ACTA ARITHMETICA
146.4 (2011)

Terms in elliptic divisibility sequences divisible by their indices

by

Joseph H. Silverman (Providence, RI) and
Katherine E. Stange (Burnaby and Vancouver)

Introduction. In this note we investigate the terms in elliptic divisibility sequences that are divisible by their indices. The analogous problem has been studied for a number of other types of sequences. For example, the Fibonacci sequence $(F_n)_{n\ge 1}$ satisfies

$$n \mid F_n \;\Leftrightarrow\; n \in \{1, 5, 12, 24, 25, 36, 48, 60, 72, 96, \ldots\}.$$

See [1, 9, 10, 19, 20, 21, 24] for results on index divisibility in the Fibonacci sequence and in more general Lucas sequences. To cite another example, composite values of n that divide $a^n - a$ are called *pseudoprimes to the base a*. They have been studied for their intrinsic interest and for applications to cryptography [2, 11, 12, 14, 23].

In general, for any integer sequence $\mathsf{A} = (A_n)_{n\ge 1}$ we define the *index divisibility set* of A to be

$$\mathcal{S}(\mathsf{A}) = \{n \ge 1 : n \mid A_n\}.$$

Our goal is to build $\mathcal{S}(\mathsf{A})$ multiplicatively via a directed graph that connects each element $n \in \mathcal{S}(\mathsf{A})$ to its (minimal) multiples in $\mathcal{S}(\mathsf{A})$. Thus we define a directed graph by taking the set $\mathcal{S}(\mathsf{A})$ to be the set of vertices and by drawing an arrow from n to m if the following two conditions are true:

(1) $n \mid m$ with $n < m$.
(2) If $k \in \mathcal{S}(\mathsf{A})$ satisfies $n \mid k \mid m$, then $k = n$ or $k = m$.

In other words, if we partially order $\mathcal{S}(\mathsf{A})$ by divisibility, then we draw an arrow from n to m if n is strictly smaller than m and if there are no elements of $\mathcal{S}(\mathsf{A})$ that are strictly between n and m.

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11B37, 14G25, 14H25.
Key words and phrases: elliptic divisibility sequence, elliptic curve, aliquot cycle.

DOI: 10.4064/aa146-4-4

We denote the set of arrows by $\mathrm{Arr}(\mathsf{A})$, and we say that the arrow $(n \to m)$ has *weight* m/n. (Smyth [19, Section 8] defines a similar structure, but he allows only arrows of prime weight, so his graphs may be disconnected.)

Definition 1. Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation and let $P \in E(\mathbb{Q})$ be a nontorsion point. The *elliptic divisibility sequence* (EDS) associated to the pair (E, P) is the sequence of positive integers $\mathsf{D} = (D_n)_{n\geq 1}$ obtained by writing

$$x([n]P) = \frac{A_n}{D_n^2} \in \mathbb{Q}$$

as a fraction in lowest terms. The EDS is *minimal* if E is given by a minimal Weierstrass equation. An EDS is *normalized* if $D_1 = 1$.

An arbitrary EDS $(D_n)_{n\geq 1}$ can be normalized by a change of variables in the defining Weierstrass equation, in which case the new EDS is $(D_n/D_1)_{n\geq 1}$. Note, however, that the normalized sequence may not be minimal.

We remark that there is an alternative definition of EDS via a nonlinear recurrence that gives almost the same set of sequences; see Remark 6.2 for further details. We also note that, as its name suggests, an EDS is a divisibility sequence, i.e.,

$$m \mid n \;\Rightarrow\; D_m \mid D_n.$$

The arithmetic properties of EDS have been extensively studied as examples of nontrivial nonlinear recursions that possess enough additional structure to make them amenable to Diophantine analysis. See for example Ward's original papers [25, 26], subsequent work including [5, 7, 8, 18], and applications of EDS to Hilbert's 10th problem and to cryptography [3, 6, 13, 22].

Although EDS are defined via a nonlinear process, their underlying structure comes from the associated elliptic curve. They are thus a natural generalization of linear recursions such as the Fibonacci and Lucas sequences, which are associated to the multiplicative group.

Example 0.1. Let D be the EDS

$$\mathsf{D} = (1, 1, 1, 1, 2, 1, 3, 5, 7, 4, 23, 29, 59, 129, \\ 314, 65, 1529, 3689, 8209, 16264, 83313, \dots)$$

associated to the elliptic curve and point

$$E : y^2 + y = x^3 - x, \qquad P = (0, 0).$$

Then

$$\mathcal{S}(\mathsf{D}) = \{1, 40, 53, 63, 80, 127, 160, 189, 200, 320, 400, 441, 443, \dots\}.$$

We remark that the sequence D grows very rapidly. Thus the first two nontrivial elements of $\mathcal{S}(\mathsf{D})$ in this example come from

$$\begin{aligned} D_{40} &= 40 \cdot 13\,526\,278\,251\,270\,010, \\ D_{53} &= 53 \cdot 299\,741\,133\,691\,576\,877\,400\,370\,757\,471. \end{aligned}$$

The reader may have noticed that $\mathcal{S}(\mathsf{D})$ contains the primes 53, 127, and 443, which are the first three anomalous primes for E, i.e., primes satisfying $\#E(\mathbb{F}_p) = p$. This is not a coincidence.

Smyth has given an explicit description of index divisibility for Lucas sequences. For comparison with our results, we state one of his theorems, reformulated using the terminology of directed graphs.

Theorem 0.2 (Smyth [19, Theorem 1]). *Let $a, b \in \mathbb{Z}$, and let $\mathsf{L} = (L_n)_{n\ge 1}$ be the associated Lucas sequence of the first kind, i.e., defined by the recursion*

$$L_{n+2} = aL_{n+1} - bL_n, \quad L_0 = 0, \quad L_1 = 1.$$

Let $\Delta = a^2 - 4b$ and let $n \in \mathcal{S}(\mathsf{L})$ be a vertex. Then the arrows originating at n are

$$\{n \to np : p \textit{ is prime and } p \mid L_n\Delta\} \cup \mathcal{B}_{a,b,n},$$

where

$$\mathcal{B}_{a,b,n} = \begin{cases} \{n \to 6n\} & \textit{if } (a,b) \equiv (3, \pm 1) \pmod 6 \textit{ and } \gcd(6, L_n) = 1, \\ \{n \to 12n\} & \textit{if } (a,b) \equiv (\pm 1, 1) \pmod 6 \textit{ and } \gcd(6, L_n) = 1, \\ \emptyset & \textit{otherwise.} \end{cases}$$

Smyth's theorem says in particular that at any vertex, there is at most one outgoing arrow whose weight is not prime. By way of contrast, it turns out that an EDS vertex may have infinitely many composite-weight outgoing arrows. These composite-weight arrows are associated to so-called composite aliquot numbers. A Lucas sequence has at most one composite aliquot number, while EDS (probably) have infinitely many. This dichotomy can be traced to the fact that the number $\#E(\mathbb{F}_q)$ of points on an elliptic curve over a finite field varies irregularly and is often prime, while the number of points in the multiplicative group $\mathbb{F}_q^*$ of a finite field is $q-1$.

Definition 2. Let D be an EDS associated to the elliptic curve E. A list $p_1, \ldots, p_\ell$ of distinct primes of good reduction for E is an *aliquot cycle* for D if

$$p_{i+1} = \min\{r \ge 1 : p_i \mid D_r\} \quad \text{for all } 1 \le i \le \ell,$$

where we require $p_{\ell+1} = p_1$ to complete the cycle. The associated *aliquot number* is the product $p_1 \cdots p_\ell$. Note that $\ell = 1$ is allowed in this definition, but that it is composite aliquot numbers ($\ell \ge 2$) that lead to composite-weight arrows.

The index divisibility graph of an EDS is considerably more complicated than that of a Lucas sequence. We state here a simplified version of Theorem 3.3, which is the main result of this paper. We remark that an analogue of our main result for EDS associated to singular elliptic curves would give a version of Smyth's theorem; see Remark 4.7 for details.

Theorem 0.3. *Let* D *be a minimal regular EDS associated to the elliptic curve* $E/\mathbb{Q}$ *and point* $P \in E(\mathbb{Q})$. (*See Section* 3 *for the definition of regularity. In particular, every EDS has a regular subsequence.*)

(a) *If* $n \in \mathcal{S}(\mathsf{D})$ *and* p *is prime and* $p \mid D_n$, *then* $(n \to np) \in \mathrm{Arr}(\mathsf{D})$.
(b) *If* $n \in \mathcal{S}(\mathsf{D})$ *and* d *is an aliquot number for* D *and* $\gcd(n,d) = 1$, *then* $(n \to nd) \in \mathrm{Arr}(\mathsf{D})$.
(c) *If* $p \geq 7$ *is a prime of good reduction for* E *and if* $(n \to np) \in \mathrm{Arr}(\mathsf{D})$, *then either* $p \mid D_n$ *or* p *is an aliquot number for* D.
(d) *If* $\gcd(n,d) = 1$ *and if* $(n \to nd) \in \mathrm{Arr}(\mathsf{D})$ *and if* $d = p_1 \cdots p_\ell$ *is a product of* $\ell \geq 2$ *distinct primes of good reduction for* E *satisfying* $\min p_i > (2^{-1/2\ell} - 1)^{-2}$, *then* d *is an aliquot number for* D.

