Divisibility Sequences and Powers of Algebraic Integers

Joseph H. Silverman

Received: November 15, 2005

Abstract. Let α be an algebraic integer and define a sequence of rational integers $d_n(\alpha)$ by the condition

$$d_n(\alpha) = \max\{d \in \mathbb{Z} : \alpha^n \equiv 1 \pmod{d}\}.$$

We show that $d_n(\alpha)$ is a strong divisibility sequence and that it satisfies $\log d_n(\alpha) = o(n)$ provided that no power of α is in $\mathbb{Z}$ and no power of α is a unit in a quadratic field. We completely analyze some of the exceptional cases by showing that $d_n(\alpha)$ splits into subsequences satisfying second order linear recurrences. Finally, we provide numerical evidence for the conjecture that aside from the exceptional cases, $d_n(\alpha) = d_1(\alpha)$ for infinitely many n, and we ask whether the set of such n has postive (lower) density.

2000 Mathematics Subject Classification: Primary: 11R04; Secondary: 11A05, 11D61

Keywords and Phrases: divisibility sequence, multiplicative group

Introduction

A sequence of positive integers $\{d_n\}$ is called a *divisibility sequence* if it has the property

$$m|n \Longrightarrow d_m|d_n. \tag{1}$$

Well-known examples of divisibility sequences include sequences of the form $d_n = a^n - 1$, the Fibonacci sequence F_n, and elliptic divisibility sequences D_n. The first two also satisfy a linear recurrence. A complete characterization of linear recurrence divisibility sequences is given in [2]. Elliptic divisibility sequences are associated to points of infinite order on elliptic curves. Thus if $P \in E(\mathbb{Q})$, then the sequence D_n is formed by writing $x(nP) = A_n/D_n^2$, see [9].

In this paper we investigate divisibility sequences $(d_n(\alpha))_{n\geq 1}$ associated to algebraic integers $\alpha \in \bar{\mathbb{Z}}$ by the rule

$$d_n(\alpha) = \max\{d \in \mathbb{Z} : \alpha^n \equiv 1 \pmod{d}\}. \tag{2}$$

(We assume throughout that $\alpha \neq 0$ and that α is not a root of unity.) It is not difficult to show that $d_n(\alpha)$ is a divisibility sequence, and indeed that it satisfies the stronger divisibility property

$$\gcd\bigl(d_m(\alpha), d_n(\alpha)\bigr) = d_{\gcd(m,n)}(\alpha),$$

see Proposition 2.

These sequences are interesting in their own right as generalizations of the classical divisibility sequences $a^n - 1$ with $a \in \mathbb{Z}$. They are also interesting as a special case of divisibility sequences attached to points of infinite order on algebraic groups (see [8, Section 6]) for which we can prove unconditional results.

We now briefly summarize the contents of this paper. We begin in Section 1 with the proof that $d_n(\alpha)$ is a strong divisibility sequence. Section 2 contains a variety of numerical examples illustrating varied behaviors of $d_n(\alpha)$ for different choices of α. In Section 3 we prove a useful result on linear dependence of Galois conjugates, and in Section 4 we combine this with a deep result of Corvaja and Zannier [5] to prove:

Theorem 1. *Let $\alpha \in \bar{\mathbb{Z}}$ and let $d_n(\alpha)$ be the associated divisibility sequence* (2). *Then*

$$\lim_{n\to\infty} \frac{\log d_n(\alpha)}{n} = 0$$

unless either some power of α is in $\mathbb{Z}$ or some power of α is a unit in a quadratic extension of $\mathbb{Q}$.

The theorem says that aside from a few specific cases, the sequences $d_n(\alpha)$ grow slower than exponentially. One of the exceptional cases is easy to analyze. If $\alpha^r \in \mathbb{Z}$ with $|\alpha^r| \geq 2$ and if no smaller power of α is in $\mathbb{Z}$, then one easily checks that

$$d_n(\alpha) = \begin{cases} |\alpha^n - 1| & \text{if } r|n, \\ 1 & \text{if } r \nmid n. \end{cases}$$

In particular, $d_n(\alpha)$ contains a subsequence that grows exponentially.

In Section 5 we analyze the other exceptional case and give a complete description of $d_n(\alpha)$ for real quadratic units $\alpha = u + v\sqrt{D}$. If the norm of α is 1, we prove that $d_n(\alpha)$ satisfies a fourth order linear recurrence. More precisely, we show that the subsequences $d_{2n}(\alpha)$ and $d_{2n+1}(\alpha)$ both satisfy the same second order linear recurrence, but with different starting values. If the norm of α is -1, then we prove that $d_n(\alpha) = 1$ for all of the odd values of n. The subsequence of even terms $d_{2n}(\alpha) = d_n(\alpha^2)$ satisfies a fourth order linear recurrence, since α^2 has norm 1. The proofs of these statements involve elementary, but rather intricate, calculations.

Finally, in Section 6 we observe that except in the two exceptional cases, the sequences $d_n(\alpha)$ appear to include many small values. Theorem 1 says that $\log d_n(\alpha) = o(n)$, and $d_n(\alpha)$ does contain arbitrarily large values, but experimentally one finds for example that $d_n(\alpha)$ is frequently equal to $d_1(\alpha)$. We present one such experiment in Section 6 and use it to conjecture that the set

$$\{n \geq 1 : d_n(\alpha) = d_1(\alpha)\}$$

is infinite (generalizing a conjecture of Ailon and Rudnick [1]) and to ask whether this set in fact has positive (lower) density.

Acknowledgements. The author thanks Mike Rosen for his assistance in simplifying the proof of Proposition 3.

1. Divisibility sequences associated to algebraic integers

We begin by reminding the reader of some classical definitions.

Definition 1. A *divisibility sequence* is a sequence of of positive integers $(d_n)_{n\geq 1}$ with the property that

$$m|n \Longrightarrow d_m|d_n. \tag{3}$$

The sequence is *normalized* if $d_1 = (1)$, which can always be arranged by replacing d_n by d_n/d_1. A *strong divisibility sequence* satisfies the more stringent requirement that

$$d_{\gcd(m,n)} = \gcd(d_n, d_m) \qquad \text{for all } m, n \in \mathbb{N}. \tag{4}$$

Examples of strong divisibility sequences include the Fibonacci sequence and elliptic divisibility sequences.

