TRINOMIALS WITH INTEGRAL S-UNIT COEFFICIENTS HAVING A QUADRATIC FACTOR

ATTILA BÉRCZES, FLORIAN LUCA, ISTVÁN PINK, AND VOLKER ZIEGLER

1. Introduction

Reducibility of trinomials has been in the focus of intensive research for many decades. For general results on the reducibility of trinomials see the papers [18], [19], [20], [21] and [22] of Schinzel.

Investigating the reducibility of trinomials of the special shape

$$f(X) = X^n - BX + A \in \mathbb{Z}[X] \tag{1.1}$$

also has a long history. In 1988, Rabinowitz [14] proved that if $n = 5$, $B = \pm 1$ and $f(X)$ has an irreducible quadratic factor we then have $A \in \{\pm 1, \pm 6, \pm 15, \pm 22440, \pm 2759640\}$. Later for $B = 1$ and $n > 512880$ Chen [4], and for $n > 5$ Le [9] determined all trinomials $f(X)$ of the above shape having an irreducible quadratic factor. A similar result has been obtained for $B = -1$ and $n > 5$ by Lin [11], for $n > \max\{512900, \frac{8}{7}B\}$ by Yang [25], and for $n > \max\{30, \frac{1}{2}|B| + 1\}$ by Liu [12].

In [15], Ribenboim bounded $|A|$ by a constant depending on n and $|B|$, and $|B|$ by a constant depending on n and $|A|$ if $f(X)$ has an irreducible quadratic factor in $\mathbb{Z}[X]$. Herendi and Pethő [8] generalized the result of

Key words and phrases. trinomials, reducibility, Diophantime properties of polynomials.

The research was supported in part by the University of Debrecen, and by grants K115479 (A.B.) and NK104208 (A.B.) of the Hungarian National Foundation for Scientific Research. This paper was supported by the János Bolyai Scholarship of the Hungarian Academy of Sciences. The research was granted by the Austrian Science Fund (FWF) under the project P 24801-N26 (I.P.) This research was carried out while the author (F.L.) was a guest of the Max Planck Institute for Mathematics in Bonn, Germany between January and June 2017. He is also supported by grants CPRR160325161141 and an A-rated researcher award both from the NRF of South Africa and by grant no. 17-02804S of the Czech Granting Agency (F.L.) .

Ribenboim for trinomials of the form $X^n - BX^k + A$. We also mention a result of Bremner [3], where all the irreducible cubic factors of the trinomial $x^n + Ax^m + 1$ are explicitly determined.

Later, for $n > 40000$ Yang and Fu [24] bounded $|A|$ by a constant depending only on $|B|$ and bounded $|B|$ by a constant depending only on $|A|$, assuming that $f(X)$ has an irreducible quadratic factor in $\mathbb{Z}[X]$.

Let S be a finite set of positive primes and denote by $\mathscr{S}$ the set of all integers having no prime factors outside of S. Denote by s the cardinality of S and by P the largest prime in S. Although $\mathscr{S}$ is not a ring, we will denote by $\mathscr{S}[X]$ the set of all polynomials with coefficients in $\mathscr{S}$. However, whenever we refer to the factorization of $f(X) \in \mathscr{S}[X]$, we always mean its factorization as a polynomial in $\mathbb{Z}[X]$.

Theorem 1.1. *Assume that the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has a quadratic factor $g(X) = X^2 - bX + a \in \mathbb{Z}[X]$. Then we have one of the following cases:*

(i) $n \leq \max\{30, P + 1\}$;
(ii) $f(X) = X^{6k+2} - X + 1$, $f(X) = X^{6k+5} + X - 1$ *for* $k \in \mathbb{Z}_{>0}$, *and these polynomials are all divisible by* $X^2 - X + 1$;
(iii) $f(X) = X^{3k+2} + X + 1$ *for* $k \in \mathbb{Z}_{>0}$, *and this polynomial is divisible by* $X^2 + X + 1$;
(iv) $f(X) = X^n + (-1)^n nX + (-1)^n(n - 1)$ *for* $n \in \mathbb{Z}_{>1}$, *and these polynomials are divisible by* $X^2 + 2X + 1$;
(v) $f(X) = X^n - nX + (n - 1)$ *for* $n \in \mathbb{Z}_{>1}$, *and these polynomials are divisible by* $X^2 - 2X + 1$.

