Sciences and Engineering Research Council of Canada Discovery Grant. The fourth author's work is supported by a European Research Council Advanced Grant under the European Union's Horizon 2020 research and innovation programme via grant agreement no. 695223.

$g \in \mathbb{Z}[t]$ of some degree $k = k(\varepsilon) \geq 1$ having the property that each irreducible factor of $f(g(t))$ has degree at most εkd?

If the answer to this question is in the affirmative, then the aforementioned smoothness conjecture on polynomial values would follow at once. Regrettably, with the exception of polynomials of special shape, an affirmative answer has been available only in the case $d = 1$. Our primary goal in this paper is to answer this question in the affirmative in the case $d = 2$.

THEOREM 1.1. *Let $f \in \mathbb{Z}[t]$ be quadratic. Then for some $c > 0$ there are polynomials $g \in \mathbb{Z}[t]$ of arbitrarily large odd degree k for which $f(g(t))$ factors as a product of polynomials of degree at most $ck/\sqrt{\log\log k}$. Thus f admits polysmoothness ε for any $\varepsilon > 0$.*

COROLLARY 1.2. *When $\varepsilon > 0$ and $f \in \mathbb{Z}[t]$ is a quadratic polynomial, there are infinitely many $n \in \mathbb{N}$ for which $f(n)$ is n^{ε}-smooth. Thus f admits smoothness ε.*

The sharpest conclusion available for quadratic polynomials hitherto is due to Schinzel [9, Theorem 15]. This work, half a century old, shows that when $f \in \mathbb{Z}[t]$ is quadratic, then it admits smoothness θ, where

$$\theta = \tfrac{1}{2}(1 - \tfrac{1}{3})(1 - \tfrac{1}{7})(1 - \tfrac{1}{47})(1 - \tfrac{1}{2207}) \cdots = 0.27950849\ldots.$$

For certain classes of quadratic polynomials one can do better. For example, Schinzel [9, Theorem 14] shows that if $f(t) = a(rt + s)^2 \pm b$ with $a, r, s \in \mathbb{Z}$, $ar \neq 0$ and $b \in \{1, 2, 4\}$, then f admits smoothness ε for any $\varepsilon > 0$. However, as is implicit in the concluding remarks of Schinzel [9], polynomials such as $4t^2 + 4t + 9 = (2t + 1)^2 + 8$ remain inaccessible to these methods. It is for awkward polynomials of this type that Corollary 1.2 for the first time confirms the longstanding smoothness conjecture.

The state of knowledge for polynomials of degree exceeding two is in general far less satisfactory. Discussion here requires that we return to the topic of well-factorable polynomial compositions. Consider a polynomial $f \in \mathbb{Z}[t]$ of degree $d \geq 2$. Then the simplest approach that is generally applicable stems from the trivial identity $f(t) \equiv 0 \pmod{f(t)}$, which yields the only slightly less trivial congruential relation $f(t + f(t)) \equiv 0 \pmod{f(t)}$. The latter is of course merely another means of expressing the factorisation $f(t + f(t)) = f(t)h(t)$, where $h \in \mathbb{Z}[t]$ is some polynomial of degree $d^2 - d$. This instantly shows that f admits polysmoothness $1 - 1/d$, but more can be extracted by iterating this construction. Thus, in the next step, one substitutes $t = x + h(x)$ into the polynomial $f(t + f(t))$ and so on. In this way one sees that a polynomial $g \in \mathbb{Z}[t]$ may be found having the property that $f(g(t))$ has as many irreducible factors as desired, and moreover that f admits polysmoothness $\theta(d)$, with

$$\theta(d) = 1 - \frac{1}{d-1} + O\Big(\frac{1}{d^3}\Big).$$

Schinzel [9, Lemma 10] offers a more elaborate construction, which we will revisit in Section 3, showing that for a degree d polynomial $f \in \mathbb{Z}[t]$, there exists a degree $d - 1$ polynomial $g \in \mathbb{Z}[t]$ having the property that $f(g(t))$ has a degree d factor.

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

This construction may also be iterated. In order to describe the limit of Schinzel's circle of ideas, we introduce some notation. When $d \geq 2$, we define the sequence $(u_i)_{i=1}^{\infty}$ by putting $u_1 = d - 1$ and then setting $u_{i+1} = u_i^2 - 2$ $(i \geq 1)$. We may now define the exponent $\theta(d)$ by taking

$$\theta(d) = \begin{cases} \frac{1}{2}P(2d) & \text{when } d = 2, 3, \\ P(d) & \text{when } d > 3, \end{cases}$$

where

$$P(d) = \prod_{i=1}^{\infty}(1 - 1/u_i). \tag{1.1}$$

Then Schinzel [9, Theorem 15] shows that every polynomial $f \in \mathbb{Z}[t]$ of degree d admits polysmoothness η for any $\eta > \theta(d)$. A modest computation reveals that

$$\theta(2) = 0.27950849\ldots, \quad \theta(3) = 0.38188130\ldots, \quad \theta(4) = 0.55901699\ldots$$

and that, for large d, one has

$$\theta(d) = 1 - \frac{1}{d-2} + O\Big(\frac{1}{d^3}\Big).$$

Although the conclusion of Theorem 1.1 supersedes this result in the case $d = 2$, further progress for larger degrees remains elusive. This absence of progress for larger degrees motivates the exploration of families of polynomials f admitting sharper smoothness than attained via Schinzel's construction. In Section 3 we reinterpret Schinzel's method in terms of field structures associated with the splitting field for f over $\mathbb{Q}$. Thereby, we obtain some enhancements applicable for special families of polynomials summarised in the following result.

THEOREM 1.3. *Let $f \in \mathbb{Z}[t]$ be irreducible and let α be a root of f lying in its splitting field. Suppose that for some $\gamma \in \mathbb{Q}(\alpha)$ and $g \in \mathbb{Z}[t]$ of degree $k \geq 2$, one has $\alpha = g(\gamma)$. Then $f(g(t))$ is divisible by the minimal polynomial of γ over $\mathbb{Q}$ and hence f admits polysmoothness $1 - 1/k$.*

Suppose that $f \in \mathbb{Z}[t]$ is irreducible of degree d and that α is a root of f lying in its splitting field. Then, given any $\gamma \in \mathbb{Q}(\alpha)$ with $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha)$, since $\alpha \in \mathbb{Q}(\gamma)$, we find that there exists a polynomial $g \in \mathbb{Q}[t]$ of degree at most $d - 1$ with $\alpha = g(\gamma)$. Thus, save for establishing that $\deg(g) > 1$ and further that the coefficients of g may be taken to be integers, Theorem 1.3 recovers the conclusion of Schinzel. It is apparent, moreover, that there is the potential for this polynomial g to have degree significantly smaller than that of f and in such circumstances one does better than Schinzel.