Our principal objects of study in this note are the sequences $(d_n(\alpha))$ defined by (2). Our first task is to show that they are strong divisibility sequences.

Proposition 2. *Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer. The associated sequence $(d_n(\alpha))_{n\geq 1}$ defined by (2) is a strong divisibility sequence.*

Proof. We begin by verifying that (d_n) is a divisibility sequence, i.e., it satisfies (3). Let $m, n \in \mathbb{N}$ satisfy $m|n$ and write

$$\alpha^m - 1 = d_m v \qquad \text{and} \qquad \alpha^n - 1 = d_n w.$$

By assumption, $m|n$, so we can use the identity

$$X^N - 1 = (X-1)(X^{N-1} + X^{N-2} + \cdots + X + 1)$$

with $X = \alpha^m$ and $N = n/m$ to obtain

$$\alpha^n - 1 = (\alpha^m - 1)z \qquad \text{with } z \in \bar{\mathbb{Z}}.$$

Let $g = \gcd(d_m, d_n)$ and write

$$d_m x + d_n y = g \qquad \text{with } x, y \in \mathbb{Z}.$$

We multiply through by w and substitute to obtain

$$gw = d_m xw + d_n yw = d_m xw + d_m vzy = d_m(xw + vzy).$$

Subtituting this in above yields (note that $g|d_m$)

$$\alpha^n - 1 = d_n \cdot \frac{d_m}{g} \cdot (xw + vzy).$$

Thus $d_n d_m/g$ divides $\alpha^n - 1$. But d_n is, by definition, the largest natural number dividing $\alpha^n - 1$, so $d_m = g$. This shows that $d_m | d_n$, so (d_n) is a divisibility sequence.

We next show that (d_n) is a strong divisibility sequence, i.e., it satisfies (4). Let $m, n \in \mathbb{N}$ be arbitrary and let $k = \gcd(m, n)$. Then $k|m$ and $k|n$, so from above we know that $d_k | d_m$ and $d_k | d_n$. Therefore $d_k | \gcd(d_m, d_n)$.

To prove the opposite divisibility, we write $m = kM$ and $n = kN$. Then $\gcd(M, N) = 1$, so there are polynomials $A(X), B(X) \in \mathbb{Z}[X]$ satisfying

$$A(X) \cdot (X^M - 1) + B(X) \cdot (X^N - 1) = X - 1.$$

(To see this, it is enough to observe that the resultant of $\frac{X^M-1}{X-1}$ and $\frac{X^N-1}{X-1}$ is 1.) Substituting $X = \alpha^k$ yields

$$A(\alpha^k) \cdot (\alpha^m - 1) + B(\alpha^k) \cdot (\alpha^n - 1) = \alpha^k - 1.$$

As above, write $\alpha^m - 1 = a_m v$ and $\alpha^n - 1 = a_n w$ and let $g = \gcd(a_m, a_n)$. Then

$$g \cdot \left(A(\alpha^k) \cdot \frac{d_m}{g} \cdot v + B(\alpha^k) \cdot \frac{d_n}{g} \cdot w \right) = \alpha^k - 1,$$

where the quantity in parentheses is in $\bar{\mathbb{Z}}$. It follows that $g \le d_k$, since d_k is the largest natural number dividing $\alpha^k - 1$. We have now shown that $g \le d_k$ and $d_k | g$, which completes the proof that $d_k = g = \gcd(d_m, d_n)$. $\square$

Remark 1. The fact that $d_n(\alpha)$ is a divisibility sequence follows from the [8, Proposition 8] applied to the torus obtained by restriction of scalars from $\mathbb{Z}[\alpha]$ to $\mathbb{Z}$ of the multiplicative group $\mathbb{G}_m$. Thus Proposition 2 strengthens [8] (for certain tori) by showing that the divisibility sequence is strong. To avoid introducing unnecessary machinery, we have been content to prove here the case that we need, but we note that it is not difficult to generalize Proposition 2 to the more general setting of commutative algebraic groups studied in [8].

2. Numerical examples

In this section we look at numerical examples that illustrate different sorts of behavior.

Example 1. The most elementary example is $\alpha \in \mathbb{Z}$ with $|\alpha| > 1$, which yields most classical examples $a_n = \alpha^n - 1$ of divisibility sequences. However, there are many deep open problems for even this simple case. For example, are there infinitely many values of n for which $a_n(2)$ is prime?

Example 2. Let $\alpha = 1 + i$. The associated sequence is

$$(a_n(1+i)) = 1, 1, 1, 5, 1, 1, 1, 15, 1, 1, 1, 65, 1, 1, 1, 255, 1, 1, 1, 1025, \ldots$$

The pattern is clear and, using the fact that $\alpha^4 = -4$, it is easy to verify

$$a_n = |(-4)^{n/4} - 1| \quad \text{if } 4|n, \text{ and otherwise} \quad a_n = 1.$$

Although very elementary, we point out that for this example we have

$$\limsup_{n\to\infty} \frac{\log(a_n)}{n} = \frac{1}{4}\log(4) > 0. \tag{5}$$

Example 3. We again work in the Gaussian integers, but now we take $\alpha = 2+i$. The associated sequence is

$$(a_n(2+i)) = 1, 2, 1, 8, 1, 2, 1, 48, 1, 2, 1, 104, 1, 2, 1, 1632, 1, 2, 1, 8, 1, 2, 1, \dots$$

The pattern for $\alpha = 2+i$ is less regular than for $\alpha = 1+i$, but the data certainly suggest that all of the odd entries are equal to 1. Unfortunately, it turns out that this is not true, since $a_{27} = 109$. Indeed, 914 of the first 1000 a_n's with n odd are equal to 1, but some of them get quite large, for example $a_{1917} = 835921$. (Question: Are there infinitely many n satisfying $a_n(2+i) = 1$?)