Remark. In the above theorem cases (ii) and (iii) represent infinite families of polynomials $f(X) \in \mathscr{S}[X]$ which have a quadratic factor. However, in cases (iv) and (v) there are only finitely many polynomials $f(X)$ with this property, since for a given set S there are only finitely many values of $n \in \mathbb{Z} > 0$ with the property $n \in \mathscr{S}$ and $n - 1 \in \mathscr{S}$. Indeed in this last case $x = n$ and $y = n - 1$ are solutions of the S-unit equation $x - y = 1$, which has only finitely many solutions in $x, y \in \mathscr{S}$ (see e.g. Corollary 1.1 in [23]).

Theorem 1.1 shows that there are infinite families of polynomials $f(X) = X^n - BX + A \in \mathscr{S}[X]$ divisible by $X^2 \pm X + 1$. In the next theorem, we

exclude this case, and we prove an effective finiteness theorem for polynomials $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ which have a quadratic factor different from $X^2 \pm X + 1$.

Theorem 1.2. *Let $n \geq 3$, $A, B \in \mathscr{S}$ and $\gcd(A, B) = 1$. Then the tuples (n, A, B) for which $f(X) = X^n - BX + A$ has a quadratic factor $g(X) = X^2 - bX + a$ with $g(X) \neq X^2 \pm X + 1$ belong to a finite set which can be determined effectively.*

Theorem 1.3. *Let $S := \{2, 3, 5, 7\}$ and put $M := \{3, 4, 5, 6, 7, 8, 9, 10, 15, 16, 21, 25, 28, 36, 49, 50, 64, 81, 126, 225, 2401, 4375\}$.*

(i) *Assume that the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has a quadratic factor different of $X^2 \pm X + 1$ and $X^2 \pm 2X + 1$. Then*
- *if $n = 3$ we have $\mathrm{ord}_2(AB) \leq 10$, $\mathrm{ord}_3(AB) \leq 7$, $\mathrm{ord}_5(AB) \leq 4$, $\mathrm{ord}_7(AB) \leq 4$;*
- *if $n = 4$ we have $\mathrm{ord}_2(AB) \leq 4$, $\mathrm{ord}_3(AB) \leq 4$, $\mathrm{ord}_5(AB) \leq 4$, $\mathrm{ord}_7(AB) \leq 4$;*
- *if $n \geq 5$, then $f(X)$ is one of the polynomials listed in Table 1.*

(ii) *If the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has the quadratic factor $X^2 + 2X + 1$, then we have $f(X) = X^n + (-1)^n nX + (-1)^n(n-1)$ with $n \in M$.*

(iii) *If the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has the quadratic factor $X^2 - 2X + 1$, then $f(X) = X^n - nX + (n-1)$ with $n \in M$.*

(iv) *If the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has the quadratic factor $X^2 \pm X + 1$, then $f(X)$ belongs to one of the infinite families given in (ii) and (iii) of Theorem 1.1.*

For $n = 3$, there are 736 distinct polynomials $X^3 - BX + A \in \mathscr{S}[X]$ with a quadratic factor. We do not list them in a table since it would be too long, and based on the information from Theorem 1.3 one can easily compute and list all of them. The situation is similar in the case of $n = 4$, where one can easily compute the 64 distinct quartic polynomials $X^4 - BX + A \in \mathscr{S}[X]$ having a quadratic factor.

TABLE 1

n	A	B	n	A	B	n	A	B
5	± 28	5	5	± 370440	441	7	± 280	1
5	± 15	1	6	3	± 16	7	± 10	7
5	± 6	-1	6	-2	± 5	7	± 16	-8
5	± 3	5	6	-5	± 8	7	± 15000	-875
5	± 1	-1	6	-120	± 56	8	14	± 3
5	± 54	-45	6	-8	± 8	8	1	± 1
5	± 27	9	6	24	± 80	8	162	± 567
5	± 250	-25	6	-250	± 375	8	-81	± 81
5	± 1029	-245	6	-5145	± 2744	13	90	-1

2. Properties of Lucas sequences

Let α, β be such that $\alpha + \beta$ and $\alpha\beta$ are non-zero co-prime integers, and α/β is not a root of unity. The sequence

$$U_n(\alpha, \beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{2.1}$$

is called the Lucas sequence corresponding to the Lucas pair (α, β). Whenever it is clear to which pair (α, β) the sequence $U_n(\alpha, \beta)$ corresponds then we just write U_n. In fact, $\{U_n\}_{n\geq 0}$ can also be defined as the binary recurrence sequence given by $U_n = bU_{n-1} - aU_{n-2}$ for all $n \geq 2$ with $U_0 := 0$, $U_1 := 1$, where $b := \alpha + \beta$ and $a := \alpha\beta$. Two Lucas pairs (α_1, β_1) and (α_2, β_2) are said to be equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$. A prime p is a *primitive prime divisor* of U_n if $p \mid U_n$ but $p \nmid (\alpha - \beta)^2 \cdot U_1 \dots U_{n-1}$.