We briefly describe the contents of this note. In Section 1 we give some basic properties of elliptic divisibility sequences. In particular, Lemma 1.2 states fairly delicate divisibility estimates whose origins lie in the formal group of E. The brief Section 2 gives the definition of aliquot cycles and aliquot numbers for EDS. Section 3 contains the statement and proof of Theorem 3.3, which is the main result of this paper. Theorem 3.3, which is an expanded version of Theorem 0.3, explains how to construct the arrows that are used to build $\mathcal{S}(\mathsf{D})$. This is followed in Section 4 with a number of remarks and examples related to our main theorem. Section 5 defines aliquot cycles on an elliptic curve (see [17]) and explains how they are related to aliquot cycles for an EDS on that curve. Finally, in Section 6, we make some miscellaneous remarks on general index divisibility sets and on an alternative definition of EDS.

1. Preliminaries on elliptic divisibility sequences.

Let D be a minimal EDS associated to an elliptic curve $E/\mathbb{Q}$ and point $P \in E(\mathbb{Q})$. We let $\mathrm{Disc}(E)$ denote the minimal discriminant of E. For all primes p we have

$$p \mid D_n \;\Leftrightarrow\; [n]P \equiv O \pmod{p}.$$

Definition 3. We write $r_n = r_n(\mathsf{D})$ for the *rank of apparition* of n in D, which is defined by

$$r_n = \min\{r \geq 1 : n \mid D_r\}.$$

Let $\mathfrak{E}/\operatorname{Spec}\mathbb{Z}$ denote the Néron model of E. Then an equivalent definition of r_n is that it is the smallest value of $r \geq 1$ such that

$$[r]P \equiv O \pmod{n},$$

where the congruence takes place in $\mathfrak{E}(\mathbb{Z}/n\mathbb{Z})$.

The following three lemmas contain virtually all of the information about EDS that we will use in our analysis of EDS index divisibility.

LEMMA 1.1. *Let D be a minimal EDS associated to an elliptic curve $E/\mathbb{Q}$ and point $P \in E(\mathbb{Q})$. Then*

$$n \mid D_m \iff r_n \mid m \iff [m]P \equiv O \pmod{n}.$$

Proof. Immediate from the definitions. ■

The next lemma describes the growth of p-divisibility for EDS. A direct corollary is that an EDS is a divisibility sequence.

LEMMA 1.2. *Let $\mathsf{D} = (D_n)_{n \geq 1}$ be a minimal EDS, let $n \geq 1$, and let p be a prime satisfying $p \mid D_n$.*

(a) *For all $m \geq 1$ we have*

$$\operatorname{ord}_p(D_{mn}) \geq \operatorname{ord}_p(mD_n).$$

(b) *The inequality in* (a) *is strict,*

$$\operatorname{ord}_p(D_{mn}) > \operatorname{ord}_p(mD_n),$$

if and only if

$$p = 2 \text{ and } 2 \mid m \text{ and } \operatorname{ord}_2(D_n) = 1 \text{ and } \left(\begin{array}{l} E \text{ has ordinary or multi-} \\ \text{plicative reduction at } 2 \end{array}\right).$$

(*For the definition of ordinary reduction, see* [16, §V.3]. *In particular, E has ordinary reduction at* 2 *if and only if* $2 \mid \#E(\mathbb{F}_2)$.)

Proof. The assumption that $p \mid D_n$ is equivalent to the assertion that $[n]P$ is in $E_1(\mathbb{Q}_p)$, the kernel of reduction modulo p. We use the standard isomorphism between $E_1(\mathbb{Q}_p)$ and the formal group $\hat{E}(p\mathbb{Z}_p)$ associated to E given by

$$\phi : E_1(\mathbb{Q}_p) \to \hat{E}(p\mathbb{Z}_p), \qquad (x, y) \mapsto -x/y.$$

Note that this isomorphism is valid even if E has bad reduction at p, in which case $\hat{E}$ is the formal additive or multiplicative group. (See [16, Chapter IV] for basic properties of formal groups.)

Writing $x([n]P) = (A_n/D_n^2, B_n/D_n^3)$, our assumption that $p \mid D_n$ implies that $p \nmid A_nB_n$, so

$$\operatorname{ord}_p \phi([n]P) = \operatorname{ord}_p(-A_nD_n/B_n) = \operatorname{ord}_p(D_n). \tag{1.1}$$

Standard properties of formal groups [16, IV.2.3(a), IV.4.4] say that the multiplication-by-p map has the form

$$[p]_{\hat{E}}(z) = pf(z) + g(z^p), \tag{1.2}$$

where $f, g \in \mathbb{Z}_p[[z]]$ are power series with no constant term, and f has the form $f(z) = z + O(z^2)$. It follows that for $\operatorname{ord}_p(z) \geq 1$, we have

$$\operatorname{ord}_p([p]_{\hat{E}}(z)) \geq \operatorname{ord}_p(pz). \tag{1.3}$$

We write $m = p^k s$ with $p \nmid s$. Repeated application of (1.3) gives

$$\operatorname{ord}_p([p^k]_{\hat{E}}(z)) \geq \operatorname{ord}_p(p^k z). \tag{1.4}$$

Further, we have $[s]_{\hat{E}}(z) = sz + O(z^2)$, so

$$\operatorname{ord}_p([sp^k]_{\hat{E}}(z)) = \operatorname{ord}_p([p^k]_{\hat{E}} z). \tag{1.5}$$

Combining (1.4) and (1.5) gives

$$\operatorname{ord}_p([m]_{\hat{E}}(z)) \geq \operatorname{ord}_p(p^k z),$$

with equality if $k = 0$. Substituting $z = \phi([n]P)$ and using (1.1) gives (a), and it also gives (b) if $p \nmid m$.

To prove (b) in general, we assume that $p \mid m$. Analyzing (1.2) more closely, we see that

$$\operatorname{ord}_p([p]_{\hat{E}}(z)) = \operatorname{ord}_p(pz) = \operatorname{ord}_p(z) + 1 \tag{1.6}$$

unless $\operatorname{ord}_p(pz) = p \operatorname{ord}_p(z)$. (Note that $\operatorname{ord}_p(z) \geq 1$.) Since

$$\operatorname{ord}_p(pz) = p \operatorname{ord}_p(z) \iff 1 = (p-1)\operatorname{ord}_p(z),$$

we see that (1.6) holds except possibly in the case $p = 2$ and $\operatorname{ord}_p(z) = 1$.

Suppose now that $p = 2$ and $\operatorname{ord}_p(z) = 1$. The formal group law for an elliptic curve starts [16, §IV.1]

$$[2]_{\hat{E}}(z) = 2z - a_1 z^2 - 2a_2 z^3 + (a_3 + a_1 a_2) z^4 + \cdots,$$

where $a_1, \ldots, a_6$ are Weierstrass coefficients. Hence under the assumption that $\operatorname{ord}_2(z) = 1$, we see that (1.6) fails if and only if

$$\begin{aligned} \operatorname{ord}_2(2z - a_1 z^2 + O(2z^3)) \geq 3 &\iff \operatorname{ord}_2(1 - a_1 z/2) \geq 1 \\ &\iff \operatorname{ord}_2(a_1) = 0, \quad \text{i.e., } a_1 \in \mathbb{Z}_2^*. \end{aligned}$$

(The last equivalence follows because $z \equiv 2 \pmod{4}$, so $1 - a_1 z/2 \equiv 1 - a_1 \pmod{2}$.) If E has good reduction modulo 2, then

$$j(E) \equiv a_1^{12}/\operatorname{Disc}(E) \pmod{2},$$

so [16, Exer. 5.7] gives

$$\operatorname{ord}_2(a_1) = 0 \iff j(E) \not\equiv 0 \pmod{2} \iff E \text{ is ordinary mod } 2.$$

On the other hand, if E has bad reduction at 2, then an easy computation shows that $a_1 \equiv 1 \pmod{2}$ for multiplicative reduction and $a_1 \equiv 0 \pmod{2}$

for additive reduction. This completes the proof that (1.6) fails if and only if $p = 2$ and $p \mid m$ and $\operatorname{ord}_p(D_n) = 1$ and E has either ordinary or multiplicative reduction. We call this the exceptional case.

Repeated application of (1.6) shows that if we are not in the exceptional case, then

$$\operatorname{ord}_p([p^k]_{\hat{E}}(z)) = \operatorname{ord}_p(z) + k.$$

In the exceptional case, the first multiplication by $[p]$ gives a strict inequality, after which we are out of the exceptional case and can apply (1.6), so we find that

$$\operatorname{ord}_p([p^k]_{\hat{E}}(z)) = \operatorname{ord}_p([p]_{\hat{E}}(z)) + k - 1 > \operatorname{ord}_p(z) + k.$$

Now using (1.5) and the fact that $m = p^k s$ with $p \nmid s$, we get

$$\operatorname{ord}_p([m]_{\hat{E}}(z)) > \operatorname{ord}_p(mz)$$

in the exceptional case and

$$\operatorname{ord}_p([m]_{\hat{E}}(z)) = \operatorname{ord}_p(mz)$$

otherwise. Substituting $z = \phi([n]P)$ and using (1.1) proves (b). ∎

The third lemma gives bounds for r_p.