The a_n with even n seem to fluctuate more than the odd n, and in particular, many large values appear, as is apparent from the following longer list of values:

$$\begin{aligned}(a_n(2+i)) = {} & 1, 2, 1, 8, 1, 2, 1, 48, 1, 2, 1, 104, 1, 2, 1, 1632, 1, 2, 1, 8, 1, 2, 1, 1872,\\ & 1, 2, 109, 232, 1, 1342, 1, 3264, 1, 2, 1, 3848, 149, 2, 1, 1968, 1, 2,\\ & 1, 712, 1, 2, 1, 445536, 1, 2, 1, 424, 1, 218, 1, 1392, 1, 2, 1, 69784,\\ & 1, 2, 1, 6528, 1, 2, 1, 8, 1, 2, 1, 15168816, 1, 298, 1, 8, 1, 2, 1, \dots\end{aligned}$$

It is not hard to see that $\sup a_n = \infty$. More precisely, if p is a rational prime with $p \equiv 1 \pmod 4$, then $\alpha^{p-1} \equiv 1 \pmod p$, so $p|a_{p-1}$. Hence there are infinitely many n such that $\log(a_n) \ge \log(n)$. However, this is much slower growth than (5), so we might ask whether $\log(a_n)/n$ has a positive limsup. Table 1 lists the values of a_n for those $n < 3000$ satisfying $a_n > a_m$ for all $m < n$. The table suggests that

$$\limsup_{n\to\infty} \frac{\log(a_n(2+i))}{n} = 0.$$

In Section 4 we use [5] to prove that this is indeed the case, but we note that [5] itself relies on Schmidt's subspace theorem, so is far from elementary.

Example 4. Let $\alpha = 2+\sqrt{3}$. The associated sequence is

$$\begin{aligned}(a_n(2+\sqrt{3}\,)) = {} & 1, 2, 5, 8, 19, 30, 71, 112, 265, 418, 989, 1560, 3691, 5822,\\ & 13775, 21728, 51409, 81090, 191861, 302632, 716035, 1129438,\\ & 2672279, 4215120, 9973081, 15731042, 37220045, 58709048, \dots\end{aligned}$$

The sequence clearly grows quite rapidly and regularly. We will show that it satisfies the linear recurrence

$$a_{n+4} = 4a_{n+2} - a_n.$$

In other words, if we define two subsequences using the odd and even terms, respectively,

$$b_n = a_{2n-1} \qquad \text{and} \qquad c_n = \frac{1}{2}a_{2n} \qquad \text{for } n = 1, 2, 3, \dots,$$

Then b_n and c_n satisfy the linear recurrence, $x_{n+2} = 4x_{n+1} - x_n$, with starting values 1 and 5 for b_n and 1 and 4 for c_n. This is typical for the division

n	a_n	$\log(a_n)/n$
1	1	0.0000
2	2	0.3466
4	8	0.5199
8	48	0.4839
12	104	0.3870
16	1632	0.4623
24	1872	0.3139
32	3264	0.2528
36	3848	0.2293
48	445536	0.2710
72	15168816	0.2296
96	2679453504	0.2261
144	4682401135776	0.2026
288	73018777396433948352	0.1588
576	16262888139288561844854144	0.1008
1152	288392072178343567593456815132l6	0.0629
1440	118208444086469083866098414522688	0.0513
1728	1949747046346392624042760227691249992	0.0470
2016	773127404949837686996635213979409984	0.0410
2160	5420808200020996828593211756294642430390 4	0.0434

TABLE 1. Growth of $a_n(2+i)$

sequences associated to *units* in real quadratic fields (see Section 5). As the next example shows, nonunits appear to behave quite differently.

Example 5. Let $\alpha = 2+3\sqrt{3}$. The associated sequence is

$$\begin{aligned}(a_n(2+3\sqrt{3}\,)) = {}&1, 6, 13, 24, 1, 234, 1, 48, 13, 66, 1, 34632, 1, 6, 13, 96,\\ &1, 702, 1, 264, 13, 6, 1, 346320, 1, 6, 13, 24, 59, 2574, \dots\end{aligned}$$

Notice the striking difference between this sequence and the sequence for $2+\sqrt{3}$ examined in Example 4. We will show that

$$\log\bigl(a_n(2+3\sqrt{3}\,)\bigr) = o(n),$$

so this example resembles Example 3.

3. LINEAR DEPENDENCE OF GALOIS CONJUGATES

In this section we prove an elementary result on the linear dependence of Galois conjugates. With an eye towards future applications and since the proof is no more difficult, we give a result that is more general than needed in this paper.

PROPOSITION 3. *Let K be a field with separable closure K^s, let X/K be a commutative algebraic group, which we write additively, and let $x \in X(K^s)$. Suppose that for every $\sigma \in G_{K^s/K}$, the points x and x^σ are dependent in X. Then one of the following two conditions is true:*

(a) *There is an $n \geq 1$ such that $nx \in X(K)$.*

(b) *There is an* $n \ge 1$ *such that*

$$[K(nx):K]=2, \qquad \textit{and also} \qquad \operatorname{Trace}_{K(x)/K}(x) \in X(K)_{\text{tors}}.$$

Conversely, if either (a) *or* (b) *is true, then* x *and* x^σ *are dependent for every* $\sigma \in G_{K^s/K}$.

Proof. Let $V = X(K^s) \otimes \mathbb{Q}$ and for any $y \in X(K^s)$, let V_y be the vector subspace (over $\mathbb{Q}$) of V generated by y and all of its Galois conjugates. Then $G_{K^s/K}$ acts continuously on V_y and we obtain a represenation $\rho_y : G_{K^s/K} \to \mathrm{GL}(V_y)$. The image is a finite subgroup of $\mathrm{GL}(V_y)$, which in general will yield information about y if $\dim(V_y)$ is smaller than $[K(y):K]$. We have $y^\sigma = \rho_y(\sigma)y$ in V, so there are torsion points $t_\sigma \in X(K^s)_{\text{tors}}$ so that $y^\sigma = \rho_y(\sigma)y + t_\sigma$ in $X(K^s)$. There are only finitley many distinct t_σ, so we can find an integer $n \ge 1$ such that

$$(ny)^\sigma = \rho_y(\sigma)(ny) \qquad \text{for all } \sigma \in G_{K^s/K}. \tag{6}$$

We start with the assumption that x and x^σ are dependent for all $\sigma \in G_{K^s/K}$, or equivalently, that V_x has dimension 1. Hence $\rho_x : G_{K^s/K} \to \mathrm{GL}(V_x) = \mathbb{Q}^*$, and since the image has finite order, it lies in $\{\pm 1\}$. We consider two cases depending on this image.

First, if $\operatorname{Image}(\rho_x) = \{1\}$, then (6) tells us that nx is fixed by $G_{K^s/K}$. Hence $x \in X(K)$, which verifies that x satisfies (a).

