JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Anthony FLATTERS

Power values of certain quadratic polynomials

Tome 22, n° 3 (2010), p. 645-660.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_3_645_0>

Journal de Théorie des Nombres
de Bordeaux **22** (2010), 645-660

Power values of certain quadratic polynomials

par Anthony FLATTERS

Résumé. Soit f un polynôme quadratique à coefficients entiers avec discriminant sans carré parfait et $q > 1$ un entier tel que q et le nombre de classes du corps de rupture de f sont premiers entre eux. Dans cet article, nous calculons les puissances q-ième qui apparaissent comme valeurs entières de f. La théorie des diviseurs primitifs de suites d'entiers permet de déduire une borne sur les valeurs possibles de q qui est suffisamment petite pour que les cas restants puissent facilement être vérifiés. Ces résultats permettent de trouver toutes les puissances parfaites qui apparaissent dans certaines suites polynômiales récursives entières, y compris la suite de Sylvester.

Abstract. In this article we compute the qth power values of the quadratic polynomials $f \in \mathbb{Z}[x]$ with negative squarefree discriminant such that q is coprime to the class number of the splitting field of f over $\mathbb{Q}$. The theory of unique factorisation and that of primitive divisors of integer sequences is used to deduce a bound on the values of q which is small enough to allow the remaining cases to be easily checked. The results are used to determine all perfect power terms of certain polynomially generated integer sequences, including the Sylvester sequence.

1. Introduction

In 1926, Siegel [35] proved that an affine curve of genus at least one has only finitely many integer points. Siegel's theorem is ineffective; it gives us no way of explicitly determining all the integer points on such a curve. The equation

$$y^q = f(x), \tag{1.1}$$

where $q \geqslant 3$ and $f(x)$ is a quadratic polynomial with two distinct roots therefore has only finitely many integer solutions. The exact determination

Manuscrit reçu le 15 janvier 2010.

I would like to thank Professors Walsh, Györy, Hajdu and Pintér for sending me comments on an original draft of this paper and for also providing me with additional references. I also thank the anonymous referee for helpful suggestions. Finally I wish to thank the EPSRC for their support via a Doctoral Training Award.

Mots clefs. Primitive divisor; Diophantine equation; Lucas sequence.

Classification math.. 11B37, 11A41, 11B39.

of all integer solutions to such an equation is generally very difficult. In [5], Baker gave the first explicit upper bounds for the integer solutions of equation (1.1) in the case where f is any integral polynomial with at least two simple zeros. This result was obtained using his theorem about lower bounds for linear forms in the logarithms of algebraic numbers. Given the nature of the theory, these bounds are typically very large and the following upper bound was derived

$$\max\{|x|, |y|\} < \exp\exp((5q)^{10}(n^{10n}H)^{n^2}),$$

where $n = \deg(f)$, H is the height of f. Since Baker's result, there have been many refinements to the theory of linear forms in logarithms which allow smaller upper bounds to be obtained, for example, see the papers [13, 15, 30, 37, 39]. In [11], a method is given for the complete determination of integral solutions to an equation of the form $ay^p = f(x)$ where $a \in \mathbb{Z} \setminus \{0\}, p \geqslant 3$ and $f(x)$ is separable of degree at least 2. It was first proved by Tijdeman [38], using Baker's transcendence methods, that if f has at least 2 simple rational zeros and if $y^q = f(x)$ has an integer solution with $|y| > 1$, then q is bounded above by a computable constant depending only on f. Later this was improved by Schinzel and Tijdeman [31], who showed that for $P(x) \in \mathbb{Q}[x]$ with at least 2 distinct zeros, an integer solution $|y| > 1$, to the equation $y^m = P(x)$ implies m is bounded by an effectively computable constant depending only on P. Once again however, their technique is to use lower bounds for linear forms in logarithms and the bound for m obtained is very large. There have been several improvements to Schinzel and Tijdeman's result. In [8], the authors prove that if f is a monic irreducible polynomial of degree $n \geqslant 2$, $b \in \mathbb{Z} \setminus \{0\}$ and $y^z = bf(x)$ in integers x, y, z, $z > 1$, then $z < cM^{3n}(\log|2b|)^3$ where M denotes the Mahler measure of F and c is an effectively computable constant depending only on n. See also [14] for the result that if $f(x)$ is a monic irreducible polynomial of degree $n \geqslant 2$ then $y^z = f(x)$ in integers implies $z < (6n^3)^{30n^3}|D(f)|^{5n^2}$, where $D(f)$ is the discriminant of f. For further results on this area consult [7, 23, 25, 26, 34]. We will approach the problem of finding solutions differently. In this paper, we use Bilu, Hanrot and Voutier's wonderful theorem about prime appearance in Lucas sequences (see [10]) to give a very small bound on the exponent q in equation (1.1) (independent of the equation) in the case where f is a quadratic polynomial whose discriminant belongs to a subset of the negative integers. The bound on q is small enough to allow a bare-hands approach to computing all integral solutions, and in particular does not use any transcendence methods directly. We begin by stating our most general result.

Theorem 1.1. *Let f be a monic quadratic polynomial with integral coefficients such that $D(f)$ is negative and squarefree with the property that the class number h of $\mathbb{Q}(\sqrt{D(f)})$ is greater than one. Let $q > 2$ be a prime, and assume x, y are integers such that*

$$y^q = f(x).$$

Then $q \leqslant \max\{3, P(h)\}$, where $P(h)$ denotes the greatest prime factor of h.