COROLLARY 1.4. *Suppose that $f \in \mathbb{Z}[t]$ is irreducible and let α be a root of f lying in its splitting field. Suppose that $f(t) = g(h(t)) - t$, with $g, h \in \mathbb{Z}[t]$ of degree exceeding one. Then $f(g(t))$ is divisible by the minimal polynomial of $h(\alpha)$ over $\mathbb{Q}$ and hence f admits polysmoothness $1 - 1/\deg(g)$.*

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

The point here is that, since $f(\alpha) = 0$, one has $\alpha = g(h(\alpha))$ and so one can apply Theorem 1.3 with $\gamma = h(\alpha)$. Thus, for example, the polynomial $f(t) = t^4 + 4t^2 - t + 1$ satisfies the relation

$$f(t) = (t^2 + 1)^2 + 2(t^2 + 1) - t - 2 = g(h(t)) - t$$

with $g(t) = t^2 + 2t - 2$ and $h(t) = t^2 + 1$. One may verify that f is irreducible over $\mathbb{Q}$. Hence, if α is a root of f lying in its splitting field, one deduces from the corollary that $f(t^2 + 2t - 2)$ is divisible by the minimal polynomial of $h(\alpha)$ over $\mathbb{Q}$. Note that since $\alpha = g(h(\alpha))$, it is not possible that $h(\alpha)$ lies in a proper subfield of $\mathbb{Q}(\alpha)$ and hence its minimal polynomial has degree four. In this way, one finds that $f(t^2 + 2t - 2) = m_1(t)m_2(t)$ for polynomials $m_i \in \mathbb{Z}[t]$ each having degree four. Indeed, one has

$$f(t^2 + 2t - 2) = (t^4 + 4t^3 - 9t + 5)(t^4 + 4t^3 - 7t + 7).$$

Thus f admits polysmoothness $\frac{1}{2}$, which is already sharper than the conclusion of Schinzel, which shows f to admit polysmoothness at best $0.559\ldots$. From here, one can continue by iterating Schinzel's construction on m_1m_2, thereby showing that f admits polysmoothness η for any $\eta > \frac{1}{2}P(8)$, where $P(8)$ is defined as in (1.1). In this way, one may verify that f admits polysmoothness $0.41926274\ldots$.

The method underlying the proof of Theorem 1.1 may be seen as a hybrid of the cyclotomic construction of Section 2 with the field-theoretic approach described in Section 3. This we describe in Section 4. Another class of polynomials is susceptible to a decomposition in some ways reminiscent of the Aurifeuillian factorisations discussed by Granville and Pleasants in [5]. We illustrate our ideas in Section 5 with the simplest classes of trinomials. Here and throughout, we write $\phi(n)$ for the Euler totient of the natural number n.

THEOREM 1.5. *Suppose that k is a natural number with $k \geq 2$.*

(i) *Let $f(t) = t^k + at^{k-1} - b$ with $a, b \in \mathbb{Z}$ and $b \neq 0$. Then f admits polysmoothness $\phi(k-1)/(k-1)$.*

(ii) *Let $f(t) = at^k - t + b$ with $a, b \in \mathbb{Z}$ and $ab \neq 0$. Then f admits polysmoothness $\phi(k)/k$.*

To illustrate the potential effectiveness of this theorem, consider the polynomial $f_k(t) = t^k - t - 1$. It was shown by Selmer [11] that f_k is irreducible over $\mathbb{Q}$ for each $k \geq 2$. Meanwhile, Theorem 1.5 shows that f admits polysmoothness $\phi(k)/k$, and this can be made arbitrarily close to 0 by taking a sequence of exponents k equal to the product of the first n prime numbers, and letting $n \to \infty$. In this special case, the method of proof is simple to describe. We take a polynomial g of large degree and put $t = g(x)^k - 1$. Thus, we find that

$$f_k(g(x)^k - 1) = (g(x)^k - 1)^k - g(x)^k$$

and so, as a difference of two kth powers, we may employ a decomposition via cyclotomic polynomials to factorise $f_k(g(x)^k - 1)$.

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

In our discussion of smooth values of polynomials, we have emphasised the application of polysmoothness to establish smoothness. An alternative approach to the problem of showing that polynomials take smooth values at integral arguments is via sieve theory. Typical of the kind of result that may be established is a conclusion of Dartyge, Tenenbaum and the third author [4]. Let $f \in \mathbb{Z}[t]$ be an irreducible polynomial of degree $d \geq 1$ and let $\varepsilon > 0$. Then, in particular, these authors show that for a positive proportion of integers n, the integer $N = |f(n)|$ is $N^{1-1/d+\varepsilon}$-smooth. Thus, f admits smoothness $1 - 1/d + \varepsilon$. Although weaker than the conclusions described above, this smoothness result has the merit that it applies for a positive proportion of the values represented by f. In the same vein, subject to the truth of a certain uniform quantitative form of the Schinzel–Sierpiński hypothesis, the third author [8] has obtained an asymptotic formula for the number of integers n with $1 \leq n \leq x$ for which $N = |f(n)|$ is $N^{1-1/(d-1)+\varepsilon}$-smooth when f is irreducible.

2. A cyclotomic construction

The polysmoothness question described in the introduction can be answered for polynomials $f \in \mathbb{Z}[t]$ equal to any product of binomials. Consider then integers a_j, b_j, k_j with $k_j \geq 1$ $(1 \leq j \leq l)$ and the polynomial

$$f(t) = \prod_{j=1}^{l} (a_j t^{k_j} - b_j). \tag{2.1}$$

The argument employed by Balog and the fourth author in their proof of [1, Lemma 2.2] is easily modified to confirm that f admits polysmoothness ε for any $\varepsilon > 0$, as we now show.