Second, suppose that $\operatorname{Image}(\rho_x) = \{\pm 1\}$, and let L be the fixed field of the kernel of ρ_x, so $[L:K]=2$. Then (6) tells us that nx is fixed by $G_{K^s/L}$, so $nx \in X(L)$, and further it tells us that if $\sigma \notin G_{K^s/L}$, then $(nx)^\sigma = -nx$. Thus $nx \notin G(K)$, so $L = K(nx)$, which gives the first part of (b). For the second part, we use the fact that $nx \in X(L)$ to compute

$$\begin{aligned} n\operatorname{Trace}_{K(x)/K}(x) &= \operatorname{Trace}_{K(x)/K}(nx) \\ &= \frac{[K(x):L]}{n}\operatorname{Trace}_{L/K}(nx) = nx + (-nx) = 0. \end{aligned}$$

This shows that $\operatorname{Trace}_{K(x)/K}(x)$ is in $X(K)_{\text{tors}}$, which completes the proof that x satisfies (b)

We will not need the opposite implication, but for completeness, we sketch the proof. First, if $nx \in X(K)$, then for every $\sigma \in G_{K^s/K}$ we have $x^\sigma = x + t_\sigma$ for some n-torsion point $t_s \in X(K^s)_{\text{tors}}$. Hence $nx^\sigma - nx = 0$, so x^σ and x are dependent.

Next suppose that $[K(nx):K]=2$ and $\operatorname{Trace}(x) \in X(K)_{\text{tors}}$. Let $\sigma \in G_{K^s/K}$. If σ fixes $K(nx)$, then $(nx)^\sigma - nx = 0$, so $(nx)^\sigma$ and nx are dependent. If σ does not fix $K(nx)$, then

$$\begin{aligned} [K(x):K(nx)]\big((nx)^\sigma + nx\big) &= [K(x):K(nx)]\operatorname{Trace}_{K(nx)/K}(nx) \\ &= \operatorname{Trace}_{K(x)/K}(nx) \\ &= n\operatorname{Trace}_{K(x)/K}(x) \in X(K)_{\text{tors}}. \end{aligned}$$

This proves that $(nx)^\sigma$ and nx are dependent, which completes the proof of the theorem. $\square$

We state as a corollary the special case that is needed later.

COROLLARY 4. *Let $\alpha \in \bar{\mathbb{Q}}^*$ and suppose that for every $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$, the elements α and α^σ are multiplicatively dependent. Then there is an integer $n \geq 1$ so that one of the following is true.*

(a) $\alpha^n \in \mathbb{Q}$.
(b) $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] = 2$ *and* $\mathrm{N}(\alpha) = \pm 1$.

Proof. Apply Proposition 3 to the multiplicative group $\mathbb{G}_m/\mathbb{Q}$ and note that the torsion subgroup of $\mathbb{G}_m(\mathbb{Q})$ consists only of ± 1. □

4. THE GROWTH OF DIVISIBILITY SEQUENCES

In this section we apply Corvaja and Zannier's recent results [5] on generalized greatest common divisors (see also [3, 4]) to bound the growth rate of divisibility sequences $(d_n(\alpha))$. More precisely, Theorem 5 describes precise conditions that force a divisibility sequence $(d_n(\alpha))$ to grow slower than exponentially. We note that [5] is itself an application of Schmidt's subspace theorem, so although the proof of the theorem is not long, it describes a deep property of divisibility sequences associated to algebraic integers.

THEOREM 5. *Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer and let $(d_n(\alpha))$ be the associated divisibility sequence,*

$$d_n(\alpha) = \max\{d \in \mathbb{Z} : \alpha^n \equiv 1 \pmod{d}\}.$$

Assume that one of the following two conditions is true:

(a) $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \geq 3$ *for all* $r \geq 1$.
(b) $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \geq 2$ *for all* $r \geq 1$ *and* $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \neq \pm 1$.

Then

$$\limsup_{n\to\infty} \frac{\log(d_n(\alpha))}{n} = 0.$$

In other words, $d_n(\alpha)$ grows slower than exponentially.

Proof. To ease notation, we write d_n for $d_n(\alpha)$. Let $K = \mathbb{Q}(\alpha)$, let $L/\mathbb{Q}$ be the Galois closure of K and let $\mathcal{O}_L$ be the ring of integers of L. By definition we have

$$\alpha^n - 1 \in d_n R,$$

so in particular $\alpha^n - 1 \in d_n\mathcal{O}_L$. Applying an automorphism $\sigma \in G_{L/\mathbb{Q}}$, we see that $(\alpha^\sigma)^n - 1 \in d_n\mathcal{O}_L$, since $d_n \in \mathbb{Z}$. Hence for every prime ideal $\mathfrak{p}$ of L we have

$$\min\bigl\{\mathrm{ord}_{\mathfrak{p}}(\alpha^n - 1), \mathrm{ord}_{\mathfrak{p}}(\alpha^{\sigma n} - 1)\bigr\} \geq \mathrm{ord}_{\mathfrak{p}}(d_n).$$

Multiplying by an appropriate multiple of $\log \mathrm{N}_{L/\mathbb{Q}}\,\mathfrak{p}$ and summing over primes yields

$$\log \gcd(\alpha^n - 1, \alpha^{\sigma n} - 1) \geq \log d_n, \tag{7}$$

where gcd is the generalized greatest common divisor used in [5, 8].

Suppose now that α and α^σ are multiplicatively independent in $\bar{\mathbb{Q}}^*$. Then [5, Proposition] tells us that for every $\epsilon > 0$ there is an $n_0 = n_0(\epsilon, \alpha, \alpha^\sigma)$ with the property that

$$\log \gcd(\alpha^n - 1, \alpha^{\sigma n} - 1) \le \epsilon n \qquad \text{for all } n \ge n_0. \tag{8}$$

Combining (7) and (8) yields the desired result.

So we are reduced to the case that for every $\sigma \in G_{L/\mathbb{Q}}$, the elements α and α^σ are multiplicatively dependent. Corollary 4 says that in this case, there is an integer r with the property $[\mathbb{Q}(\alpha^r) : \mathbb{Q}] \le 2$, which completes the proof of the theorem if α satisfies condition (a). If in addition $[\mathbb{Q}(\alpha^s) : \mathbb{Q}] \ne 1$ for all $s \ge 1$, then Corollary 4 says that α has norm ± 1, which proves the theorem when α satisfies condition (b). □

The theorem says that except in special cases, the sequence $d_n(\alpha)$ cannot grow too rapidly. One might ask if $d_n(\alpha)$ is frequently very small. We consider this question later in Section 6.