We then go on to consider the case where the ring of integers of the splitting field of f is a unique factorisation domain and we obtain the following result.

Theorem 1.2. *Let f be a monic quadratic polynomial with integer coefficients. Further, suppose that $-D(f) \in \{7, 11, 19, 43, 67, 163\}$. If the equation (1.1) is soluble in integers $x, |y| > 1, q > 2$ prime, then $q \leqslant q_0$, where*

$$q_0 = \begin{cases} 13 & \text{if } D(f) = -7, \\ 7 & \text{if } D(f) = -19, \\ 5 & \text{if } D(f) = -11, \\ 3 & \text{if } D(f) = -43, -67, -163. \end{cases}$$

Moreover, if q is prime and $D(f) = -3, -8$, then equation (1.1) has no integer solutions x, y with $y > 1$ for $q > 3$.

Remark. *Monic quadratic polynomials $f, g \in \mathbb{Z}[x]$ have equal discriminant if and only if $f(x) = g(x + k)$ for some $k \in \mathbb{Z}$. It follows that in order to determine the integer solutions to the equations $y^q = g(x)$ where $D(g)$ is fixed, it is enough to determine them for the equation $y^q = h(x)$ where h is a quadratic polynomial such that $D(h) = D(g)$.*

An immediate corollary to Theorem 1.2 is the following.

Corollary 1.3. *Let $|y| > 1$ be an integer which satisfies equation (1.1) with $q > 1$, then*

(a) If $D(f) = -7$, the only solutions are

$$(y, q) \in \{(2, 13), (2, 5), (2, 3), (\pm 2, 2)\}.$$

(b) If $D(f) = -11$, the only solutions are $(y, q) \in \{(3, 5), (\pm 3, 2)\}$.
(c) If $D(f) = -19$, the only solutions are $(y, q) \in \{(5, 7), (\pm 5, 2)\}$.
(d) If $D(f) = -8$, the only solution is $(y, q) = (3, 3)$.
(e) If $D(f) = -43$, the only solution is $(y, q) = (\pm 11, 2)$.
(f) If $D(f) = -67$, the only solution is $(y, q) = (\pm 17, 2)$.
(g) If $D(f) = -163$, the only solution is $(y, q) = (\pm 41, 2)$.
(h) If $D(f) = -3$, the only solution is $(y, q) = (7, 3)$.

Remark. *The procedure which is implemented to derive this corollary also works for the case $D(f) = -4$. There is no need for us to give this here, since by our previous remark it suffices to study the equation*

$$y^q = x^2 + 1,$$

which was shown to have no non-trivial solutions by Lebesgue in [27].

Bugeaud [16] (with a correction by Bilu [9]) proved that for D_1, D_2 squarefree positive integers, the only solutions of the Diophantine equation

$$D_1 x^2 + D_2^m = 4y^n$$

in positive integers x, y, m odd, $n \geqslant 5$ prime with $\gcd(D_1 x, D_2 y) = 1$ and $\gcd(n, h(\mathbb{Q}(\sqrt{-D_1 D_2}))) = 1$ are given by

$$(y, n) \in \{(2,5), (2,7), (2,13), (3,5), (3,7), (4,7), (5,7)\}.$$

Our main results can be extracted from Bugeaud's. The approach here also uses the deep result of Bilu, Hanrot and Voutier [10] but is more explicit in that we identify (in the case $D_1 = m = 1$) the equations where each of these powers appear. Many special forms of this equation have been considered via similar methods in the papers [3, 4] and the survey article [2].

1.1. Applications. The above results can be used in the explicit determination of all perfect power terms in sequences generated by certain quadratic polynomials. The study of perfect power terms in integer sequences is becoming increasingly popular. In [32], it is shown using Baker-type estimates that any non-degenerate binary linear recurrence sequence has only a finite number of terms which are perfect powers, and in [33] the same result was proven for non-degenerate n-th order linear recurrences. In [19] it is shown that the only squares in the Fibonacci sequence are 0,1,144 and in [29] it is shown using transcendence methods that the only cubes in the Fibonacci sequence are 0,1,8. In [17] it is shown that 0,1,8,144 are the only perfect power terms in the Fibonacci sequence, which was a long standing open problem. This result uses a combination of Baker theory and the modular method which has grown out of Wiles' proof of Fermat's last theorem. In addition, for results on perfect powers in arithmetic progressions see the papers [6, 22, 24] which also use a combination of classical methods and the modular method.

The sequences that interest us are the following.

Definition 1.4. *Let $g_m(x) = x^2 - mx + m$ where $m \in \mathbb{N}$ and furthermore choose $a \in \mathbb{N}$ such that $a > m$ and $\gcd(a, m) = 1$. Fix $m \neq 0, 4$ and define a sequence $G^{(m)}(a) = (G_n^{(m)}(a))_{n \geqslant 0}$ where $G_n^{(m)}(a) = g_m^n(a)$, for g_m^n the n-th iterate of g_m. We will call $G^{(m)}(a)$ a generalised Sylvester sequence of type m.*

Remark. *Note that the assumption $a > m$ will ensure that the terms of these sequences are positive and strictly increasing, and therefore the sequence is not eventually periodic.*