THEOREM 2.1. *Let $f \in \mathbb{Z}[t]$ be a polynomial of the shape (2.1) with $a_1 \dots a_l \neq 0$. Then, for some $c = c(\mathbf{k}) > 0$, there are polynomials $g \in \mathbb{Z}[t]$ of arbitrarily large degree d for which $f(g(t))$ factors as a product of polynomials of degree at most $cd/(\log\log d)^{1/l}$. Thus f admits polysmoothness ε for any $\varepsilon > 0$.*

PROOF. Write $k = k_1 \dots k_l$ and let y be a natural number sufficiently large in terms of k. Then it follows from [1, Lemma 2.1] that the prime numbers not exceeding y and coprime to k can be partitioned into l sets $\mathcal{P}_1, \dots, \mathcal{P}_l$ with the property that for each i, one has

$$\prod_{p \in \mathcal{P}_i} (1 - 1/p) < 2\Big(\frac{k}{\phi(k)\log y}\Big)^{1/l} \quad \text{and} \quad \prod_{p \in \mathcal{P}_i} p < y^2 e^{5y/(4l)}. \tag{2.2}$$

Put

$$\gamma_i = \prod_{p \in \mathcal{P}_i} p \quad \text{and} \quad \Gamma_i = \prod_{\substack{1 \leq j \leq l \\ j \neq i}} \gamma_j,$$

and write $\Gamma = \gamma_1 \dots \gamma_l$. It follows from standard prime number estimates that $k^{-1} e^{3y/4} < \Gamma < e^{5y/4}$. Since $(k_j \Gamma_j, \gamma_j) = 1$ $(1 \leq j \leq l)$, we find that for each index j there exist

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

integers $\widetilde{\lambda}_j, \widetilde{\mu}_j$ with $1 \le \widetilde{\lambda}_j, \widetilde{\mu}_j < \gamma_j$, and satisfying

$$k_j \Gamma_j \widetilde{\lambda}_j \equiv -1 \pmod{\gamma_j} \quad \text{and} \quad k_j \Gamma_j \widetilde{\mu}_j \equiv 1 \pmod{\gamma_j}.$$

We put $\lambda_j = \Gamma_j \widetilde{\lambda}_j$ and $\mu_j = \Gamma_j \widetilde{\mu}_j$ $(1 \le j \le l)$. Also, when $1 \le i, j \le l$ and $i \ne j$, we define the integers Λ_{ij} and M_{ij} via the relations

$$\Lambda_{ij} = k_j \lambda_i / \gamma_j \quad \text{and} \quad \mathrm{M}_{ij} = k_j \mu_i / \gamma_j,$$

and

$$\Lambda_{jj} = (k_j \lambda_j + 1)/\gamma_j \quad \text{and} \quad \mathrm{M}_{jj} = (k_j \mu_j - 1)/\gamma_j.$$

We are now equipped to define the auxiliary polynomial

$$g(t) = t^{\Gamma} \prod_{j=1}^{l} a_j^{\lambda_j} b_j^{\mu_j}.$$

This polynomial has degree Γ satisfying $k^{-1} e^{3y/4} < \Gamma < e^{5y/4}$, whence

$$y \asymp \log \Gamma. \tag{2.3}$$

Moreover, when $1 \le j \le l$, one has $a_j g(t)^{k_j} - b_j = b_j (z_j^{\gamma_j} - 1)$, where

$$z_j = t^{k_j \Gamma_j} \prod_{i=1}^{l} a_i^{\Lambda_{ij}} b_i^{\mathrm{M}_{ij}}.$$

But $z_j^{\gamma_j} - 1 = \prod_{e \mid \gamma_j} \Phi_e(z_j)$, where Φ_e denotes the eth cyclotomic polynomial. It therefore follows that

$$f(g(t)) = \prod_{j=1}^{l} b_j (z_j^{\gamma_j} - 1)$$

factors as a product of polynomials of degree at most

$$\max_{1 \le j \le l} \max_{e \mid \gamma_j} \phi(e) \deg(z_j) = \max_{1 \le j \le l} k_j \Gamma_j \phi(\gamma_j) = \Gamma \max_{1 \le j \le l} \frac{k_j \phi(\gamma_j)}{\gamma_j}.$$

But, in view of (2.2) and (2.3), one has

$$\frac{k_j \phi(\gamma_j)}{\gamma_j} = k_j \prod_{p \in \mathcal{P}_j} (1 - 1/p) < 2 k_j \left(\frac{k}{\phi(k) \log y} \right)^{1/l} \ll (\log \log \Gamma)^{-1/l}.$$

Then we are forced to conclude that there is a number $c = c(\mathbf{k}) > 0$ for which $f(g(t))$ factors as a product of polynomials of degree at most $c\Gamma/(\log \log \Gamma)^{1/l}$, where $\Gamma = \deg(g)$. This completes the proof of the theorem. □

The special case of Theorem 2.1 corresponding to the polynomial

$$f(t) = (a_1 t - b_1)(a_2 t - b_2),$$

with $l = 2$, $k_1 = k_2 = 1$, confirms the conclusion of Theorem 1.1 in the special case of quadratic polynomials that factor as a product of two linear factors. We may consequently restrict attention in our proof of Theorem 1.1 in Section 4 to irreducible quadratic polynomials.

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

3. Field-theoretic constructions

We begin in this section by describing the proof of Theorem 1.3. This permits an abstract explanation of the construction of Schinzel described in the introduction, though for the sake of simplicity we restrict ourselves in such matters to monic polynomials.

The proof of Theorem 1.3. Let $f \in \mathbb{Z}[t]$ be irreducible of degree $d \geq 2$ and let α be a root of f lying in its splitting field. Suppose that $\gamma \in \mathbb{Q}(\alpha)$ and that for some $g \in \mathbb{Z}[t]$ of degree $k \geq 2$, one has $\alpha = g(\gamma)$. Since $f(g(\gamma)) = f(\alpha) = 0$, it follows that the minimal polynomial m of γ over $\mathbb{Q}$ divides $f(g)$. By Gauss' lemma, we infer that $f(g)$ is divisible by an integral multiple $\widetilde{m}$ of m lying in $\mathbb{Z}[t]$. One has

$$\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha) = \mathbb{Q}(g(\gamma)) \subseteq \mathbb{Q}(\gamma)$$

and hence

$$\deg(\widetilde{m}) = [\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = d.$$

Then, for some polynomial $h \in \mathbb{Z}[t]$, one has $f(g) = \widetilde{m}h$ with $\deg(\widetilde{m}) = d$, $\deg(f(g)) = kd$ and $\deg(h) = kd - d$. We thus conclude that every polynomial factor of $f(g)$ has degree at most $d(k-1)$, whence f admits polysmoothness $1 - 1/k$. This completes the proof of Theorem 1.3. □

The factorisation of $f(g(x))$ is in general closely related to the factorisation of $g(x) - \alpha$, as various authors have noticed. The conclusion of Theorem 1.3 is closely related to the following proposition, which Schinzel [10, Theorem 22] attributes to Capelli. (This proposition also appears, in a slightly infelicitous form, as [5, Lemma 1].)