5. Real quadratic divisibility sequences

Theorem 5 says that $d_n(\alpha)$ grows slowly except in a few specified instances. In this section we analyze the cases that $d_n(\alpha)$ may grow rapidly. We assume throughout that α is not a root of unity.

The first case allowed by Theorem 5 is when there is an $r \ge 1$ such that $\alpha^r \in \mathbb{Z}$. By assumption, $|\alpha^r| \ge 2$, so we find that

$$d_{rn}(\alpha) = |\alpha^{rn} - 1| \ge |\alpha^r|^n - 1 \ge 2^n - 1.$$

Thus this "Kummer case" yields

$$\limsup_{n\to\infty} \frac{\log(d_n(\alpha))}{n} \ge \frac{\log 2}{r} > 0.$$

Further, if α^r is the smallest power of α that is in $\mathbb{Z}$, then it is easy to see that $d_n(\alpha) = 1$ if $r \nmid n$.

The more interesting case arises when α^r lies in a real quadratic extension of $\mathbb{Q}$ and has norm ± 1. The following elementary identities will be useful in analyzing this case.

Lemma 6. *For each $n \in \mathbb{N}$, let $A_n, B_n \in \mathbb{Q}[X, X^{-1}]$ be the Laurent polynomials*

$$A_n(X, X^{-1}) = \frac{X^n + X^{-n}}{2} \qquad \text{and} \qquad B_n(X, X^{-1}) = \frac{X^n - X^{-n}}{2}.$$

Then the following identities hold in $\mathbb{Q}[X, X^{-1}]$.

(a) $A_{2n} - 1 = 2B_n^2$
(b) $B_{2n} = 2A_nB_n$
(c) $(A_1 + 1)(A_{2n-1} - 1) = (B_n + B_{n-1})^2$
(d) $B_1B_{2n-1} = B_n^2 - B_{n-1}^2$

Proof. Substitute the definition of A_n and B_n into each of the stated identities and use elementary algebra to simplify. We illustrate with (c). First we compute

$$\begin{aligned} 2(B_n + B_{n-1}) &= X^n - X^{-n} + X^{n-1} - X^{-n+1} \\ &= X^{n-1}(X+1) - X^{-n}(1+X) \\ &= (X+1)(X^{n-1} - X^{-n}). \end{aligned}$$

Replacing X by X^{-1} introduces a minus sign into B_n and B_{n-1}, so

$$2(B_n + B_{n-1}) = -(X^{-1}+1)(X^{-n+1} - X^n).$$

Now multiplying these two expressions yields

$$\begin{aligned} 4(B_n + B_{n-1})^2 &= -(X+1)(X^{-1}+1)(X^{n-1} - X^{-n})(X^{-n+1} - X^n) \\ &= (X + X^{-1} + 2)(X^{2n-1} + X^{-2n+1} - 2) \\ &= 4(A_1 + 1)(A_{2n-1} - 1). \end{aligned}$$

The other parts are similar. □

The next two propositions give a complete description of $d_n(\alpha)$ for $\alpha = u + v\sqrt{D}$ with $u, v \in \mathbb{Z}$. The other cases of real quadratic irrationalities are handled similarly. The details are left to the reader.

THEOREM 7. *Let $D \geq 2$ be an integer that is not a perfect square, and let $\alpha = u + v\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ be the unit associated to a nontrivial positive solution (i.e., $u, v > 0$) of the Pell equation*

$$u^2 - v^2 D = 1.$$

Write

$$\alpha^n = \bigl(u + v\sqrt{D}\,\bigr)^n = u_n + v_n\sqrt{D},$$

so the divisibility sequence associated to α is given by

$$d_n(\alpha) = \gcd(u_n - 1, v_n).$$

Then

$$d_n(\alpha) = \begin{cases} 2v_{n/2} & \text{if } n \text{ is even,} \\ \gcd(u-1, v)\dfrac{v_{(n+1)/2} + v_{(n-1)/2}}{v} & \text{if } n \text{ is odd.} \end{cases}$$

The sequence $d_n(\alpha)$ satisfies the fourth order linear recursion

$$d_{n+4} = 2ud_{n+2} - d_n$$

whose characteristic polynomial is

$$T^4 - 2uT^2 + 1 = \bigl(T^2 - (u + v\sqrt{D}\,)\bigr)\bigl(T^2 - (u - v\sqrt{D}\,)\bigr).$$

The sequence grows exponentially,

$$\lim_{n\to\infty} \frac{\log d_n(\alpha)}{n} = \frac{1}{2}\log(\alpha) > 0. \tag{9}$$

Theorem 8. *Let $D, \alpha, u_n, v_n, d_n(\alpha)$ be as in the statement of Theorem 7 except now we assume that*

$$u^2 - v^2 D = -1.$$

Then

$$d_n(\alpha) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 2, \\ 2v_{n/2} & \text{if } n \equiv 0 \pmod 4, \\ \dfrac{v_{n/2+1} + v_{n/2-1}}{u} & \text{if } n \equiv 2 \pmod 4, \end{cases}$$

In particular, the even terms $d_{2n}(\alpha)$ satisfy a linear recurrence and grow exponentially, but the odd terms $d_{2n+1}(\alpha)$ form a constant sequence.