This class of sequences contains, as special cases, the Fermat numbers [36, A000058] which is $G^{(2)}(3)$ and the Sylvester sequence $G^{(1)}(2)$ [36, A000215]. It was shown by Mohanty in [28] that the n-th term $G_n^{(m)}(a)$, of a generalised Sylvester sequence of type m satisfies the following special recurrence relation,

$$G_n^{(m)}(a) = m + (a-m)G_0^{(m)}(a)G_1^{(m)}(a)...G_{n-1}^{(m)}(a),$$

which when combined with an easy congruence condition allows one to show that any two distinct terms of the sequence are coprime. Aside from this the Sylvester sequence has some unusual properties which make it especially interesting. The Sylvester sequence has the property that its n-th term is the closest integer to H^{2^n} for some real number $H > 0$, see [36]. In fact this property holds for all sequences $G^{(1)}(a)$, and in general $G_n^{(m)}(a)$ is the closest integer to $H_1^{2^n} + \frac{m-1}{2}$ for some real number $H_1 > 0$, (see [20]) which can be derived from the work done in [21]. The Sylvester sequence gives a way of obtaining infinitely many Egyptian fraction representations of 1, see [36]. A consequence of Corollary 1.3 is that the Sylvester sequence has no terms which are perfect powers. This fact seems not to have been previously established, all that has been known is that there are no terms in $G^{(1)}(2)$ which are squares, [36]. In fact we can deduce much more.

Corollary 1.5. *The only perfect power terms in a generalised Sylvester sequence of type 1 are $G_0^{(1)}(a)$ when a is itself a perfect power, and $G_1^{(1)}(19)$.*

We therefore know exactly which inputs give rise to perfect power terms and the position of these perfect powers in the sequence. The methods which we apply can also be used to give results for generalised Sylvester sequences of types 2 and 3.

2. Proofs of the Main Results

Throughout this section for α a quadratic algebraic integer we denote by $\bar{\alpha}$, the algebraic conjugate of α not equal to α and by $u_n(\alpha, \bar{\alpha})$, the expression $\frac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}}$. In addition by $\langle x \rangle$ we will mean the principal ideal generated by x. We begin with a few definitions which will allow us to state the theorem of Bilu, Hanrot and Voutier that is instrumental in the proof of Theorems 1.1, 1.2 and hence Corollary 1.3.

Definition 2.1. *A Lucas pair is a pair of algebraic integers (α, β) such that $\frac{\alpha}{\beta}$ is not a root of unity and $\alpha + \beta, \alpha\beta$ are non-zero coprime rational integers.*

For a Lucas pair $(\alpha, \bar{\alpha})$ the sequence $(u_n(\alpha, \bar{\alpha}))_{n \geqslant 1}$ is called the Lucas sequence associated to α. We now give the classical definition of a primitive prime divisor of a term in a Lucas sequence.

Definition 2.2. *A prime divisor p of $u_n(\alpha, \bar{\alpha})$ is called a primitive prime divisor of $u_n(\alpha, \bar{\alpha})$ if $p \nmid (\alpha - \bar{\alpha})^2 u_1(\alpha, \bar{\alpha}) ... u_{n-1}(\alpha, \bar{\alpha})$.*

However for the purposes of this paper, the following definition is more convenient and will be used throughout.

Definition 2.3. *Let $A = (a_i)_{i \geqslant 1}$ be an integer sequence. We say that a prime p is a primitive prime divisor of a_n if $p \mid a_n$ but $p \nmid a_m$ for any $m < n$ with $a_m \neq 0$.*

The reason that we use Definition 2.3 in this work is because it reduces the amount of case checking that needs to be done in the proofs of Theorem 1.2 and Corollary 1.3.

Theorem 2.4 (**Bilu, Hanrot and Voutier** [10])**.** *Let $a, b, n \in \mathbb{Z}$ with $4 < n \leqslant 30$ and $n \neq 6$. Then, up to equivalence, all Lucas pairs $(\alpha, \bar{\alpha}) = (\frac{a+\sqrt{b}}{2}, \frac{a-\sqrt{b}}{2})$ and n such that $u_n(\alpha, \bar{\alpha})$ fails to have a primitive prime divisor (in the context of Definition 2.3) are listed in the following table.*

n	(a, b)
5	$(1, -7), (1, -11), (12, -76), (12, -1364)$
7	$(1, -19)$
8	$(2, -24), (1, -7)$
10	$(2, -8), (5, -3), (5, -47)$
12	$(1, 5), (1, -7), (1, -11), (2, -56), (1, -15), (1, -19)$
13	$(1, -7)$
18	$(1, -7)$
30	$(1, -7)$

In particular, for all Lucas pairs $(\alpha, \bar{\alpha})$, $u_n(\alpha, \bar{\alpha})$ has a primitive prime divisor for each $n > 30$.

For a complete list of all such Lucas pairs $(\alpha, \bar{\alpha})$ such that $u_n(\alpha, \bar{\alpha})$ fails to have a primitive prime divisor (in the context of Definition 2.2) for $n = 2, 3, 4, 6$ see the paper [1].

Remark. *Here two Lucas pairs $(\alpha, \bar{\alpha})$ and $(\beta, \bar{\beta})$ are said to be equivalent if $\frac{\alpha}{\beta} = \frac{\bar{\alpha}}{\bar{\beta}} = \pm 1$. Thus, it is clear that if $(\alpha, \bar{\alpha})$ and $(\beta, \bar{\beta})$ are equivalent, then $u_n(\alpha, \bar{\alpha}) = u_n(\beta, \bar{\beta})$ for all $n \in \mathbb{N}$.*

Now we have everything that is needed to prove the results stated in the introduction.