Proposition 3.1. *Let $f \in \mathbb{Q}[t]$ be monic and irreducible, let α be any root of f in its splitting field and put $K = \mathbb{Q}(\alpha)$. Then, for any $g \in \mathbb{Q}[t]$, if the factorisation of $g(t) - \alpha$ as a product of irreducibles over $K[t]$ is*

$$g(t) - \alpha = a_1(t;\alpha)^{r_1} \dots a_k(t;\alpha)^{r_k},$$

then the factorisation of $f(g(t))$ as a product of irreducibles over $\mathbb{Q}[t]$ is

$$f(g(t)) = A_1(t)^{r_1} \dots A_k(t)^{r_k}$$

with

$$A_j(t) = \prod_{f(\beta)=0} a_j(t;\beta) \quad (1 \leq j \leq k).$$

Theorem 1.3 follows from Proposition 3.1 as the special case in which one of the irreducible factors $a_i(t;\alpha)$ is linear. It is apparent that, in the setting of Proposition 3.1, the wider generality that it has the potential to offer may be exploited to improve polysmoothness bounds for f whenever one has corresponding polysmoothness bounds for polynomials $g(t) - \alpha$ over $\mathbb{Q}(\alpha)$.

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

The idea underlying the construction of Schinzel described in [9, Lemma 10] can be interpreted in the guise of Theorem 1.3 as follows. We restrict attention to monic irreducible polynomials

$$f(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0.$$

Let α be a root of f lying in its splitting field and put $\beta = 1/\alpha$. Then, since $f(\alpha) = 0$, it follows that

$$\alpha = -(a_{d-1} + a_{d-2}\beta + \cdots + a_0\beta^{d-1}).$$

We take $g(t) = -(a_0 t^{d-1} + \cdots + a_{d-1})$. Then $\alpha = g(\beta)$ with $g \in \mathbb{Z}[t]$ a polynomial of degree $d-1$. Theorem 1.3 consequently delivers the conclusion that f admits polysmoothness $1 - 1/(d-1)$.

Two comments are in order here. First, the restriction that f be irreducible is easily negotiated away with a little careful thought. Second, the condition that f be monic in the above argument can be surmounted with the application of carefully chosen shifts, as Schinzel demonstrates. This is a little delicate, and we have chosen to avoid such technical issues with the hope that the underlying ideas may be more clearly visible from our simplified discussion.

Incidentally, the strategy employed in the above argument is relevant to the question raised by Granville and Pleasants following [5, Corollary 1].

Question (Granville and Pleasants). *Suppose that $f(t) \in \mathbb{Q}[t]$ is irreducible. Can one find infinitely many $g(y) \in \mathbb{Q}[y]$ with $\deg(g) < \deg(f)$ for which $f(g(y))$ is reducible in $\mathbb{Q}[y]$, where the $g(y)$ are distinct under transformations replacing y by a polynomial in y?*

When $f \in \mathbb{Q}[t]$ is irreducible of degree two and $g \in \mathbb{Q}[y]$ has degree smaller than that of f, it is apparent that g is linear and hence the answer to this question is negative. Suppose then that f has degree $d \geq 3$ and let α be a root of f in its splitting field. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. We take β to be any element of $\mathbb{Q}(\alpha)$ not lying in $\mathrm{span}_{\mathbb{Q}}\{1, \alpha\}$ with $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$. There are infinitely many such elements β. Then, since $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, one has $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. But $\alpha \in \mathbb{Q}(\beta)$, so there exists a polynomial $g \in \mathbb{Q}[y]$ of degree at most $d-1$ with the property that $\alpha = g(\beta)$. Furthermore, since $\beta \notin \mathrm{span}_{\mathbb{Q}}\{1, \alpha\}$, one sees that $\deg(g) > 1$. We have $f(g(\beta)) = f(\alpha) = 0$, so that $f(g(y))$ is divisible by the minimal polynomial of β over $\mathbb{Q}$. Since the latter has degree $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$, it follows that $f(g(y))$ is reducible and yet $\deg(g) \leq d - 1 < \deg(f)$. What is unclear is whether or not the polynomials g generated by this process are distinct under polynomial transformations, although it seems unlikely that all of these polynomials could be generated by a finite set by such substitutions. In the cubic case, however, we are able to resolve this issue.

Theorem 3.2. *Suppose that $f(t) \in \mathbb{Q}[t]$ is irreducible of degree three. Then there are infinitely many quadratic polynomials $g(y) \in \mathbb{Q}[y]$ for which $f(g(y))$ is reducible in $\mathbb{Q}[y]$, where the $g(y)$ are distinct under transformations replacing y by a polynomial in y.*

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

Proof. We follow the construction described above, employing the same notation, and initially seek a more detailed description of the factorisations of the compositions in question. Thus, for a quadratic polynomial $g \in \mathbb{Q}[y]$, one finds that $f(g(y))$ is divisible by the minimal polynomial m_β of β over $\mathbb{Q}$, and $\deg(m_\beta) = 3$. Thus, $f(g(y)) = m_\beta(y)l(y)$ for some polynomial $l \in \mathbb{Q}[y]$ of degree three. Note that $\beta \in \mathbb{Q}(\alpha)$ is one root of the quadratic polynomial $g(y) - \alpha$. The second root γ must also lie in $\mathbb{Q}(\alpha)$. We observe that γ cannot be a root of m_β, for then one would have that $g(y) - \alpha$ divides $m_\beta(y)$. The quotient $q(y)$ here is linear, and cannot lie in $\mathbb{Q}[y]$, since $m_\beta(y)$ is irreducible over $\mathbb{Q}[y]$. But the leading coefficient of $q(y)$ is rational, so the coefficient of y^2 in $m_\beta(y)$ cannot be rational, leading to a contradiction. Thus, indeed, we have $m_\beta(\gamma) \neq 0$, confirming our earlier assertion.

The polynomial l cannot have linear or quadratic factors over $\mathbb{Q}[y]$, for any root θ of such a factor would supply a root $g(\theta)$ of f lying in a field extension of $\mathbb{Q}$ of degree one or two, contradicting the irreducibility of f. Then $l(y)$ is a scalar multiple of a cubic polynomial irreducible over $\mathbb{Q}[y]$. But γ is a root of this polynomial, so that l is a scalar multiple of its minimal polynomial m_γ, and we have $f(g) = \kappa m_\beta m_\gamma$, for some nonzero rational number κ. Moreover, since $g \in \mathbb{Q}[y]$ and both β and γ are roots of the quadratic polynomial $g(y) - \alpha$, then an examination of the coefficient of y in the latter polynomial reveals that $\beta + \gamma \in \mathbb{Q}$. There is therefore a rational number r for which $\gamma = r - \beta$ and we have $f(g(y)) = \kappa m_\beta(y)m_{r-\beta}(y)$.