Lemma 1.3. *Let* D *be a minimal EDS associated to an elliptic curve* $E/\mathbb{Q}$ *and point* $P \in E(\mathbb{Q})$ *and let* p *be a prime. Then*

$$r_n \mid \#\mathfrak{E}(\mathbb{Z}/n\mathbb{Z}).$$

In particular, if p *is a prime with* $P \in E_{\mathrm{ns}}(\mathbb{F}_p)$, *then*

$$r_p \le (\sqrt{p} + 1)^2.$$

If $P \in E_{\mathrm{ns}}(\mathbb{F}_p)$ *and* E *has bad reduction at* p, *then* r_p *divides* $p - 1$, $p + 1$, *or* p *depending respectively on whether the reduction is split multiplicative, nonsplit multiplicative, or additive.*

Proof. The first statement is immediate, since r_n is the order of the point P in the group $\mathfrak{E}(\mathbb{Z}/n\mathbb{Z})$. The estimates for r_p follow from the Hasse–Weil bound $\#E(\mathbb{F}_p) \le (\sqrt{p} + 1)^2$ when E has good reduction, and the explicit description of $E_{\mathrm{ns}}(\mathbb{F}_p)$ for the three types of bad reduction. ∎

Example 1.4. The minimal EDS associated to

$$E : y^2 + xy = x^3 - 2x + 1 \quad \text{and} \quad P = (1, 0)$$

is the sequence

$$1, 1, 1, 2, 1, 3, 7, 8, 25, 37, \ldots.$$

Thus $D_4 = 2$ and $D_8 = 8$, so

$$3 = \operatorname{ord}_2(D_{2^3}) > \operatorname{ord}_2(2D_{2^2}) = 2.$$

The strictness of the inequality in Lemma 1.2(a) corresponds to the exceptional case $p = 2$, $m = 2$, and $n = 4$, where we note that $\operatorname{ord}_2(D_4) = 1$ and $\#E(\mathbb{F}_2) = 4$, so in particular E has ordinary reduction at 2.

Remark 1.5. More generally, for any integer $N \geq 2$ there exists a minimal EDS such that

$$\operatorname{ord}_2(D_2) = \operatorname{ord}_2(D_1) + N.$$

Here is one construction. Choose an elliptic curve of positive rank having a rational 2-torsion point T in the formal group $\hat{E}(2\mathbb{Z}_2)$. Taking a multiple of a point of infinite order, we can find a rational nontorsion point Q in $\hat{E}(2^N\mathbb{Z}_2)$. Then the EDS associated to $P = Q + T$ will have $\operatorname{ord}_2(D_1) = 1$ and $\operatorname{ord}_2(D_2) = N + 1$. The reason that this only works for the prime $p = 2$ is because for $p \geq 3$, the formal group $\hat{E}(\mathbb{Z}_p)$ is torsion free; in fact, it is isomorphic to the additive group $\mathbb{Z}_p^+$.

Proposition 1.6. *Let* D *be a minimal EDS.*

(a) D *is a divisibility sequence.*
(b) *The set* $\mathcal{S}(\mathsf{D})$ *is closed under multiplication.*

Proof. (a) We need to prove that $D_m \mid D_{mn}$. It suffices to prove that

$$\operatorname{ord}_p(D_{mn}) \geq \operatorname{ord}_p(D_n) \quad \text{for all primes } p,$$

but this is immediate from Lemma 1.2(a).

(b) Suppose that $m, n \in \mathcal{S}(\mathsf{D})$ and let $p \mid n$. Then $p \mid D_n$, so Lemma 1.2(a) and the assumption that $n \mid D_n$ give

$$\operatorname{ord}_p(D_{mn}) \geq \operatorname{ord}_p(mD_n) \geq \operatorname{ord}_p(mn).$$

Reversing the roles of m and n for $p \mid m$ again gives $\operatorname{ord}_p(D_{mn}) \geq \operatorname{ord}_p(mn)$. Hence $mn \mid D_{mn}$, so $mn \in \mathcal{S}(\mathsf{D})$. ∎

Remark 1.7. If $p \geq 3$ and $p \mid D_1$, then Lemma 1.2(b) with $n = 1$ says that $\operatorname{ord}_p(D_m) = \operatorname{ord}_p(mD_1)$ for all m.

Remark 1.8. Although we will not need this fact, we mention that elliptic divisibility sequences grow extremely rapidly. Thus if D is associated to (E, P), then

$$\lim_{n\to\infty} \frac{\log |D_n|}{n^2} = \hat{h}_E(P),$$

where $\hat{h}_E(P) > 0$ is the canonical height of P [16, §VIII.9].

2. Aliquot cycles and aliquot numbers for EDS. In this section we define aliquot cycles and aliquot numbers associated to an EDS.

Definition 4. Let D be an EDS associated to the curve $E(\mathbb{Q})$ and point $P \in E(\mathbb{Q})$. We recall that $r_n(\mathsf{D})$ denotes the rank of apparition of n in the sequence D; see Section 1. An *aliquot cycle* (*of length* ℓ) for D is a sequence $(p_1,\dots,p_\ell)$ of distinct primes of good reduction for E such that

$$r_{p_1}(\mathsf{D}) = p_2,\quad r_{p_2}(\mathsf{D}) = p_3,\ \dots,\ r_{p_{\ell-1}}(\mathsf{D}) = p_\ell,\quad r_{p_\ell}(\mathsf{D}) = p_1.$$

An *amicable pair* is an aliquot cycle of length two.

If we drop the requirement that E have good reduction, then we call $(p_1,\dots,p_\ell)$ a *generalized aliquot cycle.*

In our study of index divisibility for EDS, the products of the primes appearing in each aliquot cycle play a key role, so we give them a name.

Definition 5. Let D be a minimal EDS. We define the set of *aliquot numbers* of D to be

$$\mathcal{A}(\mathsf{D}) = \{p_1\cdots p_\ell : (p_1,\dots,p_\ell) \text{ is an aliquot cycle for } \mathsf{D}\}.$$

We also define the larger set

$$\mathcal{A}_{\mathrm{gen}}(\mathsf{D}) = \{p_1\cdots p_\ell : (p_1,\dots,p_\ell) \text{ is a generalized aliquot cycle for } \mathsf{D}\}.$$

Remark 2.1. We observe that an aliquot cycle of length one consists of a single prime p satisfying $r_p(\mathsf{D}) = p$. If $p \ge 7$, Hasse's estimate for $\#E(\mathbb{F}_p)$ tells us that

$$r_p(\mathsf{D}) = p \iff \#E(\mathbb{F}_p) = p.$$

Thus in standard terminology, the primes $p \ge 7$ in $\mathcal{A}(\mathsf{D})$ are exactly the *anomalous primes* for the elliptic curve E.

3. Arrows in the index divisibility graph.

This section contains our main results. In Theorem 3.3 we classify the arrows $(n \to nd) \in \mathrm{Arr}(\mathsf{D})$ for a large class of EDS, as described in the following definition.

Definition 6. Let D be a minimal EDS associated to the elliptic curve and point (E,P). We say that D is 2-*irregular* if the following five irregularity conditions are true:

(I$_1$) E has good reduction at 2, (I$_2$) $\#E(\mathbb{F}_2) = 4$, (I$_3$) $r_2 = 4$,

(I$_4$) D_2 is odd, (I$_5$) $\mathrm{ord}_2(D_4) = 1$.

If any of the conditions (I$_1$)–(I$_5$) is false, then we say that D is 2-*regular*. If in addition we have

$$P \in E_{\mathrm{ns}}(\mathbb{F}_p) \quad \text{for all primes } p \mid \mathrm{Disc}(E),$$

then we simply say that D is *regular.*

Remark 3.1. Our main result, Theorem 3.3, gives a good description of the index divisibility graph $\mathcal{S}(\mathsf{D})$ for regular EDS. Our decision to restrict attention to regular EDS represents a compromise between our desires for generality and conciseness, as well as the need to keep our exposition to a reasonable length. We remark that much of our analysis goes through for nonregular EDS, in the sense that Theorem 3.3 is still true for many (but generally not all) values of n, and that a long case-by-case analysis would give a lengthy statement that applies to most (maybe even all) values of n. In any case, we note that every $\mathsf{D} = (D_n)_{n\geq 1}$ contains a regular subsequence $\mathsf{D}' = (D_{nk})_{n\geq 1}$, and then Theorem 3.3 applies to this subsequence.

We start with a description of the index divisibility set of an EDS that will be a key tool for our classification. Its proof uses only the formal group properties of an EDS (Lemma 1.2).

Proposition 3.2. *Let* D *be a minimal regular EDS associated to the elliptic curve and point* (E, P). *Then the following are equivalent*:

(a) $n \mid D_n$, *i.e.*, $n \in \mathcal{S}(\mathsf{D})$.
(b) *There is some exponent* $e \geq 1$ *such that* $n \mid D_n^e$.
(c) *Every prime dividing* n *also divides* D_n.
(d) *For all primes* p, *we have* $p \mid n \Rightarrow r_p \mid n$.

Proof. Statements (b) and (c) are obviously equivalent, and (c) and (d) are equivalent by Lemma 1.1. It is also clear that (a) implies (b). It remains to show that (b) implies (a), i.e., that

$$n \mid D_n^e \to n \mid D_n.$$

It suffices to prove that for all primes p we have

$$p \mid \gcd(n, D_n) \;\Rightarrow\; \operatorname{ord}_p(D_n) \geq \operatorname{ord}_p(n). \tag{3.1}$$

So we let p be a prime dividing both n and D_n and we write $n = p^\nu k$ with $p \nmid k$ and $\nu \geq 1$. If $\nu = 1$, then (3.1) is obviously true (note $p \mid D_n$), so we may assume that $\nu \geq 2$.

We consider first the case that $p \mid D_{pk}$. Applying Lemma 1.2(a) to $D_n = D_{p^{\nu-1}\cdot pk}$, we obtain

$$\operatorname{ord}_p(D_n) = \operatorname{ord}_p(D_{p^\nu k}) \geq \operatorname{ord}_p(p^{\nu-1} D_{pk}) \geq \nu = \operatorname{ord}_p(n).$$

This shows that (3.1) is true in this case.