Proof of Theorem 1.1. Factorise $f(x)$ over the ring of integers R of $\mathbb{Q}(\sqrt{D(f)})$ to obtain

$$y^q = x^2 + ax + b = (x - \alpha)(x - \bar{\alpha}).$$

where $\alpha = \frac{-a+\sqrt{D(f)}}{2}$. The ring R is not a unique factorisation domain, so we work with ideals. Hence

$$\langle y \rangle^q = \langle x - \alpha \rangle \langle x - \bar{\alpha} \rangle. \tag{2.1}$$

Now let $\mathfrak{p}$ be a prime ideal dividing both $\langle x - \alpha \rangle, \langle x - \bar{\alpha} \rangle$, so

$$x - \alpha \in \mathfrak{p} \quad \text{and} \quad x - \bar{\alpha} \in \mathfrak{p}$$

and thus

$$\alpha - \bar{\alpha} = \sqrt{D(f)} \in \mathfrak{p}.$$

It follows that $D(f) \in \mathfrak{p}$. In addition, $\mathfrak{p} \mid (x - \alpha)(x - \bar{\alpha}) = y^q$, thus $\mathfrak{p} \mid y$ and hence $y \in \mathfrak{p}$. We now claim that $D(f)$ and y are coprime. Suppose not. Then $\gcd(D(f), y) = p_1 \cdots p_r$, for some $r \in \mathbb{N}$ where the p_i's are distinct rational primes. Also

$$4y^q = (2x + a)^2 - D(f)$$

and so $p_1 \cdots p_r \mid (2x + a)$. Then for some integers k_1, k_2, k_3 with $p_i \nmid k_3$ for each i, we have

$$4p_1^q \cdots p_r^q k_1 = p_1^2 \cdots p_r^2 k_2 + p_1 \cdots p_r k_3$$

so that

$$4p_1^{q-1} \cdots p_r^{q-1} k_1 = p_1 \cdots p_r k_2 + k_3$$

which implies $p_i \mid k_3$, a contradiction. Hence $D(f), y$ are coprime and thus there exist integers $m, n \in \mathbb{Z}$ with

$$my + nD(f) = 1.$$

This in turn implies that $1 \in \mathfrak{p}$, a contradiction to the fact that $\mathfrak{p}$ is prime. Hence $\langle x - \alpha \rangle, \langle x - \bar{\alpha} \rangle$ are coprime, and so by (2.1), we have

$$\langle x - \alpha \rangle = I^q$$

for some integral ideal I. Since q is coprime to h and I^q is principal, I too must be principal. Therefore

$$\langle x - \alpha \rangle = \langle \beta \rangle^q = \langle \beta^q \rangle$$

for some $\beta \in R$. From which we easily deduce

$$x - \alpha = \epsilon \beta^q$$

for some unit ϵ of R. In R, the only units are ± 1 and so themselves are q-th powers. Thus

$$x - \alpha = \delta^q, \tag{2.2}$$

for some $\delta \in R$. By applying the non-trivial Galois automorphism one obtains

$$x - \bar{\alpha} = \bar{\delta}^q \tag{2.3}$$

We now claim that the pair $(\delta, \bar{\delta})$ is a Lucas pair. If either of $\delta + \bar{\delta}, \delta\bar{\delta}$ equal 0 then the equations (2.2) and (2.3) along with the condition that $D(f)$ is squarefree imply that $x \notin \mathbb{Z}$, so this is a contradiction. So both $\delta + \bar{\delta}, \delta\bar{\delta}$ are non-zero. The fact that $D(f), y$ are coprime forces $\delta + \bar{\delta}, \delta\bar{\delta}$ to be coprime also. The only roots of unity in R are ± 1 so if $\frac{\delta}{\bar{\delta}}$ is a root of unity it must be either 1 or -1. So we would have either $\delta = \pm\bar{\delta}$. If $\delta = \bar{\delta}$, then $\alpha = \bar{\alpha}$ which cannot hold as f is irreducible over $\mathbb{Q}$. If $\delta = -\bar{\delta}$, then $\delta + \bar{\delta} = 0$ and we have already ruled this out. Thus $\frac{\delta}{\bar{\delta}}$ is not a root of unity. So $(\delta, \bar{\delta})$ is indeed a Lucas pair.

Using equations (2.2) and (2.3) we see that

$$\bar{\alpha} - \alpha = \delta^q - \bar{\delta}^q.$$

and thus

$$-\sqrt{D(f)} = k\sqrt{D(f)}u_q(\delta, \bar{\delta}),$$

where k is some non-zero rational integer. Now $u_q(\delta, \bar{\delta})$ is an integer, hence $k = \pm 1$ which gives

$$u_q(\delta, \bar{\delta}) = \pm 1.$$

Therefore the q-th term of the Lucas sequence $(u_n(\delta, \bar{\delta}))_{n \geqslant 1}$ fails to have a primitive divisor, so by Theorem 2.4, coupled with the facts $D(f)$ is squarefree, $h > 1$ and q is prime means that $q \leqslant 3$. We have not taken into account the case where q is not coprime to h. When $q \mid h$, the above method does not apply as I^q principal does not imply I principal in general. So for these values of q, we need to solve the equation $y^q = f(x)$ by hand. □