We next attend to the matter of confirming that infinitely many of these polynomials g are distinct under transformations replacing y by a polynomial in y. It is apparent that the only possibility for such a transformation is a linear one taking y to $ay + b$ for some rational numbers a and b with $a \neq 0$. Motivated by this observation, when $F, G \in \mathbb{Q}[y]$, we write $F \sim G$ when there exist $a, b \in \mathbb{Q}$ with $a \neq 0$ for which $F(y) = G(ay + b)$. It is readily confirmed that this relation defines an equivalence relation on elements of $\mathbb{Q}[y]$. Returning now to the discussion of the previous paragraph, one may check that

$$f\left(g\left(\frac{y-b}{a}\right)\right) = \kappa m_{a\beta+b}(y)m_{a(r-\beta)+b}(y).$$

Hence, whenever $G \sim g$, then $f(G(y)) = \kappa h_1(y)h_2(y)$ for some monic polynomials $h_1, h_2 \in \mathbb{Q}[y]$ with $h_i \sim m_\beta$ $(i = 1, 2)$.

Suppose that $\beta = A\alpha^2 + B\alpha + C$ and $\beta' = A'\alpha^2 + B'\alpha + C'$, with $A, B, C \in \mathbb{Q}$ satisfying $A \neq 0$, and likewise for the decorated analogues of these coefficients. Consider the composition factorisations

$$f(g(y)) = \kappa m_\beta(y)m_{r-\beta}(y) \quad \text{and} \quad f(g'(y)) = \kappa' m_{\beta'}(y)m_{r'-\beta'}(y)$$

induced from these elements by the process described above. If $g \sim g'$, then the conclusion of the previous paragraph shows that one must have $m_{\beta'} \sim m_\beta$. It is possible that β is the only root of m_β lying in $\mathbb{Q}(\alpha)$, in which case we see that for some $a, b \in \mathbb{Q}$ with $a \neq 0$, one must have $\beta' = a\beta + b$. Thus, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, it follows that $A' = aA$ and $B' = aB$, whence $B'/A' = B/A$. In such circumstances, it follows that the equivalence classes for g are classified by distinct ratios B/A, of which there are

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

infinitely many, and the conclusion of the theorem follows. It is possible, meanwhile, that m_β splits over $\mathbb{Q}(\alpha)[y]$. One then has $m_\beta(y) = (y-\beta_1)(y-\beta_2)(y-\beta_3)$, with $\beta_i = A_i\alpha^2 + B_i\alpha + C_i$, for suitable rational coefficients A_i, B_i, C_i. In such circumstances, a similar argument to that just employed reveals that for suitable rational numbers a and b with $a \neq 0$, and for some $i \in \{1,2,3\}$, one has $\beta' = a\beta_i + b$. In particular, one sees that $A_i \neq 0$ and $B'/A' = B_i/A_i$. Consequently, were there to be at most N distinct equivalence classes for the polynomials g generated by choices for $\beta = A\alpha^2 + B\alpha + C$, then the number of possible ratios B_i/A_i occurring amongst the associated roots $\beta_i = A_i\alpha^2 + B_i\alpha + C_i$ would be at most 3^N. Since there are infinitely many such ratios available to us, we derive a contradiction to the hypothesis that the number of equivalence classes is finite. Once again, therefore, we obtain the conclusion of the theorem. □

We are confident that a somewhat more elaborate argument would establish the quartic analogue of this theorem. Degrees exceeding four, on the other hand, would appear to be substantially more challenging. We finish this section by establishing Corollary 1.4.

The proof of Corollary 1.4. Assume the hypotheses of the statement of Corollary 1.4, so that $f(t) = g(h(t)) - t$. Let α be a root of f lying in its splitting field. Then $\alpha = g(h(\alpha))$, so one can apply Theorem 1.3 with $\gamma = h(\alpha)$. All that remains is to observe that the minimal polynomial of γ over $\mathbb{Q}$ must have degree $\deg(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, since $\mathbb{Q}(\alpha) = \mathbb{Q}(g(\gamma)) \subseteq \mathbb{Q}(\gamma)$. □

4. Smoothness of quadratic polynomials

Our goal in this section is the proof of Theorem 1.1 in the situation that $f \in \mathbb{Z}[t]$ is quadratic and irreducible. As we have commented already at the end of Section 2, this special case is all that we must now address in order to complete the proof of Theorem 1.1. Our argument can be construed as a hybrid of the methods discussed in Sections 2 and 3. We begin with an auxiliary lemma, the utility of which will become apparent in due course.

Lemma 4.1. *Let $f(t) = at^2 + bt + c \in \mathbb{Z}[t]$ be irreducible with $a \neq 0$. Denote by α a root of f in its splitting field. Then, for any $k \in \mathbb{N}$, there exist integers m, n, A and B with $A \neq 0$ and $(A, B) = 1$ such that $(ma\alpha + n)^k = A\alpha + B$.*

Proof. There exists some rational prime p not dividing a which splits in $K = \mathbb{Q}(\alpha)$, so $(p) = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1$ and $\mathfrak{p}_2$ contained in the order $\mathbb{Z}[a\alpha]$. Denoting the class number of K by $h(K)$, one has that $\mathfrak{p}_1^{h(K)}$ is principal and hence generated by $ma\alpha + n$ for some $m, n \in \mathbb{Z}$ with $m \neq 0$. Since $ma\alpha + n$ is an algebraic integer of K, it follows that for any $k \in \mathbb{N}$, one has $(ma\alpha + n)^k = A\alpha + B$ for some $A, B \in \mathbb{Z}$ with $A \neq 0$ and $a|A$. It remains now only to confirm that $(A, B) = 1$. But since $ma\alpha + n$ generates $\mathfrak{p}_1^{h(K)}$ and

$$\mathrm{Norm}_{K/\mathbb{Q}}((ma\alpha + n)^k) = \mathrm{Norm}_{K/\mathbb{Q}}(A\alpha + B) = a^{-1}(aB^2 - bAB + cA^2),$$

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

we find that $(A/a)Ac - (A/a)Bb + B^2$ is a power of p. Any prime which divides both A and B must divide this norm and thus must be equal to p. However, one cannot have both $p|A$ and $p|B$, for then the ideal $(A\alpha + B) = (ma\alpha + n)^k$ would be divisible by the ideal $(p) = \mathfrak{p}_1\mathfrak{p}_2$, contradicting our assumption that $\mathfrak{p}_1^{h(K)}$ is generated by $ma\alpha + n$. Thus, we conclude that $(A, B) = 1$. □