For the convenience of the reader we recall a well known property of a primitive prime divisor p of U_n.

Lemma 2.1. *Let $U_n = U_n(\alpha, \beta)$ be the Lucas sequence corresponding to the Lucas pair (α, β), having companion polynomial $X^2 - bX + a$. If p is a primitive prime divisor of U_n then $n \leq p + 1$.*

Proof. Let p be a primitive prime divisor of U_n. By combining (IV.24), (IV.18) and (IV.19) of [17] we easily get that $n \mid p - (\frac{\Delta}{p})$, where $\Delta = (\alpha - \beta)^2$ is the discriminant of U_n and $(\frac{\cdot}{p})$ denotes the Legendre symbol. Thus, $n \leq p + 1$. □

We now state a shortened version of the deep theorem of Bilu, Hanrot and Voutier on primitive prime divisors of Lucas sequences which is enough for our purposes.

Proposition 2.2 (Bilu, Hanrot, Voutier [2])**.** *Consider the Lucas sequence*

$$U_n := \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

We then have the following:

- *For $n > 30$ the sequence U_n always has a primitive prime divisor.*
- *For $n = 5$ and $7 \leq n \leq 30$, U_n always has a primitive prime divisor, except when (up to equivalence) $(\alpha, \beta) = \left((c + \sqrt{d})/2, (c - \sqrt{d})/2\right)$ with the pairs (c, d) listed in Table 2.*

Table 2. Exceptional pairs (c, d)

n	(c, d)
5	$(1,5), (1,-7), (2,-40), (1,-11), (1,-15), (12,-76), (12,-1364)$
7	$(1,-7), (1,-19)$
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	$(1,-7)$

3. Proof of Theorem 1.1

We need in our proof the following fairly trivial observation.

Lemma 3.1. *Let $f(X) = X^n - BX + A \in \mathbb{Z}[X]$ be a polynomial with $\gcd(A, B) = 1$. If a polynomial $g(X) = X^2 - bX + a \in \mathbb{Z}[X]$ divides $f(X)$ then we also have $\gcd(a, b) = 1$.*

Proof. If we have $f(X) = g(X) \cdot h(X)$ with $h(X) = X^{n-2} + c_{n-3}X^{n-3} + \cdots + c_1X + c_0 \in \mathbb{Z}[X]$, then we have $A = c_0a$ and $-B = c_1a - c_0b$. Thus we have

$$\gcd(a, b) \mid \gcd(A, B) = 1,$$

which completes our proof. □

The following lemma has been used in several preceding papers (see e.g. [24]).

Lemma 3.2. *Let $f(X) = X^n - BX + A \in \mathbb{Z}[X]$ $(n \geq 3)$ and $g(X) = X^2 - bX + a \in \mathbb{Z}[X]$ be two polynomials with $a \neq 0$. Assume that $g(X) = (X - \alpha)(X - \beta)$ and denote by $U_n(\alpha, \beta)$ the Lucas sequence corresponding to the Lucas pair (α, β). Then*

$$g(X) \mid f(X) \iff B = U_n(\alpha, \beta) \quad \text{and} \quad A = a \cdot U_{n-1}(\alpha, \beta).$$

Proof. For convenience we include a short proof. We have $g(X) \mid f(X)$ if and only if $f(\alpha) = f(\beta) = 0$. By expressing A and B from this system we get $B = U_n(\alpha, \beta)$ and $A = a \cdot U_{n-1}(\alpha, \beta)$. Further, if $B = U_n(\alpha, \beta)$ and $A = a \cdot U_{n-1}(\alpha, \beta)$ we clearly get $f(\alpha) = f(\beta) = 0$. □

Proof of Theorem 1.1. Since $g(X) = X^2 - bX + a \in \mathbb{Z}[X]$ divides $f(X) = X^n - BX + A \in \mathscr{S}[X]$ and $\gcd(A, B) = 1$, by Lemma 3.1 we also have $\gcd(a, b) = 1$. Let α and β denote the two roots of g. Then, by Lemma 3.2, we see that $B = U_n(\alpha, \beta)$ and $A = aU_{n-1}(\alpha, \beta)$.