Remark. *Actually, the proof of the above theorem tells us that we only need to check the cases $q = 2, 3$ and q is a prime divisor of h. So we only need check at most $2 + \omega(h)$ cases, where $\omega(h)$ is the number of prime factors of h.*

Proof of Theorem 1.2. Let $f(z) = z^2 + az + b$ be such that $a, b \in \mathbb{Z}$ and with discriminant $D(f)$ where $-D(f) \in \{7, 11, 19, 43, 67, 163\}$. Let R be the ring of integers of the splitting field of f over $\mathbb{Q}$. In addition, let us assume $q > 30$ and that there are integers x, y which satisfy equation (1.1). We have the factorisation of $f(x)$ as $(x - \alpha)(x - \bar{\alpha})$, for $\alpha = \frac{-a + \sqrt{D(f)}}{2}$. We may assume that $x - \alpha$ and $x - \bar{\alpha}$ are coprime in R. If $x - \alpha$ and $x - \bar{\alpha}$ have a common factor $d \in R$, then d has to divide $\sqrt{D(f)}$, which is a prime of R as $D(f)$ is a rational prime. This means that d is either a unit or a unit

multiple of $\sqrt{D(f)}$. Assume that $d = \pm\sqrt{D(f)}$ then we can re-write our equation $y^q = f(x)$ as

$$y^q = D(f)\left(\frac{x-\alpha}{\sqrt{D(f)}}\right)\left(\frac{x-\bar{\alpha}}{\sqrt{D(f)}}\right). \tag{2.4}$$

Now the terms on the RHS of (2.4) are pairwise coprime. We know that the two bracketed terms are coprime so all we need to check is that $D(f)$ has no factors in common with $A = \frac{x-\alpha}{\sqrt{D(f)}}$ say. Suppose that ϵ is a non-trivial common factor of A and $D(f)$, then as $\epsilon \mid D(f)$ we have $\epsilon = \pm\sqrt{D(f)}$ or $\pm D(f)$. Applying the non-trivial Galois automorphism tells us that $\bar{\epsilon} = \pm\epsilon$. Now $\bar{\epsilon} \mid \bar{A}$, so $\epsilon \mid \bar{A}$ also. This is a contradiction and so ϵ must be a unit. Hence, as R is a unique factorisation domain, each of $D(f), A, \bar{A}$ is a unit multiple of a q-th power. However, since $q > 2$, $D(f)$ is not a q-th power so there are no integer solutions to (2.4). Therefore we assume that $x - \alpha$ and $x - \bar{\alpha}$ are coprime in R. Then equation (1.1) implies that

$$x - \alpha = \pm\beta^q,$$

for some $\beta \in R$. Once again ± 1 are q-th powers so

$$x - \alpha = \gamma^q$$

for some $\gamma \in R$. Applying the non-trivial Galois automorphism yields

$$x - \bar{\alpha} = \bar{\gamma}^q.$$

The last two equations imply that

$$\bar{\alpha} - \alpha = \gamma^q - \bar{\gamma}^q,$$

which in turn yields

$$-\sqrt{D(f)} = k\sqrt{D(f)}u_q(\gamma, \bar{\gamma}),$$

for some non-zero $k \in \mathbb{Z}$. Once again $k = \pm 1$ which gives

$$u_q(\gamma, \bar{\gamma}) = \pm 1. \tag{2.5}$$

As before we can now apply the result of Theorem 2.4 to conclude that $u_q(\gamma, \bar{\gamma})$ has a primitive prime divisor for all $q > 30$ and equation (2.5) is therefore untenable. Hence for (1.1) to be soluble in integers x, y we require that $q \leqslant 30$.

We will now prove the statement for $D(f) = -7$; the other cases follow similarly. Assume that we have a solution to (1.1) for $q > 13$. Then we know that equation (2.5) holds for some $\gamma \in \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, and the qth term in the Lucas sequence $(u_n(\gamma, \bar{\gamma}))_{n\geqslant 1}$ fails to have a primitive prime divisor. From Theorem 2.4 we have a complete list of conjugate pairs $(\gamma, \bar{\gamma})$ and positive integers n such that $u_n(\gamma, \bar{\gamma})$ fails to have a primitive prime divisor. By the

equivalence condition of Theorem 2.4 we may assume that the only candidate for γ is $\frac{1+\sqrt{-7}}{2}$, consequently the only $n > 13$ for which $u_n(\gamma, \bar{\gamma})$ fails to admit a primitive prime divisor, are $n = 18, 30$. Computing the values of $u_n\left(\frac{1+\sqrt{-7}}{2}, \frac{1-\sqrt{-7}}{2}\right)$ for $n = 18, 30$, the values ± 1 are never obtained, so there are no solutions to (2.5) when $q > 13$, which establishes the result for $D(f) = -7$.

We are now left to prove the claims when $D(f) = -3, -8$. Let $f(x) = x^2 + ax + b$ be an integral polynomial of discriminant -3 (as before, the case $D(f) = -8$ is similar). Then for integers x, y, $y > 1$ with

$$y^q = x^2 + ax + b,$$

we have the factorisation

$$y^q = (x - \alpha)(x - \bar{\alpha}), \tag{2.6}$$

where $\alpha = \frac{-a+\sqrt{-3}}{2}$. Note that the RHS of equation (2.6) lies in the ring $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$. As before we may assume that $x - \alpha$ and $x - \bar{\alpha}$ are coprime in $\mathbb{Z}[\omega]$. Therefore, we have from equation (2.6)

$$x - \alpha = \delta \cdot \gamma^q \tag{2.7}$$

where $\gamma, \delta \in \mathbb{Z}[\omega]$ with δ a unit.