Proof of Theorem 7. Letting $\bar{\alpha} = u - v\sqrt{D}$, we have the usual formulas

$$u_n = \frac{\alpha^n + \bar{\alpha}^n}{2} \quad \text{and} \quad v_n = \frac{\alpha^n - \bar{\alpha}^n}{2\sqrt{D}}. \tag{10}$$

The sequences (u_n) and (v_n) satisfy the recurrence

$$x_{n+2} = 2ux_{n+1} - x_n$$

with initial values

$$u_0 = 1, \quad u_1 = u, \quad v_0 = 0, \quad v_1 = v.$$

We observe that $v|v_n$ for every $n \geq 0$, so if we define a reduced sequence by $\tilde{v}_n = v_n/v$, then $\tilde{v}_n$ is the linear recursion sequence defined by

$$\tilde{v}_0 = 0, \quad \tilde{v}_1 = 1, \quad \tilde{v}_{n+2} = 2u\tilde{v}_{n+1} - \tilde{v}_n. \tag{11}$$

By assumption, $\alpha\bar{\alpha} = 1$, so we have $\bar{\alpha} = \alpha^{-1}$ and the identities in Lemma 6(a,b) with $X = \alpha$ yield

$$u_{2n} - 1 = d_{2n} - 1 = 2B_n^2 = 2v_n^2 D, \tag{12}$$

$$v_{2n} = \frac{B_{2n}}{\sqrt{D}} = \frac{2A_n B_n}{\sqrt{D}} = 2u_n v_n, \tag{13}$$

Using these, it is easy to compute the even terms of the divisibility sequence,

$$d_{2n}(\alpha) = \gcd(2v_n^2 D, 2u_n v_n) = 2v_n \gcd(v_n D, u_n) = 2v_n.$$

For the last equality, we use the fact that $u_n^2 - Dv_n^2 = 1$ to conclude that u_n and $v_n D$ are relatively prime.

Similarly, the identities in Lemma 6(c,d) with $X = \alpha$ give

$$\begin{aligned} (u+1)(u_{2n-1} - 1) &= (A_1 + 1)(d_{2n-1} - 1) \\ &= (B_n + B_{n-1})^2 = (v_n + v_{n-1})^2 D, \end{aligned} \tag{14}$$

$$vv_{2n-1} = \frac{B_1 B_{2n-1}}{D} = \frac{B_n^2 - B_{n-1}^2}{D} = v_n^2 - v_{2n-1}^2. \tag{15}$$

These give us a somewhat complicated formula for the odd terms in the divisibility sequence,

$$d_{2n-1}(\alpha) = \gcd\left(\frac{(v_n + v_{n-1})^2 D}{u+1}, \frac{v_n^2 - v_{n-1}^2}{v}\right). \tag{16}$$

Using the reduced sequence $\tilde{v}_n = v_n/v$, we observe that

$$(v_n + v_{n-1})^2 D = (\tilde{v}_n + \tilde{v}_{n-1})^2 v^2 D = (\tilde{v}_n + \tilde{v}_{n-1})^2 (u^2 - 1),$$

so we can rewrite (16) as

$$\begin{aligned} d_{2n-1}(\alpha) &= \gcd\left(\frac{(\tilde{v}_n + \tilde{v}_{n-1})^2 (u^2-1)}{u+1}, \frac{(\tilde{v}_n^2 - \tilde{v}_{n-1}^2) v^2}{v} \right) \\ &= \gcd\big((\tilde{v}_n + \tilde{v}_{n-1})^2 (u-1), (\tilde{v}_n^2 - \tilde{v}_{n-1}^2) v \big) \\ &= (\tilde{v}_n + \tilde{v}_{n-1}) \gcd\left((\tilde{v}_n + \tilde{v}_{n-1})(u-1), (\tilde{v}_n - \tilde{v}_{n-1}) v \right). \end{aligned} \tag{17}$$

It remains to show the the gcd is equal to $\gcd(u-1, v)$.

A first observation is that adjacent terms of the sequence $(\tilde{v}_n)$ are relatively prime, i.e., $\gcd(\tilde{v}_n, \tilde{v}_{n-1}) = 1$, and further, they are alternately odd and even. This follows easily by induction from the initial values and recursive formula (11) satisfied by the sequence $(\tilde{v}_n)$. Hence

$$\gcd\left(\tilde{v}_n + \tilde{v}_{n-1}, \tilde{v}_n - \tilde{v}_{n-1}\right) = 1, \tag{18}$$

since the gcd certainly divides $\gcd(2\tilde{v}_n, 2\tilde{v}_{n-1}) = 2$, and it cannot equal 2 since $\tilde{v}_n + \tilde{v}_{n-1}$ is odd.

It is convenient to write out explicitly the closed sum for $\tilde{v}_n$:

$$\begin{aligned} \tilde{v}_n = \frac{v_n}{v} &= \frac{(u + v\sqrt{D})^n - (u - v\sqrt{D})^n}{2\sqrt{D}v} \\ &= \frac{1}{2\sqrt{D}v} \sum_{k=0}^{n} \binom{n}{k} u^{n-k} (v\sqrt{D})^k (1 - (-1)^k) \\ &= \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} u^{n-2k-1} v^{2k} D^k. \end{aligned}$$

In particular, there are rational integers $E_n \in \mathbb{Z}$ such that

$$\tilde{v}_n = n u^{n-1} + v^2 D E_n. \tag{19}$$

We first compute (using $v^2 D = u^2 - 1$)

$$\begin{aligned} \tilde{v}_n - \tilde{v}_{n-1} &= \big(n u^{n-1} + v^2 D E_n\big) - \big((n-1) u^{n-2} + v^2 D E_{n-1}\big) \\ &= n u^{n-2}(u-1) + u^{n-2} + (u^2-1)(E_n - E_{n-1}) \\ &\equiv 1 \pmod{u-1}. \end{aligned}$$

This proves that

$$\gcd(u-1, \tilde{v}_n - \tilde{v}_{n-1}) = 1. \tag{20}$$

If we could prove that $\gcd(\tilde{v}_n + \tilde{v}_{n-1}, v) = 1$, we would be done, but unfortunately it is easy to produce examples where this fails to be true. To obtain a weaker identity that suffices, we begin with the formula

$$\begin{aligned} \tilde{v}_n + \tilde{v}_{n-1} &= n u^{n-1} + (n-1) u^{n-2} + v^2 D (E_n + E_{n-1}) \\ &\equiv u^{n-2}\big(n(u+1) - 1\big) \pmod{v}. \end{aligned} \tag{21}$$

Multiplying by $u-1$ yields

$$\begin{aligned}
&(\tilde v_n+\tilde v_{n-1})(u-1)\\
&\qquad\equiv u^{n-2}\bigl(n(u^2-1)-(u-1)\bigr) \pmod{v} \quad \text{from (21)},\\
&\qquad\equiv u^{n-2}(nv^2D-(u-1)) \pmod{v} \quad \text{since } u^2-1=v^2D,\\
&\qquad\equiv -u^{n-2}(u-1) \pmod{v}.
\end{aligned}$$

Hence

$$\begin{aligned}
\gcd\left((\tilde v_n+\tilde v_{n-1})(u-1),v\right) &= \gcd\left(-u^{n-2}(u-1),v\right)\\
&= \gcd(u-1,v),
\end{aligned} \tag{22}$$

since u and v are relatively prime.