We next suppose that $p \nmid D_{pk}$, and we will show that either (3.1) is true or else D is 2-irregular. The assumption that $p \nmid D_{pk}$ is equivalent to $r_p \nmid pk$. But we are assuming that $p \mid D_{p^\nu k}$, so we have $r_p \mid p^\nu k$. It follows that $p^2 \mid r_p$, which is a very strong condition. In particular, since the regularity assumption implies that $P \in E_{\mathrm{ns}}(\mathbb{F}_p)$, and since r_p is the order of P in $E(\mathbb{F}_p)$, we find that

$$p^2 \mid \#E_{\mathrm{ns}}(\mathbb{F}_p).$$

Hence E has nonsingular reduction modulo p, and using the Hasse–Weil estimate, we further deduce that $p = 2$ and $r_2 = \#E(\mathbb{F}_2) = 4$. This gives conditions (I_1), (I_2), and (I_3) in the definition of 2-irregularity. Further, D_2 must be odd, since otherwise r_2 would divide 2, so we get condition (I_4).

Since $2 \mid D_4$, so $2 \mid D_{4k}$, we can apply Lemma 1.2(a) to $D_n = D_{2^{\nu-2}.4k}$ to obtain

$$\operatorname{ord}_2(D_n) = \operatorname{ord}_2(D_{2^\nu k}) \geq \operatorname{ord}_2(2^{\nu-2} D_{4k}) = \operatorname{ord}_2(D_{4k}) + \nu - 2.$$

If $\operatorname{ord}_2(D_4) \geq 2$, then this implies that $\operatorname{ord}_2(D_n) \geq \operatorname{ord}_2(n)$, so (3.1) is true and we are done. Otherwise $\operatorname{ord}_2(D_4) = 1$ and we have verified condition (I_5) for D to be 2-irregular. This is a contradiction, since we have assumed that D is regular, which completes the proof of Proposition 3.2. ■

We are now ready to state and prove our main theorem.

Theorem 3.3. *Let D be a minimal regular EDS associated to the elliptic curve and point (E, P).*

(a) *Let $n \geq 1$. Then*

$$n \in \mathcal{S}(\mathsf{D}) \text{ and } \begin{pmatrix} p \mid D_n \text{ or } E \text{ has} \\ \text{additive reduction at } p \end{pmatrix} \Rightarrow (n \to np) \in \operatorname{Arr}(\mathsf{D}).$$

(b) *Let $n \geq 1$ and $d \geq 1$. Then*

$$n \in \mathcal{S}(\mathsf{D}) \text{ and } d \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D}) \Rightarrow \begin{pmatrix} nd \in \mathcal{S}(\mathsf{D}) \text{ and} \\ \gcd(d,n) = 1 \text{ or } d \end{pmatrix}.$$

Furthermore,

$$n \in \mathcal{S}(\mathsf{D}) \text{ and } d \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D}) \text{ and } \gcd(d,n) = 1 \\ \Rightarrow (n \to nd) \in \operatorname{Arr}(\mathsf{D}).$$

(c) *Let $n \geq 1$ and let p be a prime such that*

$$n \in \mathcal{S}(\mathsf{D}), \quad p \nmid D_n, \quad \text{and} \quad (n \to np) \in \operatorname{Arr}(\mathsf{D}).$$

(1) *If E has good reduction at p and $\#E(\mathbb{F}_p) \neq 2p$, then $p \in \mathcal{A}(\mathsf{D})$. (If $p \geq 7$, then we always have $\#E(\mathbb{F}_p) \neq 2p$.)*

(2) *If E has bad reduction at p, then E has additive reduction at p.*

(d) *Let $n \geq 1$ and $d \geq 1$ with d composite. Define*

$$t = \text{number of primes } p \mid d \text{ such that } r_p \text{ is composite},$$
$$p_0 = \text{smallest prime divisor of } nd.$$

Suppose that $(n \to nd) \in \operatorname{Arr}(\mathsf{D})$. Then one of the following statements is true:

(i) *$t = 0$ and $d \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D})$.*

(ii) *$t \geq 1$ and*

$$\prod_{p \mid d} \left(1 + \frac{1}{\sqrt{p}}\right)^2 \geq \prod_{p \mid d} \frac{\#E(\mathbb{F}_p)}{p} \geq p_0^t. \tag{3.2}$$

Proof. (a) Suppose first that $n \in \mathcal{S}(\mathsf{D})$ and $p \mid D_n$. Write $n = p^i k$ with $p \nmid k$. Then

$$\begin{aligned} \operatorname{ord}_p(D_{np}) &\geq \operatorname{ord}_p(D_n) + 1 && \text{from Lemma 1.2(a)} \\ &\geq \operatorname{ord}_p(n) + 1 && \text{since } n \in \mathcal{S}(\mathsf{D}), \text{ i.e., } n \mid D_n \\ &= i + 1. \end{aligned}$$

Further, $k \mid n \mid D_n \mid D_{np}$. Hence $p^{i+1}k \mid D_{np}$, i.e., $np \mid D_{np}$, so $np \in \mathcal{S}(\mathsf{D})$. And since there are no proper divisors between n and np, it follows that the directed graph $\mathcal{S}(\mathsf{D})$ contains the arrow $n \to np$.

Next we consider the case that $n \in \mathcal{S}(\mathsf{D})$ and $p \nmid D_n$ and E has additive reduction. Additive reduction implies that $\#E_{\mathrm{ns}}(\mathbb{F}_p) = p$, so that $r_p \mid p$ and $p \mid D_p \mid D_{np}$. Meanwhile, $n \mid D_n \mid D_{np}$ by assumption. Since $p \nmid D_n$, it must be that $p \nmid n$. Hence $np \mid D_{np}$ and $np \in \mathcal{S}(\mathsf{D})$, from which we conclude that $(n \to np) \in \operatorname{Arr}(\mathsf{D})$.

(b) Let $d = p_1 \cdots p_\ell \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D})$ be a generalized aliquot number for D. We will show that $nd \in \mathcal{S}(\mathsf{D})$. First, let $p = p_i$ be one of the primes dividing d. The rank of apparition satisfies $r_{p_i} = p_{i+1}$, where for notational convenience we let $p_{\ell+1} = p_1$. Hence $p_i \mid D_{p_{i+1}} \mid D_{nd}$. Next let p be a prime dividing n. Then $p \mid n \mid D_n \mid D_{nd}$. We have shown that any prime p dividing nd satisfies $p \mid D_{nd}$. By Proposition 3.2, we conclude that $nd \in \mathcal{S}(\mathsf{D})$.

Now we determine the possible values of $\gcd(d, n)$. If $p_i \mid n$, then since $n \in \mathcal{S}(\mathsf{D})$, Proposition 3.2 implies that $p_{i+1} = r_{p_i}$ must divide n. Hence, by the construction of d, we see that either n is divisible by none of the primes dividing d, or it is divisible by all of them. Therefore $\gcd(d, n) = 1$ or d.

Suppose now that $\gcd(d, n) = 1$ and that e is a divisor of d such that $ne \in \mathcal{S}(\mathsf{D})$. Then by the reasoning of the last paragraph, with n replaced by ne, we find that $\gcd(d, ne) = 1$ or d. But $\gcd(d, n) = 1$ and $e \mid d$, so we conclude that $e = 1$ or $e = d$. Hence $(n \to nd) \in \operatorname{Arr}(\mathsf{D})$ by definition.

This completes the proof of (b). We also note that some condition such as $\gcd(n, d) = 1$ is necessary. For example, suppose that (p, q) is an amicable pair and that p divides D_n. Then there is no arrow from n to npq, because there are "shorter" arrows $n \to np \to npq$.

(c) We are given that $n \in \mathcal{S}(\mathsf{D})$, $np \in \mathcal{S}(\mathsf{D})$, and $p \nmid D_n$. Since $np \in \mathcal{S}(\mathsf{D})$, Proposition 3.2 implies $p \mid D_{np}$. We observe that

$$\begin{aligned} p \nmid D_n \ &\Leftrightarrow\ [n]P \not\equiv O \pmod{p}, \\ p \mid D_{np} \ &\Leftrightarrow\ [np]P \equiv O \pmod{p}. \end{aligned}$$

Hence under our assumptions, in particular the regularity assumption, we see that the point $[n]P$ has order exactly p in $P \in E_{\mathrm{ns}}(\mathbb{F}_p)$. Therefore $p \mid \#E_{\mathrm{ns}}(\mathbb{F}_p)$.

(c-1) Suppose first that E has good reduction at p, so $E_{\mathrm{ns}}(\mathbb{F}_p) = E(\mathbb{F}_p)$. We want to show that $p \in \mathcal{A}(\mathsf{D})$. The assumption that $\#E(\mathbb{F}_p) \neq 2p$, combined with Hasse's estimate $|p+1-\#E(\mathbb{F}_p)| \le 2\sqrt{p}$, implies that

$$p \mid \#E(\mathbb{F}_p) \;\Leftrightarrow\; \#E(\mathbb{F}_p) = p. \tag{3.3}$$

Since $r_p \mid \#E(\mathbb{F}_p)$, we see that $r_p = 1$ or $r_p = p$. But $r_p = 1$ implies that $p \mid D_1$, contradicting $p \nmid D_n$. Therefore $r_p = p$, which implies that $p \in \mathcal{A}(\mathsf{D})$, i.e., (p) is an aliquot cycle of length one.

(c-2) Next suppose that E has bad reduction at p. It follows from $p \mid E_{\mathrm{ns}}(\mathbb{F}_p)$ that E has additive reduction at p. (If it had multiplicative reduction, then $E_{\mathrm{ns}}(\mathbb{F}_p)$ would contain $p \pm 1$ points, depending on whether the reduction is split or nonsplit.)