Since $\gcd(a, b) = 1$, we know that $\alpha + \beta$ and $\alpha\beta$ are non-zero co-prime integers. First assume that α/β is not a root of unity. Then $U_n(\alpha, \beta)$ is a non-degenerate Lucas sequence, and by the result of Bilu, Hanrot and Voutier (see Proposition 2.2) for $n > 30$ every U_n has a primitive prime divisor p, which, by Lemma 2.1, implies $n \leq p + 1$. Now we have $B = U_n(\alpha, \beta)$, and since $B \in \mathscr{S}$ we see that $U_n(\alpha, \beta)$ cannot have a primitive prime divisor if $n \geq P + 2$. Thus, we either have $n \leq P + 1$, or $n \leq 30$, which proves that $n \leq \max\{P + 1, 30\}$.

Now assume that α/β is a root of unity. Since $\gcd(\alpha + \beta, \alpha\beta) = 1$, we conclude that $(b, a) \in \{(1, 1), (-1, 1), (2, 1), (-2, 1)\}$ (see [16], page 6). This means that for $g(X)$ we have the possibilities $X^2 - X + 1$, $X^2 + X + 1$, $X^2 - 2X + 1$, $X^2 + 2X + 1$.

Let us first treat the case $g(X) = X^2 - X + 1$. In this case, $X^6 \equiv 1 \pmod{g(X)}$, thus $X^n \equiv X^{n \bmod 6} \pmod{g(X)}$. This shows that mod $g(X)$

we have

$$X^n \equiv \begin{cases} 1 & \text{if } n \equiv 0 \pmod 6 \\ X & \text{if } n \equiv 1 \pmod 6 \\ X-1 & \text{if } n \equiv 2 \pmod 6 \\ -1 & \text{if } n \equiv 3 \pmod 6 \\ -X & \text{if } n \equiv 4 \pmod 6 \\ -X+1 & \text{if } n \equiv 5 \pmod 6 \end{cases},$$

which shows that $X^n - BX + A \in \mathscr{S}[X]$ is divisible by $g(X)$ exactly in the cases described in (ii) of Theorem 1.1.

Next consider the case $g(X) = X^2 + X + 1$. In this case $X^3 \equiv 1 \pmod{g(X)}$, and similarly as above working modulo $g(X)$, we get

$$X^n \equiv \begin{cases} 1 & \text{if } n \equiv 0 \pmod 3 \\ X & \text{if } n \equiv 1 \pmod 3 \\ -X-1 & \text{if } n \equiv 2 \pmod 3 \end{cases}.$$

This proves that in this case $X^n - BX + A \in \mathscr{S}[X]$ is divisible by $g(X)$ exactly in the case described in (iii) of Theorem 1.1.

Now let $g(X) = X^2 + 2X + 1$. It easy to see, by induction, that $X^n \equiv (-1)^{n+1}(nX+(n-1)) \pmod{g(X)}$. Thus, $f(X) = X^n - BX + A$ is divisible by $g(X) = X^2+2X+1$ if and only if $f(X) = X^n + (-1)^n nX + (-1)^n(n-1)$.

Finally, if $g(X) = X^2 - 2X + 1$ then, by induction, we can prove that $X^n \equiv nX - (n-1) \pmod{g(X)}$. Thus, $f(X) = X^n - BX + A$ is divisible by $g(X) = X^2 + 2X + 1$ if and only if $f(X) = X^n - nX + (n-1)$.

□

4. Proof of Theorem 1.2

For the proof of Theorem 1.2, we need some well known properties of the Dickson polynomials of second kind. For convenience of the reader we collect them in the lemma below.

Let $a \in \mathbb{R}$. The polynomial

$$E_n(X, a) := \sum_{i=0}^{[n/2]} \binom{n-i}{i} (-a)^i X^{n-2i}$$

is called the Dickson polynomial of the second kind of degree n in the indeterminate X.

Lemma 4.1. *The Dickson polynomials of the second kind have the following properties:*

(i) *We have* $E_0(X,a)=1$, $E_1(X,a)=X$, *and* E_n *fulfills the recurrence relation*

$$E_{n+2}(X,a)=XE_{n+1}(X,a)-aE_n(X,a).$$

(ii) *The polynomial* $F_n(X,Y):=E_n(X,Y^2)$ *is a binary form of degree* n.

(iii) *The polynomial* $F_n(X,1)=E_n(X,1)$ *has* n *simple real roots, more precisely the* n *roots of* $F_n(X,1)$ *are* $x_j:=2\cos\frac{j\pi}{n+1}$ *for* $j=1,2,\dots,n$.