The proof of Theorem 1.1. Let $f(t) = at^2 + bt + c \in \mathbb{Z}[t]$ be irreducible and let α and α' be the roots of f in its splitting field. We have in mind the application of Lemma 4.1 to seek a relation of the shape $\alpha = (\beta^k - B)/A$ that we hope to apply in a manner not dissimilar to Theorem 1.3. First we describe the powers k in play. We take X to be large and choose k to be the product of all the primes less than X not dividing $2a\phi(a)$. Since we are omitting only a finite set of primes, it follows that

$$\prod_{p|k}(1 - 1/p) \asymp 1/\log X \asymp 1/\log\log k. \tag{4.1}$$

By applying Lemma 4.1, one finds that there exist integers m, n, A and B with $A \neq 0$ and $(A, B) = 1$ for which $(ma\alpha + n)^k = A\alpha + B$. We put $\beta = A\alpha + B$ and note that $f((\beta - B)/A) = f(\alpha) = 0$. Denote by Ω_d the set of primitive dth roots of unity. Put $G(t) = (t^k - B)/A$ and let $\zeta \in \Omega_d$ for some $d|k$. Then

$$f(G((ma\alpha + n)\zeta)) = f(((ma\alpha + n)^k - B)/A) = f(\alpha) = 0$$

and

$$f(G((ma\alpha' + n)\zeta)) = f(((ma\alpha' + n)^k - B)/A) = f(\alpha') = 0.$$

Note here that when ζ and ζ' are distinct kth roots of unity, then

$$(ma\alpha + n)\zeta \neq (ma\alpha + n)\zeta' \quad \text{and} \quad (ma\alpha + n)\zeta \neq (ma\alpha' + n)\zeta'.$$

The first relation is self-evident, whilst the second follows by taking kth powers and observing that $A\alpha + B \neq A\alpha' + B$. It therefore follows that all of the roots of $f(G(t))$ are accounted for by $(ma\alpha + n)\zeta$ and $(ma\alpha' + n)\zeta$ with $\zeta \in \Omega_d$ for some $d|k$. Thus, one may write $f(G(t)) = C\prod_{d|k} h_d(t)$ for a suitable rational number C, where

$$h_d(t) = \prod_{\zeta\in\Omega_d}(t - (ma\alpha + n)\zeta)(t - (ma\alpha' + n)\zeta).$$

Note here that, by considering conjugation in the field extension $\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}$, for $\zeta \in \Omega_d$, it is apparent that $h_d \in \mathbb{Q}[t]$ whenever $d|k$. Moreover, the polynomial h_d has degree $2\phi(d)$.

The possibility remains of an obstruction to selecting a polynomial g having *integral* coefficients for which $f(g)$ is well factorable. In order to address this complication, we consider the polynomial $g(t) = G(At + z)$ and seek to select z in such a manner that $g \in \mathbb{Z}[t]$. Put $K = \mathbb{Q}(\alpha)$ and consider the norm of the algebraic integer $A\alpha + B$, namely

$$\mathrm{Norm}_{K/\mathbb{Q}}(A\alpha + B) = a^{-1}(aB^2 - bAB + cA^2) = (\mathrm{Norm}_{K/\mathbb{Q}}(ma\alpha + n))^k.$$

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

By construction, we have $a|A$ and thus we see that B^2 is a kth power modulo A/a. Since k is odd, this observation implies that B is also a kth power modulo d for every divisor d of A/a. Let a' be the divisor of A given by $a' = \lim_{N\to\infty}(A, a^N)$. Then, in particular, we find that B is a kth power modulo A/a'. But k is coprime to both a and $\phi(a)$, and hence to the order of $(\mathbb{Z}/a'\mathbb{Z})^\times$, and thus all integers coprime to a' are necessarily kth powers modulo a'. We may therefore conclude that B is a kth power modulo A/a' and modulo a'. Since A/a' and a' are coprime, we discern that B is a kth power modulo A, say $B \equiv z^k \pmod{A}$.

We may now put

$$g(t) = G(At + z) = ((At + z)^k - B)/A \in \mathbb{Z}[t]$$

and we deduce that $f(g(t)) = C\prod_{d|k} h_d(At + z)$. Thus, on recalling (4.1), we infer that $f(g(t))$ factors as a product of polynomials of degree at most

$$\max_{d|k} \deg(h_d) = \max_{d|k} 2\phi(d) = 2k\prod_{p|k}(1 - 1/p) \asymp 2k/\log\log k.$$

By Gauss' lemma, moreover, there is no loss in supposing that these polynomial factors lie in $\mathbb{Z}[t]$. In particular, the polynomial f exhibits polysmoothness ε for any $\varepsilon > 0$. By construction, moreover, the polynomial g has odd degree k and so the proof of Theorem 1.1 is complete. □

Unfortunately, the construction applied here in the proof of Theorem 1.1 is less successful for higher degree polynomials. When $f = at^3 + bt^2 + ct + d \in \mathbb{Z}[t]$ is cubic, for example, and α is a root of f in its splitting field, then one cannot expect that there is an integer $k > 1$ for which

$$(ma\alpha + n)^k = A\alpha + B$$

for appropriate integers m, n, A and B with $A \neq 0$. Instead, one can find integers A, B and C for which

$$(ma\alpha + n)^k = A\alpha^2 + B\alpha + C.$$

A plausible plan is then to obtain a relation of the type

$$\lambda(ma\alpha + n)^{2k} + \mu(ma\alpha + n)^k = A\alpha + B$$

for suitable integers A, B, λ and μ. At best, such an approach would deliver a polynomial g of the shape

$$g(t) = (\lambda(At + z)^{2k} + \mu(At + z)^k - B)/A \in \mathbb{Z}[t]$$

having the property that $f(g(t))$ factors as a product of the shape

$$Ch_0(At + z)\prod_{d|k} h_d(At + z),$$

wherein h_0 has degree $3k$. *A priori*, this might ensure polysmoothness $\frac{1}{2}$ at best and so is not inherently stronger than the approach of Schinzel.

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

5. Relatives of Aurifeuillian factorisations

We next describe the proof of Theorem 1.5. This will not detain us for long. Suppose in the first instance that $f(t) = t^k + at^{k-1} - b$ with $a, b \in \mathbb{Z}$ and $b \neq 0$. We rearrange f in order to engineer a cyclotomic construction, writing $f(t) = (t + a)t^{k-1} - b$. Thus, if we set $g(t) = b^k t^{k-1} - a$, we find that

$$f(g(t)) = b((btg(t))^{k-1} - 1) = b \prod_{d|(k-1)} \Phi_d(btg(t)).$$

The polynomial $f(g)$ has degree $K = k(k-1)$, whilst each irreducible factor of $f(g)$ has degree at most

$$\max_{d|(k-1)} \phi(d)k \leq K\phi(k-1)/(k-1).$$

Then f admits polysmoothness $\phi(k-1)/(k-1)$. This establishes part (i) of Theorem 1.5.