(d) We first show that $\gcd(D_n, d) = 1$, which in particular implies that $\gcd(n, d) = 1$, since $n \mid D_n$. To see this, suppose to the contrary that $\gcd(D_n, d) > 1$, and let p be a prime dividing $\gcd(D_n, d)$. Since $p \mid D_n$, we know from (a) that $(n \to np) \in \mathrm{Arr}(\mathsf{D})$. But since $p \mid d$, we have the divisibilities $n \mid np \mid nd$, so the fact that $n \to np$ and $n \to nd$ are arrows implies that either $n = np$ or $np = nd$. Neither of these is possible, since $p \ge 2$, and d is composite by assumption. This completes the proof that $\gcd(D_n, d) = 1$.

In order to analyze the arrow $(n \to nd)$, we associate to the integer d a directed graph $\mathcal{G}_d$ as in the following lemma. The graph $\mathcal{G}_d$ classifies the primes dividing each rank of apparition r_p.

LEMMA 3.4. *Let D be a minimal regular EDS, let $n \ge 1$ and $d \ge 1$ with d composite, and assume that $(n \to nd) \in \mathrm{Arr}(\mathsf{D})$. We construct a directed graph $\mathcal{G}_d$ with vertices and arrows defined as follows:*

$$\mathrm{Ver}(\mathcal{G}_d) = \{\textit{primes } p \textit{ such that } p \mid d\},$$
$$\mathrm{Arr}(\mathcal{G}_d) = \{p \to q : q \mid d \textit{ and } q \mid r_p\}.$$

(N.B., the graph $\mathcal{G}_d$ is entirely distinct from the graph on $\mathcal{S}(\mathsf{D})$.)

(a) *Every vertex of $\mathcal{G}_d$ has an in-arrow.*

(b) *Every vertex of $\mathcal{G}_d$ has an out-arrow.*

(c) *The graph $\mathcal{G}_d$ is connected.*

Proof. Let $q \mid d$ be a prime divisor of d, i.e., q is a vertex of $\mathcal{G}_d$.

(a) We need to show that the vertex q has an in-arrow. Let $d' = d/q$. Since $(n \to nd) \in \mathrm{Arr}(\mathsf{D})$, we know that $nd' \notin \mathcal{S}(\mathsf{D})$. By Proposition 3.2, this implies the existence of a prime $p \mid nd'$ satisfying $r_p \nmid nd'$. Since $r_p \mid nd$ by Proposition 3.2, this implies that $q \mid r_p$, which shows $p \to q$ as required.

(b) We need to show that q has an out-arrow. Since $q \mid d$, we have $q \mid D_d$ or $r_q \mid d$. This shows that some prime $p \mid d$ satisfies $p \mid r_q$, and thus $q \to p$ as required.

(c) Define d' to be the part of d supported on primes appearing as vertices in a connected component $\mathcal{G}'$ of $\mathcal{G}_d$. Then for each prime $p \mid d'$, all primes dividing r_p appear in $\mathcal{G}'$ by connectedness. Since $r_p \mid nd$ by the assumption that $nd \in \mathcal{S}(\mathsf{D})$, this implies $r_p \,|\, nd'$. This shows that $nd' \in \mathcal{S}(\mathsf{D})$, which contradicts $(n \to nd) \in \operatorname{Arr}(\mathsf{D})$ unless $d' = 1$ or $d' = d$. So $\mathcal{G}_d$ is connected. ■

Suppose first that r_p is prime for every $p \,|\, d$. We need to prove that $d \in \mathcal{A}_{\text{gen}}(\mathsf{D})$. By definition, for every arrow $(p \to q) \in \operatorname{Arr}(\mathcal{G}_d)$ we have $q \,|\, r_p$, so the assumption that r_p is prime implies that $r_p = q$. In particular, every vertex in the finite directed graph $\mathcal{G}_d$ has at most one outgoing arrow. But Lemma 3.4(b) tells us that every vertex in $\mathcal{G}_d$ has at least one outgoing arrow, and Lemma 3.4(c) says that the graph is connected. It follows that $\mathcal{G}_d$ consists of a single loop,

$$\begin{tikzcd} p_1 \arrow[r] & p_2 \arrow[r] & p_3 \arrow[r] & \cdots \arrow[r] & p_t \arrow[llll, bend left] \end{tikzcd}$$

This loop satisfies $r_{p_i} = p_{i+1}$, so by definition $(p_1, \ldots, p_t)$ is a generalized aliquot cycle for D, and hence $p_1 \cdots p_t \in \mathcal{A}_{\text{gen}}(\mathsf{D})$. Since we also know that $\gcd(d, n) = 1$, it follows from part (c) of the theorem that

$$(n \to np_1 \cdots p_t) \in \operatorname{Arr}(\mathsf{D}).$$

But $np_1 \cdots p_t \,|\, nd$, so the fact that $(n \to nd) \in \operatorname{Arr}(\mathsf{D})$ implies that $d = p_1 \cdots p_t$. Hence $d \in \mathcal{A}_{\text{gen}}(\mathsf{D})$. This completes the proof of part (i).

In order to analyze the case that one or more of the r_p are composite, for each vertex $q \in \mathcal{G}_d$ we let

$$\operatorname{InDeg}(q) = \#\{p \,|\, d : (p \to q) \in \operatorname{Arr}(\mathcal{G}_d)\}$$

denote the in-degree of q, i.e., the number of arrows pointing in to q; and similarly $\operatorname{OutDeg}(q)$ will denote the out-degree of q. Lemma 3.4 tells us that $\operatorname{InDeg}(q) \geq 1$ for all $q \in \mathcal{G}_d$. For each $p \in \mathcal{G}_d$ we know that r_p is divisible by the primes at the tips of the outgoing arrows from p, so we can factor r_p as

$$r_p = \Bigl(\prod_{(p \to q) \in \operatorname{Arr}(\mathcal{G}_d)} q\Bigr) M_p \quad \text{for some } M_p \geq 1.$$

Further, from Proposition 3.2, the fact that $nd \in \mathcal{S}(\mathsf{D})$ and $p \,|\, d$ implies that $r_p \,|\, nd$, so every prime divisor of M_p is also a prime divisor of nd.

We now multiply over all $p \in \mathcal{G}_d$, i.e., over all $p \,|\, d$, and rearrange the terms to deduce that

$$\prod_{p|d} r_p = \prod_{p|d} \Bigl(\prod_{\substack{q|d \,\text{such that}\\ (p \to q) \in \operatorname{Arr}(\mathcal{G}_d)}} q\Bigr) M_p = \Bigl(\prod_{q|d} q^{\operatorname{InDeg}(q)}\Bigr)\Bigl(\prod_{p|d} M_p\Bigr).$$

Since $\operatorname{InDeg}(q) \geq 1$ for every $q \,|\, d$, we can rewrite this as

$$\prod_{p|d} \frac{r_p}{p} = \Bigl(\prod_{q|d} q^{\operatorname{InDeg}(q)-1}\Bigr)\Bigl(\prod_{p|d} M_p\Bigr), \tag{3.4}$$

where the right-hand side is a positive integer. Using the Hasse–Weil bound $(\sqrt{p}+1)^2 \geq \#E_{\mathrm{ns}}(\mathbb{F}_p)$ and the fact that $r_p \mid \#E_{\mathrm{ns}}(\mathbb{F}_p)$, we obtain the useful inequalities

$$\prod_{p\mid d}\Big(1+\frac{1}{\sqrt{p}}\Big)^2 \geq \prod_{p\mid d}\frac{\#E_{\mathrm{ns}}(\mathbb{F}_p)}{p} \geq \Big(\prod_{q\mid d} q^{\mathrm{InDeg}(q)-1}\Big)\Big(\prod_{p\mid d} M_p\Big). \tag{3.5}$$

We now use (3.5) to derive a bound that depends on the number of composite r_p. (See also Remark 4.2.) Let p_0 be the smallest prime divisor of nd. Then

$$\begin{aligned}\prod_{q\mid d} q^{\mathrm{InDeg}(q)-1} \geq \prod_{q\mid d} p_0^{\mathrm{InDeg}(q)-1} &= p_0^{\sum_{q\mid d}(\mathrm{InDeg}(q)-1)}\\ &= p_0^{\#\,\mathrm{Arr}(\mathcal{G}_d)-\#\,\mathrm{Ver}(\mathcal{G}_d)} = p_0^{\sum_{p\mid d}(\mathrm{OutDeg}(p)-1)}.\end{aligned} \tag{3.6}$$

Now consider a prime $p \in \mathcal{G}_d$ such that r_p is composite. If r_p is divisible by two or more primes that also divide d, then $\mathrm{OutDeg}(p) \geq 2$, so we get a factor of p_0 in (3.6). On the other hand, if there is some $q \mid r_p$ with $q \nmid d$, then $q \mid M_p$, so we get a factor of q in (3.5). Further, we must have $q \mid n$, since as noted earlier, $r_p \mid nd$. Thus $q \geq p_0$. This proves that every composite r_p with $p \mid d$ contributes a factor to (3.5) that is greater than or equal to p_0. Hence the lower bound in (3.5) is at least p_0^t, where t is the number of $p \mid d$ such that r_p is composite. ■

The following corollary may be compared with Smyth's result [19, Corollary 2] for Lucas sequences.

Corollary 3.5. *Let* D *be a minimal regular EDS, let* $n \in \mathcal{S}(\mathsf{D})$, *and let* m *be an integer of the form*

$$m = p_1 \cdots p_s \cdot d_1 \cdots d_t,$$

where the primes p_i *and integers* d_i *satisfy*

$$p_i \mid D_n \quad \text{and} \quad d_i \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D}).$$

Then $nm \in \mathcal{S}(\mathsf{D})$.