(iv) *For the elements of the Lucas sequence* $U_n(\alpha,\beta)$ *having companion polynomial* X^2-bX+a *we have*

$$U_n(\alpha,\beta)=E_{n-1}(b,a) \qquad \text{for } n=1,2,\dots.$$

Proof. For (i), see Lemma 2.3 of [10] and (ii) is trivial by the definition. For (iii), see the explanation below Lemma 2.17 of [10]. Next, (iv) is trivial because $U_n(\alpha,\beta)$ and $E_n(b,a)$ fulfill the same binary recurrence relation, and that $U_1(\alpha,\beta)=E_0(b,a)$ and $U_2(\alpha,\beta)=E_1(b,a)$. □

In the proof of Theorem 1.2, after the application of Theorem 1.1, the main idea is to reduce the problem to the finiteness of the solutions of finitely many Thue-Mahler equations. The literature on Thue-Mahler equations is very rich, so here we only mention that the finiteness of the number of solutions has been proved by Mahler [13], the first effective finiteness result concerning Thue-Mahler equations is due to Coates (1968) and the best bound on the variables in the number field case was obtained by Győry and Yu [7]. Recently, Bérczes, Evertse and Győry [1] proved effective finiteness results for Thue equations over arbitrary finitely generated domains, which is the widest generalization of Thue-Mahler equations. In our proof, we use the following effective but inexplicit result:

Lemma 4.2. *Let* K *be a quadratic number field with discriminant* D *and denote by* $\mathcal{O}_K$ *the ring of integers of* K. *Let* $F(X,Y)\in\mathcal{O}_K[X]$ *be a binary form with at least three non-proportional factors in its factorization, and let* $p_1,\dots,p_s\in\mathbb{Z}$ *be pairwise distinct positive rational prime numbers with*

$P := \max\{p_1, \dots, p_s\}$. *For* $x \in K$ *let* $\boxed{x}$ *denote the maximum of the absolute values of the conjugates of* x. *For every solution of the equation*

$$F(x, y) = p_1^{\alpha_1} \dots p_s^{\alpha_s} \qquad \text{in} \qquad x, y \in \mathcal{O}_K, \alpha_1, \dots, \alpha_s \in \mathbb{Z}_{\geq 0}.$$

for which $\gcd(x, y) = 1$ *we have*

$$\boxed{x}, \boxed{y} < C,$$

where C *is an effectively computable constant depending only on* D, F, P *and* s.

Proof. This is a special case of Theorem 7.6 in [23]. □

In the proof, we also use effective finiteness results for S-unit equations. In the case of unit equations the first finiteness result was due to Siegel (1921). For S-unit equations in the rational case the finiteness was proved by Mahler (1933) and for S-unit equations over number fields the first finiteness result follows from a theorem of Parry (1950). The first general effective result both for unit equations and for S-unit equations has been proved by Győry (1973, 1974 and 1979, respectively). The known best effective upper bounds are due to Győry and Yu [7]. Recently Evertse and Győry [6] proved effective finiteness results for unit equations in two unknowns over arbitrary finitely generated domains. In our proof, we use the following effective but inexplicit result:

Lemma 4.3. *Let* S *be a finite set of positive primes and denote by* $\mathscr{S}$ *the set of all integers having no prime factors outside of* S. *For every solution of the equation*

$$x - y = 1 \qquad \text{in } x, y \in \mathscr{S},$$

we have

$$|x|, |y| < C,$$

where C *is an effectively computable constant depending only on* S.

Proof. This is a special case of Corollary 1.1 in [23]. □

Proof of Theorem 1.2. Let $S = \{p_1, p_2, \dots, p_s\}$ be fixed with primes $p_1 < p_2 < \dots < p_s$. Assume that the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ and $n \geq 3$ has a quadratic factor $g(X) = X^2 - bX + a$ distinct of $X^2 \pm X + 1$ and of $X^2 \pm 2X + 1$. Then, by Theorem 1.1, we have

$n \leq \max\{30, P+1\}$. Recall that $g(X) = X^2 \pm X + 1$ is excluded. The case $g(X) = X^2 \pm 2X + 1$ will be treated at the end of the proof.

Fix a value of n such that $3 \leq n \leq \max\{30, P+1\}$. Let α, β be the roots of the polynomial $g(X)$ and denote by $U_k(\alpha, \beta)$ the Lucas sequence corresponding to the Lucas pair (α, β). By Lemma 3.2 we have

$$aU_{n-1}(\alpha, \beta) = A \in \mathscr{S},$$

which proves $a \in \mathscr{S}$. Thus, we have 2^s different possibilities for the square-free part of a. Let us now fix one of these possibilities, i.e. fix the square-free part of a, and denote it by d.