Since δ is a unit, it is itself a q-th power (as q is a prime larger than 3) then from equation (2.7) we have

$$x - \alpha = \epsilon^q, \tag{2.8}$$

for some $\epsilon \in \mathbb{Z}[\omega]$. Again applying the non-trivial Galois automorphism gives

$$x - \bar{\alpha} = \bar{\epsilon}^q. \tag{2.9}$$

Subtracting (2.9) from (2.8) gives

$$\epsilon^q - \bar{\epsilon}^q = \bar{\alpha} - \alpha = -\sqrt{-3}.$$

Factorising the LHS of the above gives

$$(\epsilon - \bar{\epsilon}) u_q(\epsilon, \bar{\epsilon}) = -\sqrt{-3}.$$

Note that $\epsilon - \bar{\epsilon} = c\sqrt{-3}$ for some non-zero integer c. Hence,

$$c u_q(\epsilon, \bar{\epsilon}) = -1,$$

and since $u_q(\epsilon, \bar{\epsilon})$ is an integer we know $c \mid 1$. So $c = \pm 1$ and we end up with the following equation

$$u_q(\epsilon, \bar{\epsilon}) = \pm 1. \tag{2.10}$$

It follows immediately from Theorem 2.4, that $u_q(\epsilon, \bar{\epsilon})$ has a primitive prime divisor for all $q > 30$, so for (2.10) to hold we must have $q < 30$. Moreover, the only pairs $(n, \gamma) \in \mathbb{N} \times \mathbb{Z}[\omega]$ with $n > 4$ such that $u_n(\gamma, \bar{\gamma})$ fails to have a

primitive prime divisor are $\left(10, \pm\left(\frac{5\pm\sqrt{-3}}{2}\right)\right)$. Since q is prime, we conclude that there are no solutions to (2.10). □

Now consider Corollary 1.3. Once again, we will prove only the case that $D(f) = -7$ since the other cases follow similarly and this is the situation which gives rise to the highest bound for the exponent q.

Proof of Corollary 1.3. Note that for the equation

$$y^q = f(x)$$

to have integer solutions x, y with $|y| > 1$ we have that equation (2.5) holds, where $\gamma \in \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$. As in the proof of Theorem 1.2 the only candidate for γ is $\frac{1+\sqrt{-7}}{2}$. When $\gamma = \frac{1+\sqrt{-7}}{2}$, we see that equation (2.5) for $q \geqslant 5$ is only satisfied for $q = 5, 13$. It may be assumed that q is prime. Therefore, to fully solve this equation we need only look at the cases $q = 2, 3, 5, 13$. Without loss take $f(x) = x^2 + x + 2$, since it has discriminant -7. First solve the equation $y^2 = f(x)$ in integers x, y. Completing the square gives

$$y^2 = \left(x + \frac{1}{2}\right)^2 + 7/4$$

and multiplying through by 4 gives

$$(2y)^2 = (2x + 1)^2 + 7$$

and so

$$(2y - 2x - 1)(2y + 2x + 1) = 7.$$

So it is clear that $(2y - 2x - 1) = \pm 1, \pm 7$ and running through the possibilities yields that $x = -2, 1$ and $y = 2$.

The zeros of f are $\alpha = \frac{-1+\sqrt{-7}}{2}$ and $\bar{\alpha} = \frac{-1-\sqrt{-7}}{2}$, so

$$y^q = (x - \alpha)(x - \bar{\alpha}).$$

As in the proof of Theorem 1.2 assume that the two factors on the RHS of the equation are coprime. Therefore

$$x - \alpha = \pm\beta^q,$$

for some $\beta \in \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. We only need to check the cases $q = 3, 5, 13$. Now -1 is a perfect q-th power, so

$$x + \frac{1 - \sqrt{-7}}{2} = \epsilon^q,$$

for some $\epsilon \in \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Write $\epsilon = \frac{U+V\sqrt{-7}}{2}$ then substituting in the above gives

$$2^q x + 2^{q-1} - 2^{q-1}\sqrt{-7} = (U + V\sqrt{-7})^q. \tag{2.11}$$

First deal with the case $q = 13$. Expanding out the bracket in equation (2.11) and equating real and imaginary parts yields

$$f_1(U, V) = -4096 \tag{2.12}$$

$$g_1(U, V) = 8192x + 4096 \tag{2.13}$$

where

$$\begin{aligned} f_1(U,V) = V(&13U^{12} - 2002U^{10}V^2 + 63063U^8V^4 - 588588U^6V^6 \\ &+ 1716715U^4V^8 - 1310946U^2V^{10} + 117649V^{12}) \end{aligned}$$

and

$$\begin{aligned} g_1(U,V) = &U^{13} - 546U^{11}V^2 + 35035U^9V^4 - 588588U^7V^6 + 3090087U^5V^8 \\ &- 4806802U^3V^{10} + 1529437UV^{12}. \end{aligned}$$