Proof. This is immediate from Theorem 3.3(a,b) and induction on the number of factors of m. ■

4. Remarks on arrow construction. In this section we make a number of remarks concerning the existence of index divisibility arrows as described in Theorem 3.3, and we give examples of nonstandard arrows as per Theorem 3.3(d-ii). We assume throughout that our EDS is minimal and regular.

Remark 4.1. Given an element $n \in \mathcal{S}(\mathsf{D})$, Theorem 3.3 gives two "standard" ways to create arrows $(n \to nd) \in \mathrm{Arr}(\mathsf{D})$. First, Theorem 3.3(a) gives an arrow $n \to np$ for each prime $p \mid D_n$. Second, Theorem 3.3(b) gives an arrow for each aliquot number $d \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D})$ that is prime to n. Conversely, Theorem 3.3(d) implies that any "nonstandard" arrow satisfies

$$\prod_{p|d}\left(1+\frac{1}{\sqrt{p}}\right) \ge \sqrt{2}. \tag{4.1}$$

In particular, writing $\nu(d)$ for the number of distinct prime divisors of d and $p_{\min}(d)$ for the smallest prime dividing d, we have

$$\nu(d) \ge \frac{\frac{1}{2}\log 2}{\log(1+p_{\min}(d)^{-1/2})} = \frac{\log 2}{2}\sqrt{p_{\min}(d)} + O(1).$$

Thus if the smallest prime divisor of d is large, then $\nu(d)$ will be large, and d will be enormous. The following brief table uses (4.1) to give the smallest values of $\nu(d)$ and d for various values of $p_{\min}(d)$.

$p_{\min}(d) \ge$	10	10^2	10^3	10^4	10^5
$\nu(d) \ge$	2	4	12	36	100
$d \ge$	143	$1.21 \cdot 10^8$	$1.56 \cdot 10^{36}$	$1.80 \cdot 10^{144}$	$1.85 \cdot 10^{500}$

And if Theorem 3.3(d) gives a lower bound for (4.1) that is larger than $\sqrt{2}$, then the lower bounds for $\nu(d)$ and d in terms of $p_{\min}(d)$ will be even larger.

Remark 4.2. The formulas (3.4) and (3.5) derived during the course of proving Theorem 3.3(d) impose stringent conditions on the allowable values of d. We used these formulas to derive a general lower bound, but when analyzing a specific EDS, it is probably best to use them directly. We also note, although we will not prove, that (3.4) is true even if d is divisible by primes for which P has singular reduction. Similarly, the following version of (3.5) is true in general:

$$\prod_{p|d}\frac{\#\mathfrak{E}(\mathbb{F}_p)}{p} \ge \Bigl(\prod_{q|d} q^{\mathrm{InDeg}(q)-1}\Bigr)\Bigl(\prod_{p|d} M_p\Bigr),$$

where $\mathfrak{E}$ is the Néron model of E. Note that if E has bad reduction, then $\#\mathfrak{E}(\mathbb{F}_p) = c_p\#E_{\mathrm{ns}}(\mathbb{F}_p)$, where c_p is the number of components in the special fiber above p. In particular, $c_p \le 4$ unless the reduction is split multiplicative, in which case $c_p = \mathrm{ord}_p(\mathrm{Disc}(E))$.

Example 4.3. Continuing with the EDS associated to the elliptic curve and point from Example 0.1, we have

$$\mathrm{Disc}(E) = 37, \qquad \#E(\mathbb{F}_2) = 5, \qquad \#E(\mathbb{F}_3) = 7, \qquad \#E(\mathbb{F}_5) = 8.$$

In particular, E has multiplicative reduction at 37 and good reduction elsewhere, the point P is in $E_{\mathrm{ns}}(\mathbb{F}_{37})$, and $\#E(\mathbb{F}_p) \ne 2p$ for all primes p. Further, since $D_5 = 2$ and $D_{10} = 4$, we see that Lemma 1.2(b) is true even for $p = 2$ and all values of n and k, so we can treat 2 as we do all other primes.

We claim that for all primes p,

$$p \mid D_n \text{ or } p \in \mathcal{A}(\mathsf{D}) \;\Leftrightarrow\; (n \to np) \in \operatorname{Arr}(\mathsf{D}).$$

The implication $\Rightarrow$ follows directly from Theorem 3.3(a,c). Conversely, if $(n \to np) \in \operatorname{Arr}(\mathsf{D})$, then either $p \mid D_n$, or else Theorem 3.3(c) tells us that $p \in \mathcal{A}(\mathsf{D})$. We thus have a precise description of the arrows of prime weight.

Theorem 3.3(d) says that arrows $n \to nd$ of composite weight with $d \notin \mathcal{A}_{\mathrm{gen}}(\mathsf{D})$ have d values that either are divisible by small primes or are huge. Further, examining the proof of Theorem 3.3(d) shows that the prime divisors of such d must satisfy some fairly stringent conditions. We suspect that for this example there are no such arrows, i.e.,

$$\begin{pmatrix} d \text{ is prime} \\ \text{and } d \mid D_n \end{pmatrix} \text{ or } d \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D}) \;\overset{?}{\Leftrightarrow}\; (n \to nd) \in \operatorname{Arr}(\mathsf{D}).$$

Example 4.4. The following example shows that "nonstandard" arrows exist (cf. Remark 4.1). Let D be the EDS associated to

$$E : y^2 + 2xy + y = x^3 + x^2 + 7x + 4 \quad \text{and} \quad P = (4, 7).$$

The curve E is nonsingular at 2, 3, and 5, and

$$\#E(\mathbb{F}_2) = 3, \qquad \#E(\mathbb{F}_3) = 5, \qquad \#E(\mathbb{F}_5) = 6.$$

Further, the point P has exact order 6 in $E(\mathbb{F}_5)$. Thus $r_2 = 3$, $r_3 = 5$, and $r_5 = 6$, so

$$2, 3, 5, 6, 10, 15 \notin \mathcal{S}(\mathsf{D}) \quad \text{and} \quad 1, 30 \in \mathcal{S}(\mathsf{D}). \tag{4.2}$$

Alternatively, we can verify (4.2) directly by explicitly computing the relevant terms of D,

$$\begin{array}{llll} D_1 \bmod 1 = 0, & D_2 \bmod 2 = 1, & D_3 \bmod 3 = 2, & D_5 \bmod 5 = 4, \\ D_6 \bmod 6 = 4, & D_{10} \bmod 10 = 3, & D_{15} \bmod 15 = 3, & D_{30} \bmod 30 = 0. \end{array}$$

It follows from the definition of the directed graph $\mathcal{S}(\mathsf{D})$ that $(1 \to 30) \in \operatorname{Arr}(\mathsf{D})$. However, since $r_5 = 6$ is not prime, we have $30 \notin \mathcal{A}_{\mathrm{gen}}(\mathsf{D})$. Thus the arrow $1 \to 30$ is not predicted by Theorem 3.3(d-i). This does not contradict the theorem, of course, since

$$\frac{\#E(\mathbb{F}_2)}{2} \cdot \frac{\#E(\mathbb{F}_3)}{3} \cdot \frac{\#E(\mathbb{F}_5)}{5} = \frac{3}{2} \cdot \frac{5}{3} \cdot \frac{6}{5} = 3,$$

so condition (3.2) is satisfied and we are in the situation of Theorem 3.3(d-ii).

Remark 4.5. Generalizing Example 4.4, we sketch how to construct EDS having nonstandard arrows with arbitrarily large values of d. The proof of Theorem 3.3(d) suggests the method. We start with primes $p_1, \dots, p_N$ and integers $n_1, \dots, n_N$ and $k_1, \dots, k_N$ satisfying

$$|p_i + 1 - k_i n_i| < 2\sqrt{p_i}.$$

Our goal is to find an elliptic curve $E/\mathbb{Q}$ and point $P \in E(\mathbb{Q})$ such that $\#E(\mathbb{F}_{p_i}) = k_i n_i$ and $r_{p_i} = n_i$ for all $1 \le i \le N$.

A theorem of Deuring [4] says that there exists an elliptic curve $E_i/\mathbb{F}_{p_i}$ satisfying

$$\#E_i(\mathbb{F}_{p_i}) = k_i n_i,$$

and a result of Rück [15, Theorem 3] says that we can choose E_i so that the group structure of $E_i(\mathbb{F}_{p_i})$ ensures the existence of a point $P_i \in E_i(\mathbb{F}_p)$ of order n_i. Making a change of coordinates, we may assume that $P_i = (0, 0)$.

Next we apply the Chinese remainder theorem to the coefficients of the Weierstrass equations of $E_1, \dots, E_n$. This gives an elliptic curve $E/\mathbb{Q}$ with $(0, 0) \in E(\mathbb{Q})$ that satisfies

$$E \bmod p_i \cong E_i, \quad 1 \le i \le N.$$

If the Weierstrass equation for E is not globally minimal, then we can change coordinates to make it minimal without affecting the reduction at $p_1, \dots, p_N$, since they are primes of good reduction. For simplicity, we will assume that some n_i is divisible by a prime greater than 7, since then Mazur's theorem [16, VIII.7.5] ensures that $(0, 0)$ is not a torsion point. We may thus associate to E and P an elliptic divisibility sequence $\mathsf{D} = (D_n)_{n \ge 1}$ satisfying

$$r_{p_i} = n_i \quad \text{for all } 1 \le i \le N.$$

Finally, we observe that arbitrarily large nonstandard arrows can be constructed in this way. We begin with any prime p_1, we let $p_1, \dots, p_N$ be a list of consecutive primes, and we set

$$d = p_1^2 p_2 p_3 \cdots p_N.$$

We then find a curve and point whose associated EDS satisfies

$$r_{p_i} = p_{i+1}, \quad 1 \le i \le N - 1, \quad r_{p_N} = p_1^2.$$

If the list of primes is long enough, then the final condition $r_{p_N} = p_1^2$ is allowed by Hasse's bound, and we can proceed as in the description above to find a sequence $\mathsf{D} = (D_n)_{n \ge 1}$ with $(1 \to d) \in \mathrm{Arr}(\mathsf{D})$.