By Lemma 4.1 (iv) we know that $U_n(\alpha, \beta) = E_{n-1}(b, a)$, where E_k denotes the k^{th} Dickson polynomial of the second kind. By Lemma 3.2 we have $U_n(\alpha, \beta) = B \in \mathscr{S}$, which shows that

$$E_{n-1}(b, a) \in \mathscr{S}.$$

Thus, we also have

$$F_{n-1}(b, \sqrt{a}) \in \mathscr{S}, \tag{4.1}$$

where $\sqrt{a}$ denotes any of the square-roots of a and where the polynomial $F_k(X, Y) := E_k(X, Y^2)$ is a binary form of degree n (see Lemma 4.1 (ii)). Further, by the properties of Dickson polynomials (see Lemma 4.1 (iii)) $F_k(X, 1)$ has simple real roots. Thus, equation (4.1) is a Thue-Mahler equation over the field $\mathbb{Q}(\sqrt{d})$. Recall that n and d are fixed, so using Lemma 4.2 we see that we have only finitely many solutions $(b, \sqrt{a})$, which shows that there are only finitely many possibilities for a and b, thus also for α and β, and consequently (using Lemma 3.2 and the fact that n is fixed) there are also finitely many possibilities for A and B. Thus, we have proved that the tuples (n, A, B) belong to a finite set.

The last case is when $g(X) = X^2 \pm 2X + 1$. From Theorem 1.1 it follows that in this case $f(X) = X^n + (-1)^n nX + (-1)^n(n-1)$ for $n \in \mathbb{Z}_{>1}$ or $f(X) = X^n - nX + (n-1)$ for $n \in \mathbb{Z}_{>1}$. Since $A = \pm n$, $B = \pm(n-1)$ and $A, B \in \mathscr{S}$, we see that $(n, n-1)$ is a solution of the S-unit equation

$$x - y = 1, \qquad \text{in } x, y \in \mathscr{S}.$$

Thus, n is bounded by a constant depending only on S, and thus the tuples (n, A, B) again belong to a finite set.

□

5. Proof of Theorem 1.3

To prove (i), we assume that the quadratic factor of $f(X)$ is $g(X) = X^2 - bX + a$ and we denote by α, β the roots of $g(X)$ and by $U_n(\alpha, \beta)$ the Lucas sequence with companion polynomial $g(X)$. Recall that in case (i) $g(X) \neq X^2 \pm X + 1$ and $g(X) \neq X^2 \pm 2X + 1$. By Theorem 1.1 it is clear that we have $n \leq 30$. By Lemma 3.2, we have

$$g(X) \mid f(X) \iff B = U_n(\alpha, \beta) \text{ and } A = a \cdot U_{n-1}(\alpha, \beta).$$

Thus, it follows that

$$a,\ U_{n-1}(\alpha, \beta),\ U_n(\alpha, \beta) \in \mathscr{S}. \tag{5.1}$$

First let us treat the cases when $8 < n \leq 30$. Fix such a value of n. By Lemma 2.1, the primes $2, 3, 5, 7$ cannot be primitive prime divisors of $U_k(\alpha, \beta)$ for any $k > 8$, so $2, 3, 5, 7$ is not a primitive prime divisor for $U_n(\alpha, \beta)$ for our fixed n. Since $S = \{2, 3, 5, 7\}$ and $U_n(\alpha, \beta) \in \mathscr{S}$ this shows that for our fixed n the element $U_n(\alpha, \beta)$ has no primitive prime divisor at all. Thus, by (ii) of Proposition 2.2, U_n is one of the sequences listed for the respective n in Table 2. In the Table 3 below we list all possible sequences for each $8 < n \leq 30$ (if any) for which we computed a, U_{n-1}, U_n and checked that they belong to $\mathscr{S}$.