From (2.12), $V \mid 4096$. Using the polroots command in PARI, see [18], we compute polroots$\left(f(x) + \frac{4096}{V}\right)$ where

$$f(x) = \frac{f_1(x, V)}{V}$$

where V is fixed and takes on the values $\pm 2^d$ where d runs from 0 to 12 inclusive. We find the integer solutions to (2.12) to be

$$V = 1, U = \pm 1.$$

This implies that

$$g_1(U, V) = \pm 741376$$

which, by substituting into (2.13), yields $x = -91$ or 90 and so we conclude that $y = 2$. By substituting $q = 5$ into equation (2.11) and solving in the same way we find that the only solutions to

$$y^5 = x^2 + x + 2$$

are $x = -6, 5$ and $y = 2$. Similarly for $q = 3$ we find that the only solutions to

$$y^3 = x^2 + x + 2$$

are $x = -3, 2$ and $y = 2$. Therefore, from the remark below Theorem 1.2, the only solutions to the equation $y^q = f(x)$ where $f(x)$ has discriminant -7 are $y = 2$ and $q = 2, 3, 5, 13$ and so we have proven part (a) of Corollary 1.3. □

3. Applications to polynomially generated sequences

In this section we show how Theorems 1.1,1.2 and Corollary 1.3 can be applied to deduce perfect power results for generalised Sylvester sequences of types 1,2 and 3.

Proof of Corollary 1.5. We are looking to solve the equation $y^q = x^2 - x + 1$ in integers x, y, q where $y, q > 1$. Since $x^2 - x + 1$ has discriminant equal to -3 we see from Corollary 1.3 that the only integer solution (y, q) to this equation is $(7, 3)$. Hence if we have a perfect power term in such a sequence, the previous term x must satisfy

$$x^2 - x + 1 = 343.$$

Solving the previous equation gives $x = -18, 19$. So to see 343 appearing in our generalised Sylvester sequence of type 1, we see that the previous term needs to be 19, since all terms in the sequence are positive. However, 19 is not the image of any integer under the mapping $z \to z^2 - z + 1$, so if we have 343 appearing it must be because we have chosen 19 as our initial input. This concludes the proof. □

Remark. *From the above result, we see that the Sylvester sequence has no perfect powers since it is* $G^{(1)}(2)$.

Lemma 3.1. *The only perfect power terms in a generalised Sylvester sequence of type 2 are* $G_0^{(2)}(a)$ *when* a *is a perfect power.*

Proof. We are looking for integer solutions to the equation

$$y^q = x^2 - 2x + 2.$$

The polynomial on the RHS of the above has discriminant equal to -4, and so by the remark below Theorem 1.2, we can invoke Lebesgue's result, [27] to show that this equation has no integer solution (x, y) with $y > 1$. □

Corollary 3.2. *The only perfect power terms in a generalised Sylvester sequence of type 3 are* $G_0^{(3)}(a)$ *when* a *is a perfect power, and* $G_1^{(3)}(20)$.

Proof. To see this, we simply observe that generalised sequences of type 3 are more or less the same as those of type 1. Since $x^2 - 3x + 3 = (x - 1)^2 - (x - 1) + 1$, we see that $G^{(3)}(a) = G^{(1)}(a - 1)$. The statement of this corollary then follows from Corollary 1.5. □

We finish with an example to illustrate that the bound in Theorem 1.1 is sharp, and to show how we can find all power terms in the sequences coming from this polynomial by iterating it upon an integral input.

Example 3.3. *Let* $f(x) = x^2 + x + 6$. *We wish to solve the equation* $y^q = f(x)$ *in integers* x, y, $q \geqslant 2$. *Note that* $D(f) = -23$, *so* $f(x)$ *satisfies the hypotheses of Theorem 1.1 and we conclude at once that* $q \leqslant 3$ *since*

$h(\mathbb{Q}(\sqrt{-23})) = 3$. *To show that our bound is sharp we need only show there are solutions when* $q = 3$. *When* $q = 3$ *the equation defines an elliptic curve and the equation can be solved by using the MAGMA package,* [12]. *We find that the integer solutions to the equation are*

$$(x, y) \in \{(22, 8), (-23, 8), (-42, 12), (41, 12), (-2, 2), (1, 2), (14, 6), (-15, 6), (3625, 236), (-3626, 236)\}.$$

The case $q = 2$ *is straightforward, we can rearrange the equation a little to obtain*

$$(2y - 2x - 1)(2y + 2x + 1) = 23.$$

Using the fact that the two factors on the LHS are factors of 23 gives that the only solutions in this case are

$$(x, y) \in \{(5, \pm 6), (-6, \pm 6)\}.$$

As before we can now use this information to show that for $n \geqslant 1$, $a \in \mathbb{Z}$, $f^n(a)$ *is a perfect power exactly when* $n = 1$ *and*

$$a = -3626, -42, -23, -15, -6, -2, 1, 5, 14, 22, 41, 3625.$$

Hence no term beyond the first in the sequence $(f^n(a))_{n\geqslant 1}$ *is a perfect power.*

References

[1] M. ABOUZAID, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Théor. Nombres Bordeaux, 18 (2006), pp. 299–313.

[2] F. S. ABU MURIEFAH AND Y. BUGEAUD, *The Diophantine equation* $x^2 + c = y^n$*: a brief overview*, Rev. Colombiana Mat., 40 (2006), pp. 31–37.

[3] S. A. ARIF AND F. S. ABU MURIEFAH, *On the Diophantine equation* $x^2 + q^{2k+1} = y^n$, J. Number Theory, 95 (2002), pp. 95–100.