Suppose next that $f(t) = at^k - t + b$ with $a, b \in \mathbb{Z}$ and $ab \neq 0$. With the same plan in mind as above, we set $g(t) = a^{k+1}t^k + b$ and arrive at the relation

$$f(g(t)) = a(g(t)^k - (at)^k) = a \prod_{d|k} (at)^{\phi(d)} \Phi_d(g(t)/(at)).$$

The term in the product here indexed by d is a polynomial of degree $k\phi(d)$. Thus, the polynomial $f(g)$ has degree $K = k^2$, whilst each irreducible factor of $f(g)$ has degree at most $\max_{d|k} \phi(d)k \leq K\phi(k)/k$. Then f admits polysmoothness $\phi(k)/k$. This establishes part (ii) of Theorem 1.5 and completes the proof of the theorem.

We remark that Harrington [6, Theorem 1] has investigated the irreducibility of polynomials $f(t)$ of the shape $t^n \pm ct^{n-1} \pm d$ over $\mathbb{Z}[t]$. Thus, such polynomials are irreducible when $n, c, d \in \mathbb{N}$ satisfy

$$n \geq 3, \quad d \neq c, \quad d \leq 2(c-1), \quad (n, c) \neq (3, 3) \quad \text{and} \quad f(\pm 1) \neq 0.$$

Moreover, Ljunggren [7, Theorem 3] has shown that all of the polynomials

$$t^{3n} \pm t \pm 1, \quad t^{3n+1} \pm t \pm 1, \quad t^{6n+5} - t \pm 1 \quad \text{and} \quad t^{6n+2} \pm t - 1$$

are irreducible for all natural numbers n.

6. Polynomials resisting polysmoothness

We finish with an account of some examples demonstrating limitations to the most ambitious results one might imagine concerning polysmoothness. We concentrate on irreducible polynomials $f_d \in \mathbb{Z}[t]$ of degree d. In view of the conclusion of Theorem 1.1, it makes sense to restrict attention to degrees d exceeding two. One might optimistically hope that for each such polynomial, there should exist a quadratic polynomial $g \in \mathbb{Z}[t]$ having the property that $f_d(g(t)) = h_1(t)h_2(t)$ for some polynomials $h_i \in \mathbb{Z}[t]$ irreducible of degree d. Note here that $f_d(g(t))$ cannot be divisible by a polynomial $h \in \mathbb{Z}[t]$ of degree smaller than d, for then a root β of this polynomial in

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

its splitting field would supply a root $g(\beta)$ of f_d with $[\mathbb{Q}(g(\beta)) : \mathbb{Q}] < d$, contradicting the irreducibility of f_d. Thus, if the polynomial $f_d(g(t))$ is reducible, then necessarily it factors in precisely the shape $h_1(t)h_2(t)$ asserted.

As we have already discussed in the introduction, the construction of Schinzel [9, Lemma 10] shows that in the cubic case $d = 3$, quadratic polynomials $g \in \mathbb{Z}[x]$ can be found for which $f_3(g(x)) = h_1(x)h_2(x)$ with h_1 and h_2 both cubic. The corresponding situation for quartic polynomials is rather less clear. Consider, for example, the irreducible quartic polynomial

$$f_4(t) = t^4 + t^2 + 2t + 3.$$

One may computationally confirm that for every nontrivial integral choice of coefficients $a, b, c \in \mathbb{Z}$ with absolute value at most 1000, the degree 8 polynomial $f_4(ax^2 + bx + c)$ is irreducible, so that no decomposition of the form sought is available in this range. This does not rule out the possibility, of course, that there might be a quadratic with very large coefficients that does deliver the sought-after polysmoothness. On the other hand, if instead one works over $\mathbb{Q}[t]$ instead of $\mathbb{Z}[t]$, then obstructions are possible only for biquadratic quartics. Indeed, one has

$$f_4\Big(-\frac{x^2 + x + 3}{2}\Big) = \frac{1}{16}(x^4 + 2x^3 + 7x^2 + 2x + 9)(x^4 + 2x^3 + 7x^2 + 10x + 13).$$

This example shows that the problem of finding *integral* polynomial substitutions delivering well-factorability is in general very much more challenging than finding corresponding rational polynomial substitutions.

More generally, by completing the fourth power in the usual manner, it is apparent that decompositions similar to that of the last paragraph may be obtained for arbitrary quartic polynomials provided such is the case for irreducible quartics of the shape $f_4(t) = At^4 + Bt^2 + Ct + D$. If, in addition, one has $C \neq 0$, then we may put

$$g(x) = -\frac{Ax^2 + Bx + D}{C}$$

and we deduce that

$$f_4(g(x)) = h_1(x)h_2(x)$$

for suitable quartic irreducible polynomials $h_1, h_2 \in \mathbb{Q}[x]$. The point here is that, if α is a root of f in its splitting field, then $\alpha = g(\alpha^2)$ and so α^2 is a root of $f_4(g(x))$. Thus, the minimal polynomial of α^2 over $\mathbb{Q}$ divides $f_4(g(x))$. A straightforward exercise confirms that this minimal polynomial is not quadratic, whence $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and the assertion that h_1 and h_2 are quartic follows.

For degrees d exceeding four, obstructions to these quadratic-based decompositions appear, as can be seen from the following criterion.

THEOREM 6.1. *Let $f_d \in \mathbb{Z}[t]$ be an irreducible polynomial of degree d with leading coefficient A and define $\phi_d(x, y) = y^d f_d(x/y)$. Suppose that there exists a quadratic polynomial $g \in \mathbb{Q}[t]$ having the property that $f_d(g(t))$ is reducible. Then the equation $Az^2 = \phi_d(x, y)$ possesses a solution $(x, y, z) \in \mathbb{Q}^3$ with $yz \neq 0$.*

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

Proof. By a now familiar argument, it is apparent that if $f_d(g(t)) = h_1(t)h_2(t)$ is a factorisation of $f_d(g(t))$ with $h_i \in \mathbb{Q}[t]$ and $\deg(h_i) \geq 1$ $(i = 1, 2)$, then one must have $\deg(h_i) \geq d$. It follows, in particular, that h_1 and h_2 are both constant multiples of irreducible polynomials of degree d. Let α be a root of f_d in its splitting field and let β be a root of the polynomial $g(t) - \alpha$ in its splitting field. Then, since $f(g(\beta)) = 0$, one must have $h_i(\beta) = 0$ for either $i = 1$ or $i = 2$. Also, one has $\mathbb{Q}(\alpha) = \mathbb{Q}(g(\beta)) \subseteq \mathbb{Q}(\beta)$ and yet $[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg(h_i) = d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, so that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