Combining the above gcd computations, we find that

$$\begin{aligned}
&\gcd\bigl((\tilde v_n+\tilde v_{n-1})(u-1),(\tilde v_n-\tilde v_{n-1})v\bigr)\\
&\qquad= \gcd\left((\tilde v_n+\tilde v_{n-1})(u-1),v\right) \quad \text{from (18) and (20)},\\
&\qquad= \gcd(u-1,v) \quad \text{from (22)}.
\end{aligned}$$

We are finally able to substitute this into (17) to obtain the formula

$$\begin{aligned}
d_{2n-1}(\alpha) &= (\tilde v_n+\tilde v_{n-1})\gcd\bigl((\tilde v_n+\tilde v_{n-1})(u-1),(\tilde v_n-\tilde v_{n-1})v\bigr)\\
&= (\tilde v_n+\tilde v_{n-1})\gcd(u-1,v)\\
&= \frac{(v_n+v_{n-1})\gcd(u-1,v)}{v},
\end{aligned}$$

which completes the proof of the stated formula for the odd terms in the divisibility sequence $d_n(\alpha)$.

In order to prove that $d_n(\alpha)$ satisfies a recurrence relation and to measure its exponential growth, we observe that we have proven that there are constants c_1 and c_2 (depending on u and v) so that

$$\begin{aligned}
d_{2n}(\alpha) &= c_1 v_n,\\
d_{2n-1}(\alpha) &= c_2(v_n+v_{n-1}).
\end{aligned} \tag{23}$$

The sequence v_n satisfies $v_{n+2}=2uv_{n+1}-v_n$, so (23) implies the two recursions

$$\begin{aligned}
d_{2n+4}(\alpha) &= 2ud_{2n+2}(\alpha)-d_n(\alpha)\\
d_{2n+3}(\alpha) &= 2ud_{2n+1}(\alpha)-d_{2n-1}(\alpha).
\end{aligned}$$

Thus the sequence $d_n(\alpha)$ satisfies the recursive formula $x_{n+4}=2ux_{n+2}-x_n$ whose characteristic polynomial is

$$T^4-2uT^2+1=(T^2-\alpha)(T^2-\bar\alpha),$$

since $\alpha+\bar\alpha=2u$ and $\alpha\bar\alpha=1$. Finally, since we have chosen α to satisfy $|\alpha|>1$, the limit formula (9) follows from (23) and the fact that

$$\lim_{n\to\infty}\frac{\log v_n}{n}=\lim_{n\to\infty}\frac{\log\left(\dfrac{\alpha^n-\alpha^{-n}}{2\sqrt{D}}\right)}{n}=\log(\alpha).$$

This completes the proof of Theorem 7. □

Proof of Theorem 8. Clearly we have $d_{2n}(\alpha) = d_n(\alpha^2)$ directly from the definition. Let $\beta = \alpha^2$. Then $\beta\bar{\beta} = (\alpha\bar{\alpha})^2 = (-1)^2 = 1$, so the divisibility sequence $d_n(\beta)$ is of exactly the type described in Theorem 8. In order to obtain an explicit formula for $d_n(\beta) = d_{2n}(\alpha)$, we observe that

$$\begin{aligned} v_{n/2}(\beta) &= v_n(\alpha) \quad \text{for even } n, \\ v_{(n\pm1)/2}(\beta) &= v_{n\pm1}(\alpha) \quad \text{for odd } n, \\ u(\beta) - 1 &= u_2(\alpha) - 1 = u^2 + v^2 D - 1 = 2v^2 D, \\ v(\beta) &= v_2(\alpha) = 2uv, \\ \gcd\bigl(u(\beta) - 1, v(\beta)\bigr) &= \gcd(2v^2 D, 2uv) = 2v. \end{aligned}$$

(Note that here u and v are given by $\alpha = u + v\sqrt{D}$.) We substitute these values into the formula for $a_n(\beta)$ provided by Theorem 8. Thus if n is even we find that

$$d_{2n}(\alpha) = d_n(\beta) = 2v_{n/2}(\beta) = 2v_n(\alpha),$$

and if n is odd we obtain

$$\begin{aligned} d_{2n}(\alpha) = d_n(\beta) &= \frac{\gcd(u(\beta) - 1, v(\beta))(v_{(n+1)/2}(\beta) + v_{(n-1)/2}(\beta))}{v(\beta)} \\ &= \frac{2v(v_{n+1}(\alpha) + v_{n-1}(\alpha))}{2uv} \\ &= \frac{(v_{n+1}(\alpha) + v_{n-1}(\alpha))}{u} \end{aligned}$$

This completes the proof of the formula for the even terms in the sequence $d_n(\alpha)$. It remains to show that $d_n(\alpha) = 1$ when n is odd.

We assume henceforth that n is odd. Then $u_n^2 - v_n^2 D = -1$, which we rewrite as

$$(u_n + 1)(u_n - 1) - v_n^2 D = -2. \tag{24}$$

This equation shows that $\gcd(u_n - 1, v_n)$ divides 2. However, it cannot equal 2, since otherwise the lefthand side of (24) would be divisible by 4. This completes the proof that $d_n(\alpha) = \gcd(u_n - 1, v_n) = 1$ when n is odd. □

6. Small entries in divisibility sequences

Theorem 5 tells us that except in a few specified cases, the sequence $d_n(\alpha)$ grows slower than exponentially, and although the values do occasionally get quite large, we find experimentally that $d_n(\alpha)$ is also often quite small. This leads us to make the following conjecture, which is the analog of a conjecture of Ailon and Rudnick [1] regarding $\gcd(a^n - 1, b^n - 1)$ for multiplicatively independent integers a and b.

$n \le$	$d_n = 1$	$d_n = 2$	$d_n = 3$	$d_n = 4$	$d_n = 5$	$d_n = 6$
1000	67.30 %	6.30 %	3.90 %	2.80 %	1.10 %	0.30 %
5000	66.32 %	6.10 %	3.72 %	2.50 %	0.78 %	0.32 %
10000	65.91 %	6.03 %	3.66 %	2.47 %	0.77 %	0.33 %
15000	65.82 %	5.99 %	3.60 %	2.42 %	0.78 %	0.33 %
20000	65.59 %	5.98 %	3.60 %	2.40 %	0.76 %	0.32 %

Table 2. Frequency of $\{n : d_n(\alpha) = k\}$ for $\alpha^3 - \alpha - 1 = 0$

Conjecture 9. *Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer and let $(d_n(\alpha))$ be the associated divisibility sequence* (2). *Assume that α satisfies one of the conditions* (a) *or* (b) *in Theorem 5. Then*

$$\bigl\{n \ge 1 : d_n(\alpha) = d_1(\alpha)\bigr\}$$

is infinite.