Table 3. Exceptional sequences in the cases $8 < n \leq 30$

n	(c, d)	b	a	$g(X)$	U_{n-1}	U_n
30	$(1, -7)$	1	2	$X^2 - X + 2$	8641	$5^2 \cdot 11 \cdot 89$
18	$(1, -7)$	1	2	$X^2 - X + 2$	271	$5 \cdot 17$
13	$(1, -7)$	1	2	$X^2 - X + 2$	$3^2 \cdot 5$	-1
12	$(1, 5)$	1	-1	$X^2 - X - 1$	89	$2^4 \cdot 3^2$
12	$(1, -7)$	1	2	$X^2 - X + 2$	23	$3^2 \cdot 5$
12	$(1, -11)$	1	3	$X^2 - X + 3$	$11 \cdot 23$	$2^5 \cdot 5$
12	$(2, -56)$	2	15	$X^2 - 2X + 15$	$43 \cdot 17623$	$2 \cdot 11 \cdot 13 \cdot 41$
12	$(1, -15)$	1	4	$X^2 - X + 4$	$23 \cdot 43$	$3 \cdot 7 \cdot 11$
12	$(1, -19)$	1	5	$X^2 - X + 5$	2531	$2^4 \cdot 3^3 \cdot 7$
10	$(2, -8)$	2	3	$X^2 - X + 3$	73	$2 \cdot 11$
10	$(5, -3)$	5	7	$X^2 - 5X + 7$	$2 \cdot 3 \cdot 19$	$5^2 \cdot 149$
10	$(5, -47)$	5	18	$X^2 - 5X + 18$	$7 \cdot 15193$	$5^2 \cdot 401$

From Table 3, we see that (5.1) is fulfilled only in the case of $n = 13$, $g(X) = X^2 - X + 2$ in which case we get the polynomial $f(X) = X^{13} + X + 90$, which is indeed divisible by $X^2 - X + 2$.

Now we turn to the cases $3 \leq n \leq 8$. For $0 \leq k \leq 8$, the k^{th} element of the sequence U_n is listed below:

$$\begin{aligned} &U_0 = 0, \quad U_1 = 1, \quad U_2 = b, \quad U_3 = b^2 - a, \quad U_4 = b(b^2 - 2a), \\ &U_5 = b^4 - 3ab^2 + a^2, \quad U_6 = b(b^2 - a)(b^2 - 3a), \\ &U_7 = b^6 - 5ab^4 + 6a^2b^2 - a^3 \\ &U_8 = b(b^2 - 2a)(b^4 - 4ab^2 + 2a^2) \end{aligned} \tag{5.2}$$

For each fixed $3 \leq n \leq 8$, using (5.1), we reduced our problem to an equation of the shape

$$u + v = z^2 \qquad \text{in } u, v \in \mathscr{S}, z \in \mathbb{Z},$$

and we also had some further expressions which belong to $\mathscr{S}$. The equations and further conditions in the case of each n are listed in Table 4 below.

TABLE 4. The resulting equations of the shape $u + v = z^2$

n	the equation	conditions
3	$(b^2 - a) + a = b^2$	$b \in \mathscr{S}$
4	$(b^2 - 2a) + 2a = b^2$	$b \in \mathscr{S}, b^2 - a \in \mathscr{S}$
5	$(b^2 - 2a) + 2a = b^2$	$b \in \mathscr{S}, b^4 - 3ab^2 + a^2 \in \mathscr{S}$
6	$(b^2 - 3a) + 3a = b^2$	$b \in \mathscr{S}, b^2 - a \in \mathscr{S}, b^4 - 3ab^2 + a^2 \in \mathscr{S}$
7	$(b^2 - 3a) + 3a = b^2$	$b \in \mathscr{S}, b^2 - a \in \mathscr{S}, b^6 - 5ab^4 + 6a^2b^2 - a^3 \in \mathscr{S}$
8	$(b^2 - 2a) + 2a = b^2$	$b \in \mathscr{S}, b^4 - 4ab^2 + 2a^2 \in \mathscr{S}$, $b^6 - 5ab^4 + 6a^2b^2 - a^3 \in \mathscr{S}$

Now, for every $3 \leq n \leq 8$ in Table 4 we use Theorem 7.2 of de Weger [5] to conclude (i) of Theorem 1.3.

For (ii) and (iii), we mention that Theorem 1.1 (iv) and (v) proves that in this cases we have $f(X) = X^n + (-1)^n nX + (-1)^n(n-1)$ and $f(X) = X^n - nX + (n-1)$, respectively. We also have $f(X) \in \mathscr{S}[X]$. Thus, in both cases it follows that $n \in \mathscr{S}$ and $n - 1 \in \mathscr{S}$, which means that $(n, n-1)$ is a solution of the equation

$$x - y = 1 \qquad \text{in } (x, y) \in \mathscr{S}^2.$$

However, de Weger solved this equation even for a larger set S. Thus, from his Theorem 6.3 in [5], we know that $\mathrm{ord}_2(xy) \leq 12$, $\mathrm{ord}_3(xy) \leq 7$, $\mathrm{ord}_5(xy) \leq 5$, $\mathrm{ord}_7(xy) \leq 4$. Now checking all possible values of $x, y \in S$ with these properties we conclude that n must belong to the set M.