We may write $g(t) = at^2 + bt + c$ for some $a, b, c \in \mathbb{Q}$ with $a \neq 0$. Thus, we have

$$(2a\beta + b)^2 = 4ag(\beta) + b^2 - 4ac = b^2 - 4ac + 4a\alpha.$$

Writing $K = \mathbb{Q}(\alpha)$, and putting $m = 4a$ and $n = b^2 - 4ac$, we obtain the relation

$$(\mathrm{Norm}_{K/\mathbb{Q}}(2a\beta + b))^2 = \mathrm{Norm}_{K/\mathbb{Q}}(m\alpha + n) = A^{-1}\phi_d(n, -m).$$

Thus, on recalling that $\beta \in \mathbb{Q}(\alpha)$, we find that the equation $Az^2 = \phi_d(x, y)$ has the rational solution

$$z = \mathrm{Norm}_{K/\mathbb{Q}}(2a\beta + b), \quad x = n, \quad y = -m \neq 0.$$

This completes the proof of the theorem. □

Note that since $A = \phi_d(1, 0)$, the equation $Az^2 = \phi_d(x, y)$ has the trivial solution $(x, y, z) = (1, 0, 1)$ and hence is automatically locally soluble everywhere. Of importance for the discussion of this section is the connection with hyperelliptic curves. When d is even, say $d = 2k$, any solution $(x, y, z) \in \mathbb{Q}^3$ of this equation with $yz \neq 0$ gives a rational point on the hyperelliptic curve defined by the equation $AY^2 = \phi_{2k}(X, 1)$, namely

$$(X, Y) = \left(\frac{x}{y}, \frac{z}{y^k}\right).$$

However, as has been shown by Bhargava (see [2] and also [3] for subsequent developments), most hyperelliptic curves over $\mathbb{Q}$ have no rational points. Thus, we must expect that for most irreducible polynomials $f_d \in \mathbb{Q}[x]$ of even degree $d \geq 6$, the composition $f_d(g(x))$ should be irreducible for all quadratic polynomials $g \in \mathbb{Q}[x]$. Specific examples can be obtained with some computational effort. For example, one may check that the polynomials

$$F_1(x) = x^6 - x^4 - 21x^2 - 31 \quad \text{and} \quad F_2(x) = x^6 + x^4 - 18x^2 - 43$$

are irreducible over $\mathbb{Q}[x]$. We verified this assertion ourselves by applying the PARI/GP software package. Next, by reference to the tables of elliptic curves provided by the L-functions and Modular Forms Database (available at www.lmfdb.org), one finds that the elliptic curves with Weierstrass forms

$$y^2 = x^3 - x^2 - 21x - 31 \quad \text{and} \quad y^2 = x^3 + x^2 - 18x - 43, \tag{6.1}$$

with respective Cremona labels 76a1 and 92a2, both have rank 0 and trivial torsion. These elliptic curves consequently have only the single rational point at infinity.

https://doi.org/10.1017/S1446788718000320 Published online by Cambridge University Press

In particular, it follows that there is no rational solution to either of the equations obtained by substituting $(x, y) = (X^2, Y)$ into the equations (6.1), namely

$$Y^2 = X^6 - X^4 - 21X^2 - 31 \quad \text{and} \quad Y^2 = X^6 + X^4 - 18X^2 - 43.$$

Thus, the above discussion shows that for $i = 1$ and 2, the polynomial $F_i(g(x))$ is irreducible for all quadratic polynomials $g \in \mathbb{Q}[x]$. One might complain that these two examples are rather special, since the Galois group associated with these polynomials is not the full symmetric group S_6. We are grateful to Michael Stoll for supplying the additional example

$$F_3(X) = X^6 - 3X^5 - 4X^4 + X^3 - 2X^2 - 2.$$

This polynomial is 'generic', in the sense that it is irreducible with Galois group S_6, and moreover the equation $Y^2 = F_3(X)$ has no rational solutions. Thus, we may conclude as above that for all quadratic polynomials $g \in \mathbb{Q}[x]$, the polynomial $F_3(g(x))$ is irreducible.

Acknowledgements

The first, third and fourth authors are grateful to the Heilbronn Institute for Mathematical Research for funding a visit of the third author to the University of Bristol in 2014 that laid the foundations for the work reported here. The authors are grateful to Michael Stoll for providing the sextic example concluding Section 6.

References

[1] A. Balog and T. D. Wooley, 'On strings of consecutive integers with no large prime factors', *J. Aust. Math. Soc. Ser.* A **64**(2) (1998), 266–276.
[2] M. Bhargava, 'Most hyperelliptic curves over $\mathbb{Q}$ have no rational points', Preprint, 2013, available at arXiv:1308:0395.
[3] M. Bhargava, B. H. Gross and X. Wang, 'A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension' (with an appendix by T. Dokchitser and V. Dokchitser), *J. Amer. Math. Soc.* **30**(2) (2017), 451–493.
[4] C. Dartyge, G. Martin and G. Tenenbaum, 'Polynomial values free of large prime factors', *Period. Math. Hungar.* **43**(1–2) (2001), 111–119.
[5] A. Granville and P. Pleasants, 'Aurifeuillian factorization', *Math. Comp.* **75**(253) (2006), 497–508.
[6] J. Harrington, 'On the factorization of the trinomials $x^n + cx^{n-1} + d$', *Int. J. Number Theory* **8**(6) (2012), 1513–1518.
[7] W. Ljunggren, 'On the irreducibility of certain trinomials and quadrinomials', *Math. Scand.* **8** (1960), 65–70.
[8] G. Martin, 'An asymptotic formula for the number of smooth values of a polynomial', *J. Number Theory* **93**(2) (2002), 108–182.
[9] A. Schinzel, 'On two theorems of Gelfond and some of their applications', *Acta Arith.* **13** (1967), 177–236.
[10] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, 77 (Cambridge University Press, Cambridge, 2000).
[11] E. S. Selmer, 'On the irreducibility of certain trinomials', *Math. Scand.* **4** (1956), 287–302.

J. W. BOBER, School of Mathematics, University of Bristol,
University Walk, Clifton, Bristol BS8 1TW, UK
and
The Heilbronn Institute for Mathematical Research, Bristol, UK
e-mail: j.bober@bristol.ac.uk

D. FRETWELL, School of Mathematics, University of Bristol,
University Walk, Clifton, Bristol BS8 1TW, UK
and
The Heilbronn Institute for Mathematical Research, Bristol, UK
e-mail: daniel.fretwell@bristol.ac.uk

G. MARTIN, Department of Mathematics, University of British Columbia,
Room 121, 1984 Mathematics Road, Vancouver, BC, Canada V6T 1Z2
e-mail: gerg@math.ubc.ca

T. D. WOOLEY, School of Mathematics, University of Bristol,
University Walk, Clifton, Bristol BS8 1TW, UK
e-mail: matdw@bristol.ac.uk