Example 6. It is worthwhile looking at a nontrivial example numerically. Let α be root of $T^3 - T - 1$. We find that the associated sequence starts

$$\begin{aligned}(d_n) = {} & 1,1,1,1,1,1,2,1,1,1,1,1,3,4,1,1,1,1,1,1,2,1,1,5,1,3,1,8,\\ & 1,1,1,1,1,1,2,1,1,1,9,1,1,4,1,1,1,1,1,35,2,1,1,3,1,\\ & 1,1,16,1,59,1,1,1,1,1,2,1,3,1,1,1,1,4,1,5,1,1,1,1,2,9,1,\\ & 1,1,1,1,8,1,1,1,1,1,1,6,1,1,1,1,35,1,4,1,101,\dots\end{aligned}$$

The data appears to support Conjecture 9 that $d_n = 1$ for infinitely many values of n. From this small amount of data it is less clear how often we should expect to have, say, $d_n = 2$ or $d_n = 3$. Table 2 gives the frequency of $d_n = k$ for each $k = 1, 2, \dots, 6$ and $n \le N$ for various values of N. The table suggests that the set $\{n \in \mathbb{N} : d_n = k\}$ is infinite, and indeed possibly that it has a positive density.

However, it is easily seen that there are some values of k for which the set is empty. For example, we claim that $d_n(\alpha) \ne 7$ for all n. The reason is that the smallest power of α satsifying $\alpha^n \equiv 1 \pmod 7$ is α^{48} and

$$\alpha^{48} - 1 = 128800 + 226030\alpha + 170625\alpha^2 = 35(3680 + 6458\alpha + 4875\alpha^2).$$

Thus

$$7|d_n \Longrightarrow 48|n \Longrightarrow 35|d_n,$$

so d_n will never equal 7. It would be interesting to characterize the set $\{k \in \mathbb{N} : d_n(\alpha) \ne k \text{ for all } n\}$.

Based on this and various other examples, it is tempting to make a conjecture of the following sort, although given the scanty evidence, it seems safer to phrase it as a question.

Question 1. Let $\alpha \in \bar{\mathbb{Z}}$ be a nonzero algebraic integer and let $(d_n(\alpha))$ be the associated divisibility sequence (2) as usual. For each $k \in \mathbb{N}$, let

$$S_\alpha(k) = \bigl\{n \in \mathbb{N} : d_n(\alpha) = k\bigr\}.$$

Is it true that either $S_\alpha(k) = \emptyset$ or else $S_\alpha(k)$ has positive (lower) density in $\mathbb{N}$.

If Question 1 has an affirmative answer, it then becomes a very interesting question to describe the density of $S_\alpha(k)$ in terms of arithmetic properties of α, even for the initial nontrivial case $S_\alpha(d_1(\alpha))$.

Remark 2. The divisibility sequences $d_n(\alpha)$ studied in this paper can be defined in far more generality, for example using an element α in a ring of the form $R = \mathbb{Z}[T]/(F(T))$ for a monic polynomial $F(T) \in \mathbb{Z}[T]$. Thus $d_n(\alpha)$ is the largest rational integer d such that $\alpha^n - 1$ is divisible by d in the ring R.

As a particular example, consider the ring $R = \mathbb{Z}[T]/(T^2 - T)$ and element $\alpha = T + 2$. The natural isomorphism

$$R \cong \mathbb{Z}[T]/(T) \times \mathbb{Z}[T]/(T-1)$$

identifies $\alpha \leftrightarrow (2,3)$, so $d_n(\alpha) = \gcd(2^n - 1, 3^n - 1)$. Ailon and Rudnick [1] conjecture in this case that $d_n(\alpha) = 1$ for infinitely many n, and more generally they conjecture that if $a, b \in \mathbb{Z}$ are multiplicatively independent, then

$$\gcd(a^n - 1, b^n - 1) = \gcd(a-1, b-1) \quad \text{for infinitely many } n \geq 1. \tag{25}$$

Thus Conjecture 9 may be viewed as a generalization of Ailon and Rudnick's conjecture, and Question 1 suggests a strengthened statement. Ailon and Rudnick prove a strong version of (25) with $\mathbb{Z}$ replaced by the polynomial ring $\mathbb{C}[T]$. See also [6] and [7] for analogs over $\mathbb{F}_q[T]$ and for elliptic curves and [8, Section 7] for a more general conjecture on the infinitude, although not the density, of values of divisibility sequences associated to commutative group schemes.

References

[1] N. Ailon, Z. Rudnick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$, *Acta Arithmetica* 113 (2004), 31–38.

[2] J.P. Bézivin, A. Pethö, A.J. van der Poorten, A full characterisation of divisibility sequences, *Amer. J. of Math.* 112 (1990), 985–1001.

[3] Y. Bugeaud, P. Corvaja, U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Math. Zeit.* 243 (2003), no. 1, 79–84.

[4] P. Corvaja, U. Zannier, On the greatest prime factor of $(ab+1)(ac+1)$, *Proc. Amer. Math. Soc.* 131 (2002), 1705–1709.

[5] ——— A lower bound for the height of a rational function at S-unit points, *Monatshefte Math.*, 144 (2005), 203–224.

[6] J.H. Silverman, Common divisors of $a^n - 1$ and $b^n - 1$ over function fields, *New York Journal of Math.* (electronic) 10 (2004), 37–43.

[7] ——— Common divisors of elliptic divisibility sequences over function fields, *Manuscripta Math.*, 114 (2004), 432–446.

[8] ——— Generalized greatest common divisors, Divisibility sequences, and Vojta's conjecture for blowups *Monatsch. Math.*, 145 (2005), 333–350.

[9] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* 70 (1948), 31–74.

Joseph H. Silverman
Mathematics Department
Box 1917
Brown University
Providence
RI 02912 USA
jhs@math.brown.edu