Example 4.6. We use the method described in Remark 4.5 to construct a nonstandard arrow $1 \to d$ for the moderately large integer

$$d = 5^2 \cdot 7 \cdot 11 \cdot 17 = 32725.$$

We want to construct an elliptic curve $E/\mathbb{Q}$ and point $P \in E(\mathbb{Q})$ satisfying

$$r_5 = 7, \quad r_7 = 11, \quad r_{11} = 17, \quad r_{17} = 25. \tag{4.3}$$

Then the associated sequence $\mathsf{D} = (D_n)_{n\ge 1}$ will have $(1 \to d) \in \mathrm{Arr}(\mathsf{D})$, according to Proposition 3.2.

To do this, we first find elliptic curves $E_5/\mathbb{F}_5$, $E_7/\mathbb{F}_7$, $E_{11}/\mathbb{F}_{11}$ and $E_{17}/\mathbb{F}_{17}$ satisfying

$$\#E_5(\mathbb{F}_5) = 7, \quad \#E_7(\mathbb{F}_7) = 11, \quad \#E_{11}(\mathbb{F}_{11}) = 17, \quad \#E_{17}(\mathbb{F}_{17}) = 25.$$

This is possible because the Hasse bound is satisfied in each instance. We then use the Chinese remainder theorem to find an elliptic curve E with minimal Weierstrass equation

$$y^2 + y = x^3 + x^2 - 1\,291\,874\,622\,406\,186x + 17\,872\,226\,251\,073\,822\,113\,702,$$

and point

$$P = (20\,751\,503, 1\,073\,344).$$

(We have moved P away from $(0,0)$ to make the numbers a bit smaller.) The associated sequence $\mathsf{D} = (D_n)_{n\ge 1}$ begins

$$1, \quad 2\,146\,689, \quad 286\,883\,381\,041\,833\,542\,301,$$
$$60\,768\,120\,452\,650\,698\,495\,048\,133\,538\,894\,517, \ldots.$$

By construction, $(1 \to 32725) \in \mathrm{Arr}(\mathsf{D})$. Of course, the 32725th term is too large to print, but the claim can be verified by computation modulo 32725.

For this example, we can verify equation (3.2) in Theorem 3.3(d), which states

$$\prod_{p\mid d}\left(1 + \frac{1}{\sqrt{p}}\right)^2 \ge p_0^t. \tag{4.4}$$

In our case, $p_0 = 5$, $t = 1$, and the left-hand side exceeds 10.

Remark 4.7. In the definition of EDS, the elliptic curve may be replaced with a singular cubic curve as long as P is a nonsingular point, since $E_{\mathrm{ns}}(\mathbb{Q})$ is a group. More precisely, $E_{\mathrm{ns}}(\mathbb{Q})$ is either the additive group $\mathbb{Q}^+$, the multiplicative group $\mathbb{Q}^*$, or a subgroup of a quadratic twist of the multiplicative group; see [16, III.2.5, Exercise 3.5]. Thus EDS on singular elliptic curves are closely related to Lucas sequences.

For example, consider the nodal singular cubic curve and point

$$C : y^2 + 3xy + 3y = x^3 + 2x^2 + x \quad \text{and} \quad P = (0,0).$$

The associated EDS,

$$\mathsf{D} : 1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots,$$

consists of the even-indexed Fibonacci numbers. This is exactly the Lucas sequence generated by

$$L_{n+2} = 3L_{n+1} - L_n, \quad L_0 = 0, \quad L_1 = 1.$$

The index divisibility set of D is

$$\mathcal{S}(\mathsf{D}) = \{1, 5, 6, 12, 18, 24, 25, 30, 36, 48, 54, 55, 60, 72, 84, \ldots\}.$$

In the notation of Smyth's Theorem 0.2, we have

$$a = 3, \quad b = 1, \quad \Delta = 5, \quad \mathcal{B}_{3,1} = \{1 \to 6\}.$$

In the language of our paper, $5, 6 \in \mathcal{A}_{\mathrm{gen}}(\mathsf{D})$, since

$$r_2 = 3, \quad r_3 = 2, \quad r_5 = 5.$$

Thus $(2, 3)$ and (5) are generalized aliquot cycles. Notice that the curve C reduces modulo p to a curve having p, $p-1$ or $p+1$ nonsingular points according as p ramifies, splits, or is inert in $\mathbb{Q}(\sqrt{5})$.

In general, our Theorem 3.3 and Smyth's Theorem 0.2 can probably be combined into a general theorem on (possibly singular) cubic curves. Notice that Smyth's set $\mathcal{B}_{a,b}$ may include nonstandard arrows in the case of the multiplicative group, although the analysis is simpler because $\#C_{\mathrm{ns}}(\mathbb{F}_p) \in \{p, p+1, p-1\}$. The primes p dividing $\Delta = a^2 - 4b$ are the primes for which the group underlying the Lucas sequence reduces to the additive group $\mathbb{F}_p^+$. They are thus analogous to the primes of additive reduction whose arrows $(n \to np)$ are described in Theorem 3.3(a,c). We also note that in the multiplicative group case we never have $r_2 = 4$, so we are always in the 2-regular setting.

5. Elliptic aliquot cycles. Let D be an EDS with associated elliptic curve and point (E, P), and let $(p, q) \in \mathcal{A}(\mathsf{D})$ be an amicable pair for D. Then the point P has order q modulo p, and P has order p modulo q. This implies that

$$q \mid \#E(\mathbb{F}_p) \quad \text{and} \quad p \mid \#E(\mathbb{F}_q).$$

Conversely, if we are given D and (E, P), and if p and q are distinct primes of good reduction satisfying

$$\#E(\mathbb{F}_p) = q \quad \text{and} \quad \#E(\mathbb{F}_q) = p, \tag{5.1}$$

then (p, q) is automatically an amicable pair for D.

We note that the conditions (5.1) do not refer to the point P. This leads to the following definitions.

Definition 7. Let $E/\mathbb{Q}$ be an elliptic curve. An *aliquot cycle of length ℓ* for $E/\mathbb{Q}$ is a list $p_1, \ldots, p_\ell$ of distinct primes such that E has good reduction at every p_i and

$$\#E(\mathbb{F}_{p_1}) = p_2, \quad \#E(\mathbb{F}_{p_2}) = p_3, \ \ldots, \ \#E(\mathbb{F}_{p_{\ell-1}}) = p_\ell, \quad \#E(\mathbb{F}_{p_\ell}) = p_1.$$

An *amicable pair* for $E/\mathbb{Q}$ is an aliquot cycle of length 2.

Remark 5.1. The distribution of amicable pairs and aliquot cycles on elliptic curves is studied in [17]. In particular, it turns out that elliptic curves with complex multiplication behave quite differently from curves without CM. For the convenience of the reader, we briefly summarize some of the material in [17].

- If $E(\mathbb{Q})$ contains a nontrivial torsion point, then E has (essentially) no aliquot cycles. This is clear since $E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow E(\mathbb{F}_p)$ for all primes $p \nmid 2\,\mathrm{Disc}_{E/\mathbb{Q}}$; cf. [17, Remark 5].
- For any ℓ, there exists an elliptic curve $E/\mathbb{Q}$ that has an aliquot cycle of length ℓ. More generally, for any $\ell_1, \dots, \ell_s$ there exists an elliptic curve having disjoint aliquot cycles of length $\ell_1, \dots, \ell_s$ [17, Theorem 13].
- Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication and $j(E) \neq 0$. Then E has no aliquot cycles of length $\ell \geq 3$ composed of primes $p \geq 5$ [17, Corollary 16].
- Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 0$. Then E has no aliquot cycles of length 3 composed of primes $p \geq 11$ [17, Proposition 48].
- *Conjecture*: Assume that there are infinitely many primes p such that $\#E(\mathbb{F}_p)$ is prime. If E does not have CM, then
$$\#\{\text{aliquot cycles } (p_1, \dots, p_\ell) \text{ with } p_i \leq X\} \gg\ll \frac{\sqrt{X}}{(\log X)^\ell}.$$
If E has CM, then there is a constant $C_E > 0$ such that
$$\#\{\text{amicable pairs } (p, q) \text{ with } p, q \leq X\} \sim C_E \frac{X}{(\log X)^2}.$$

The next proposition shows that aliquot cycles for an elliptic divisibility sequence are closely related to aliquot cycles on the associated elliptic curve.

Proposition 5.2. *Let* D *be a minimal EDS, and let* (E, P) *be the associated elliptic curve* $E/\mathbb{Q}$ *and point* $P \in E(\mathbb{Q})$.

(a) *Let* $(p_1, \dots, p_\ell)$ *be an aliquot cycle for* $E/\mathbb{Q}$ *such that* $p_i \nmid D_1$ *for all* i. *Then* $(p_1, \dots, p_\ell)$ *is an aliquot cycle for* D.