[4] S. A. ARIF AND A. S. AL-ALI, *On the Diophantine equation* $x^2 + p^{2k+1} = 4y^n$, Int. J. Math. Math. Sci., 31 (2002), pp. 695–699.

[5] A. BAKER, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc., 65 (1969), pp. 439–444.

[6] M. A. BENNETT, N. BRUIN, K. GYŐRY, AND L. HAJDU, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. (3), 92 (2006), pp. 273–306.

[7] M. A. BENNETT, K. GYŐRY, M. MIGNOTTE, AND Á. PINTÉR, *Binomial Thue equations and polynomial powers*, Compos. Math., 142 (2006), pp. 1103–1121.

[8] A. BÉRCZES, B. BRINDZA, AND L. HAJDU, *On the power values of polynomials*, Publ. Math. Debrecen, 53 (1998), pp. 375–381.

[9] Y. BILU, *On Le's and Bugeaud's papers about the equation* $ax^2 + b^{2m-1} = 4c^p$, Monatsh. Math., 137 (2002), pp. 1–3.

[10] Y. BILU, G. HANROT, AND P. M. VOUTIER, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math., 539 (2001), pp. 75–122. With an appendix by M. Mignotte.

[11] Y. F. BILU AND G. HANROT, *Solving superelliptic Diophantine equations by Baker's method*, Compositio Math., 112 (1998), pp. 273–312.

[12] W. BOSMA, J. CANNON, AND C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. Computational algebra and number theory (London, 1993).

[13] B. BRINDZA, *On S-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hungar., 44 (1984), pp. 133–139.

[14] B. Brindza, J.-H. Evertse, and K. Győry, *Bounds for the solutions of some Diophantine equations in terms of discriminants*, J. Austral. Math. Soc. Ser. A, 51 (1991), pp. 8–26.
[15] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Math., 107 (1997), pp. 187–219.
[16] ———, *On some exponential Diophantine equations*, Monatsh. Math., 132 (2001), pp. 93–97.
[17] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2), 163 (2006), pp. 969–1018.
[18] H. Cohen, *Pari-gp.* `www.parigp-home.de`.
[19] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc., 39 (1964), pp. 537–540.
[20] A. Flatters, *Arithmetic properties of recurrence sequences*, PhD thesis, University of East Anglia, 2010.
[21] S. W. Golomb, *On certain nonlinear recurring sequences*, Amer. Math. Monthly, 70 (1963), pp. 403–405.
[22] K. Győry, L. Hajdu, and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compos. Math., 145 (2009), pp. 845–864.
[23] K. Győry, I. Pink, and A. Pintér, *Power values of polynomials and binomial Thue-Mahler equations*, Publ. Math. Debrecen, 65 (2004), pp. 341–362.
[24] K. Győry and Á. Pintér, *Almost perfect powers in products of consecutive integers*, Monatsh. Math., 145 (2005), pp. 19–33.
[25] K. Győry and Á. Pintér, *On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$. I*, Publ. Math. Debrecen, 70 (2007), pp. 483–501.
[26] ———, *Polynomial powers and a common generalization of binomial Thue-Mahler equations and S-unit equations*, in Diophantine equations, vol. 20 of Tata Inst. Fund. Res. Stud. Math., Tata Inst. Fund. Res., Mumbai, 2008, pp. 103–119.
[27] V. Lebesgue, *Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$*, Nouv. Ann. Math., 9 (1850), pp. 178–181.
[28] S. P. Mohanty, *The number of primes is infinite*, Fibonacci Quart., 16 (1978), pp. 381–384.
[29] A. Pethő, *Full cubes in the Fibonacci sequence*, Publ. Math. Debrecen, 30 (1983), pp. 117–127.
[30] D. Poulakis, *Solutions entières de l'équation $Y^m = f(X)$*, Sém. Théor. Nombres Bordeaux (2), 3 (1991), pp. 187–199.
[31] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith., 31 (1976), pp. 199–204.
[32] T. N. Shorey and C. L. Stewart, *On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences*, Math. Scand., 52 (1983), pp. 24–36.
[33] ———, *Pure powers in recurrence sequences and some related Diophantine equations*, J. Number Theory, 27 (1987), pp. 324–352.
[34] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, vol. 87 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 1986.
[35] C. L. Siegel, *The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$.*, Journal L. M. S., 1 (1926), pp. 66–68.
[36] N. Sloane, *Online encyclopedia of integer sequences.* `www.research.att.com/~njas/sequences`.
[37] V. G. Sprindžuk, *The arithmetic structure of integer polynomials and class numbers*, Trudy Mat. Inst. Steklov., 143 (1977), pp. 152–174, 210. Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday).
[38] R. Tijdeman, *Applications of the Gel′fond-Baker method to rational number theory*, in Topics in number theory (Proc. Colloq., Debrecen, 1974), North-Holland, Amsterdam, 1976, pp. 399–416. Colloq. Math. Soc. János Bolyai, Vol. 13.
[39] P. M. Voutier, *An upper bound for the size of integral solutions to $Y^m = f(X)$*, J. Number Theory, 53 (1995), pp. 247–271.

Anthony Flatters
School of Mathematics
University of East Anglia
Norwich
NR4 7TJ, UK
E-mail: Anthony.Flatters@uea.ac.uk
URL: http://www.uea.ac.uk/mth/mthpeople/resstudents/aflatters