Case (iv) is exactly covered by cases (ii) and (iii) of Theorem 1.1, which concludes the proof of Theorem 1.3.

Acknowledgements

We thank the referee for comments which improved the quality of our paper.

References

[1] A. Bérczes, J.-H. Evertse and K. Győry, Effective results for Diophantine equations over finitely generated domains, *Acta Arith.*, **163** (2014), 71–100.

[2] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.*, **539** (2001), 75–122.

[3] A. Bremner, On trinomials of type $x^n + Ax^m + 1$, *Math. Scand.*, **49** (1981), 145–155 (1982).

[4] H. J. Chen, On the quadratic factorization of $x^n - x - a$, *J. Math. (Wuhan)*, **22** (2002), 319–322.

[5] B. de Weger, *Algorithms for Diophantine Equations*, Ph.D. thesis, Leiden University, 1988.

[6] J.-H. Evertse and K. Győry, Effective results for unit equations over finitely generated integral domains, *Math. Proc. Camb. Phil. Soc.*, **154** (2013), 351–380.

[7] K. Győry and K. Yu, Bounds for the solutions of S-unit equations and decomposable form equations, *Acta Arith.*, **123** (2006), 9–41.

[8] T. Herendi and A. Pethő, Trinomials, which are divisible by quadratic polynomials, *Acta Acad. Paedagog. Agriensis, Sect. Mat. (N.S.)*, **22** (1994), 61–73.

[9] M. H. Le, Irreducible quadratic factors of the trinomial $x^n - x - a$, *J. Math. (Wuhan)*, **24** (2004), 635–637.

[10] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, vol. 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[11] M. Y. Lin, The irreducible quadratic factor of the trinomial $x^n + x - a$, *Math. Appl. (Wuhan)*, **19** (2006), 656–658.

[12] Z. W. Liu, Irreducible quadratic factors of the trinomial $x^n - bx + a$, *J. Math. (Wuhan)*, **27** (2007), 684–686.

[13] K. Mahler, Zur Approximation algebraischer Zahlen. I, *Math. Ann.*, **107** (1933), 691–730.
[14] S. Rabinowitz, The Factorization of $x^5 \pm x + n$, *Math. Mag.*, **61** (1988), 191–193.
[15] P. Ribenboim, On the factorization of $X^n - BX - A$, *Enseign. Math. (2)*, **37** (1991), 191–200.
[16] P. Ribenboim, *My numbers, my friends*, Springer-Verlag, New York, 2000, popular lectures on number theory.
[17] P. Ribenboim, *The little book of bigger primes*, Springer-Verlag, New York, 2004, second edn.
[18] A. Schinzel, On the reducibility of polynomials and in particular of trinomials, *Acta Arith.*, **11** (1965), 1–34.
[19] A. Schinzel, On reducible trinomials, *Dissertationes Math. (Rozprawy Mat.)*, **329** (1993), 83.
[20] A. Schinzel, On reducible trinomials. II, *Publ. Math. Debrecen*, **56** (2000), 575–608.
[21] A. Schinzel, On reducible trinomials. III, *Period. Math. Hungar.*, **43** (2001), 43–69.
[22] A. Schinzel, On reducible trinomials, IV, *Publ. Math. Debrecen*, **79** (2011), 707–727.
[23] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge–New York, 1986.
[24] H. Yang and R. Fu, On trinomials having irreducible quadratic factors, *Period. Math. Hungar.*, **69** (2014), 149–158.
[25] S. C. Yang, Integral-coefficient quadratic factorization of $x^n - bx + a$, *Nanjing Daxue Xuebao Shuxue Bannian Kan*, **21** (2004), 178–183.

A. Bérczes, I. Pink
Institute of Mathematics, University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: berczesa@science.unideb.hu

E-mail address: pinki@science.unideb.hu

F. Luca
School of Mathematics, Wits University
Private Bag X3, Wits 2050, Johannesburg, South Africa and
Department of Mathematics, Faculty of Sciences
University of Ostrava, 30 dubna 22, 701 03
Ostrava 1, Czech Republic

E-mail address: florian.luca@wits.ac.za

V. Ziegler
University of Salzburg
Hellbrunnerstrasse 34/I
A-5020 Salzburg, Austria

E-mail address: volker.ziegler@sbg.ac.at