(b) *Let* $(p_1, \dots, p_\ell)$ *be an aliquot cycle for* D. *Then*

$$\prod_{i=1}^{\ell} \frac{\#E(\mathbb{F}_{p_i})}{p_i} < 2 \;\Rightarrow\; \begin{pmatrix} (p_1, \dots, p_\ell) \textit{ is an} \\ \textit{aliquot cycle for } E \end{pmatrix}. \tag{5.2}$$

In particular,

$$\min_{1 \leq i \leq \ell} p_i > \frac{1}{(2^{1/2\ell} - 1)^2} \;\Rightarrow\; \begin{pmatrix} (p_1, \dots, p_\ell) \textit{ is an} \\ \textit{aliquot cycle for } E \end{pmatrix} \tag{5.3}$$

(*cf. Theorem* 3.3(d)).

Proof. (a) If $(p_1, \dots, p_\ell)$ is an aliquot cycle for $E/\mathbb{Q}$, then for all i we know that $\#E(\mathbb{F}_{p_i}) = p_{i+1}$ is prime. Since $p_{i+1} \nmid D_1$, the order of the point P

in $E(\mathbb{F}_{p_i})$ must equal p_{i+1}. Therefore $r_{p_i}(\mathsf{D}) = p_{i+1}$, so the cycle is aliquot for D.

(b) The proof is similar to the proof of Theorem 3.3(d). We are given that $r_{p_i}(\mathsf{D}) = p_{i+1}$ for all i, or equivalently, the point P has order p_{i+1} in the group $E(\mathbb{F}_{p_i})$. Thus for every $1 \le i \le \ell$ we have

$$\#E(F_{p_i}) = p_{i+1}M_{p_i} \qquad \text{for some } M_{p_i} \ge 1.$$

Multiplying for $1 \le i \le \ell$ and dividing by $p_1 \cdots p_\ell$ yields

$$\prod_{i=1}^{\ell} \frac{\#E(\mathbb{F}_{p_i})}{p_i} = \prod_{i=1}^{\ell} M_i.$$

Thus the assumption that $\prod_i \#E(\mathbb{F}_{p_i})/p_i < 2$ implies that $M_i = 1$ for every i, so $(p_1, \ldots, p_\ell)$ is an aliquot cycle for E. This proves (5.2).

To prove (5.3), we use the Hasse–Weil bound $\#E(\mathbb{F}_p) \le (\sqrt{p}+1)^2$ to obtain

$$\prod_{i=1}^{\ell} \frac{\#E(\mathbb{F}_{p_i})}{p_i} \le \prod_{i=1}^{\ell}\left(1+\frac{1}{\sqrt{p_i}}\right)^2 \le \left(1+\frac{1}{\min\limits_i \sqrt{p_i}}\right)^{2\ell}.$$

Now a little bit of algebra, combined with (5.2), yields (5.3). ∎

6. Miscellaneous remarks. We conclude with two brief remarks.

Remark 6.1. Recall that a sequence $\mathsf{A} = (A_n)_{n\ge1}$ is called a *divisibility sequence* if

$$m \mid n \;\Rightarrow\; A_m \mid A_n.$$

Examples of divisibility sequences include Lucas sequences of the first kind, the odd terms of Lucas sequences of the second kind, and elliptic divisibility sequences. We observe that if A is a divisibility sequence, then

$$n \in \mathcal{S}(\mathsf{A}) \text{ and } d \mid D_n \text{ and } \gcd(n,d) = 1 \;\Rightarrow\; nd \in \mathcal{S}(\mathsf{A}).$$

In particular, there is a sequence of arrows in $\mathrm{Arr}(\mathsf{A})$ satisfying

$$n \to \cdots \to nd.$$

This is one way in which the index divisibility graph of divisibility sequences exhibits a structure not found for arbitrary sequences. It might be interesting to see if there are any other general statements that one can make about the index divisibility graph of general divisibility sequences.

Remark 6.2. A classical alternative definition of an elliptic divisibility sequence is a sequence of integers $\mathsf{W} = (W_n)_{n\ge1}$ defined by four initial terms (W_1, W_2, W_3, W_4) and satisfying the recursion

$$W_{n+m}W_{n-m}W_r^2 = W_{n+r}W_{n-r}W_m^2 - W_{m+r}W_{m-r}W_n^2 \quad \text{for all } n > m > r.$$

One can show that if the sequence is normalized by $W_1 = 1$ and $W_2 \mid W_4$, then every term is an integer. Ward [25, 26] was the first to study the arithmetic properties of these sequences. Under some nondegeneracy conditions, he showed that there is an elliptic curve $E/\mathbb{Q}$ given by a Weierstrass equation and a point $P \in E(\mathbb{Q})$ such that $W_n = \psi_n(P)$, where ψ_n is the nth division polynomial for E [16, Exercise 3.7]. (See [25] or [18, Appendix A] for explicit formulas for E and P in terms of the initial terms of the EDS.) In particular, if $\mathsf{D} = (D_n)_{n\geq 1}$ is the EDS associated to (E, P), then $D_n \mid W_n$ for all $n \geq 1$. Thus

$$n \mid D_n \;\Rightarrow\; n \mid W_n, \tag{6.1}$$

so index divisibility for D is a stronger condition than it is for W. Further, one can show that $\operatorname{ord}_p(D_n) = \operatorname{ord}_p(W_n)$ for all primes p at which the Weierstrass equation has good reduction, so the implication in (6.1) can be reversed if we ignore primes of bad reduction. This shows that the divisibility properties of D and W are closely related. We have chosen in this paper to concentrate on the former.

Acknowledgments. The first author's research was supported by NSF DMS-0650017 and DMS-0854755. The second author's research was supported by NSERC PDF-373333. The research in this note was performed while the first author was a long-term visiting researcher at Microsoft Research New England and included a short visit by the second author. Both authors thank MSR for its hospitality during their visits.

References

[1] R. André-Jeannin, *Divisibility of generalized Fibonacci and Lucas numbers by their subscripts*, Fibonacci Quart. 29 (1991), 364–366.

[2] D. Bleichenbacher, *Breaking a cryptographic protocol with pseudoprimes*, in: Public Key Cryptography—PKC 2005, Lecture Notes in Comput. Sci. 3386, Springer, Berlin, 2005, 9–15.

[3] G. Cornelissen and K. Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. 613 (2007), 1–33.

[4] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.

[5] M. Einsiedler, G. Everest, and T. Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. 4 (2001), 1–13.

[6] K. Eisenträger and G. Everest, *Descent on elliptic curves and Hilbert's tenth problem*, Proc. Amer. Math. Soc. 137 (2009), 1951–1959.

[7] G. Everest and H. King, *Prime powers in elliptic divisibility sequences*, Math. Comp. 74 (2005), 2061–2071.

[8] G. Everest, G. Mclaren, and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory 118 (2006), 71–89.

[9] V. E. Hoggatt, Jr. and G. E. Bergum, *Divisibility and congruence relations*, Fibonacci Quart. 12 (1974), 189–195.

[10] D. Jarden, *Divisibility of terms by subscripts in Fibonacci's sequence and associate sequence*, Riveon Lematematika 13 (1959), 51–56.

[11] A. Paszkiewicz and A. Rotkiewicz, *On pseudoprimes of the form $a^n - a$*, Proc. Eleventh Internat. Conf. on Fibonacci Numbers and their Applications, Congr. Numer. 194 (2009), 191–197.

[12] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. 37 (1981), 587–593.

[13] B. Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$*, J. Amer. Math. Soc. 16 (2003), 981–990.

[14] A. Rotkiewicz, *Solved and unsolved problems on pseudoprime numbers and their generalizations*, in: Applications of Fibonacci Numbers, Vol. 8 (Rochester, NY, 1998), Kluwer, Dordrecht, 1999, 293–306.

[15] H.-G. Rück, *A note on elliptic curves over finite fields*, Math. Comp. 49 (1987), 301–304.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

[17] J. H. Silverman and K. E. Stange, *Amicable pairs and aliquot cycles for elliptic curves*, Experiment. Math., to appear.

[18] J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence*, J. Ramanujan Math. Soc. 21 (2006), 1–17.

[19] C. Smyth, *The terms in Lucas sequences divisible by their indices*, J. Integer Sequences 13 (2010), no. 2, art. 10.2.4, 18 pp.

[20] L. Somer, *Divisibility of terms in Lucas sequences by their subscripts*, in: Applications of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992), Kluwer, Dordrecht, 1993, 515–525.

[21] —, *Divisibility of terms in Lucas sequences of the second kind by their subscripts*, in: Applications of Fibonacci Numbers, Vol. 6 (Pullman, WA, 1994), Kluwer, Dordrecht, 1996, 473–486.

[22] K. E. Stange, *The Tate pairing via elliptic nets*, in: Pairing-based Cryptography—Pairing 2007, Lecture Notes in Comput. Sci. 4575, Springer, Berlin, 2007, 329–348.

[23] S. S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith. 41 (1982), 141–150.

[24] G. Walsh, *On integers n with the property $n \mid f_n$*, unpublished, 1986, 5 pp.

[25] M. Ward, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. 15 (1948), 941–946.

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

Joseph H. Silverman
Mathematics Department, Box 1917
Brown University
Providence, RI 02912, U.S.A.
E-mail: jhs@math.brown.edu

Katherine E. Stange
Department of Mathematics
Simon Fraser University
8888 University Drive
Burnaby, BC, Canada V5A 1S6
and
Pacific Institute for the Mathematical Sciences
200 1933 West Mall
Vancouver, BC, Canada V6T 1Z2
E-mail: stange@pims.math.ca

Received on 29.1.2010
and in revised form on 19.4.2010 (6289)