New York Journal of Mathematics

New York J. Math. **18** (2012) 409–420.

On positive integers n dividing the nth term of an elliptic divisibility sequence

Avram Gottschlich

Abstract. Elliptic divisibility sequences are integer sequences related to the denominator of the first coordinate of the n-fold sum of a nontorsion rational point on an elliptic curve. Silverman and Stange recently studied those integers n dividing D_n, where $\{D_n\}$ is an elliptic divisibility sequence. Here we discuss the distribution of these numbers n.

Contents

1. Introduction

In this paper we investigate the distribution of indices of an elliptic divisibility sequence that divide the corresponding term. This type of problem has been studied before in the cases of the Fibonacci sequence, the more general Lucas sequences, and the even more general case of linear recurrence relations of arbitrary size. See [1], [8], [15], [16] for results on these topics.

The following definitions all come from Silverman and Stange ([14]). Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation, with P a nontorsion rational point on E. We can iteratively add P to itself, producing points P, $[2]P$, $[3]P$, etc., with corresponding (rational) coordinates $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, etc. If we write $x_n = \frac{A_n}{D_n^2}$ in lowest terms with $D_n > 0$, this sequence $\{D_n\}$, dependent only on E and P, is called an elliptic divisibility sequence. As the name suggests, this is a divisibility sequence, i.e., $m \mid n \Rightarrow D_m \mid D_n$ (shown in [14]).

Silverman and Stange described how to use values of n for which $n \mid D_n$ to generate larger values of such n, either by using the prime factors of the original n or by using what they call aliquot numbers, the product of

Received September 20, 2011. Revised May 17, 2012.
2010 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Elliptic divisibility sequence, elliptic curve, rational point.

ISSN 1076-9803/2012

the members of an aliquot cycle of primes of good reduction for E. An aliquot cycle of primes for an elliptic curve E is a list of primes of good reduction $(p_1, \ldots, p_l)$ with $p_{i+1} = \min\{r \geq 1 : p_i \mid D_r\}$ for all $1 \leq i \leq l$, where $p_{l+1} = p_1$ to complete the cycle. Elliptic divisibility sequences are examples of nontrivial nonlinear recursions with enough additional structure to make them amenable to Diophantine analysis. There exist applications to Hilbert's 10th problem and to cryptography (see [6], [7], [12], [17]).

Our goal is to bound the number of $n \in [1, x]$ for which $n \mid D_n$.

Theorem 1.1. *For $x \geq 20$, let $N(x) = N_{E,P}(x)$ be the set of integers $n \leq x$ with $n \mid D_n$. Then the estimate*

$$\#N(x) \leq O_{E,P}\left(\frac{x(\log\log x)^{5/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}\right)$$

holds.

We do not have an asymptotic at this time for $N(x)$.

Ward defines another divisibility sequence (see [18], [19]) via a nonlinear recurrence relation. A sequence of integers $\{W_n\}$ is defined via four initial terms (W_1, W_2, W_3, W_4) and the relation

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

Ward first determined the arithmetic properties of these sequences; assuming some nondegeneracy conditions he showed that there is some elliptic curve $E/\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$ with

$$W_n = \psi_n(P),$$

where ψ is the nth division polynomial for E. These polynomials are defined via a recurrence relation; if $E : y^2 = x^3 + Ax + B$, then the ψ_n are found in $\mathbb{Z}[A, B, x, y]$ and are defined in [9]:

$$\begin{aligned}
&\psi_1 = 1, \quad \psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,\\
&\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ (m \geq 2),\\
&2y\psi_{2m} = \psi_m(\psi_{m+1}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ (m \geq 2).
\end{aligned}$$

The paper [18] contains explicit formulas for E and P in terms of the initial terms of Ward's divisibility sequence. If D_n is the elliptic divisibility sequence associated to (E, P), then $D_n \mid W_n$ for all $n \geq 1$, so the two definitions are closely related. We focus on the first definition given, although we use the sequence $\{W_n\}$ to help with a lemma.

Definition 1.2. If some member of the elliptic divisibility sequence D_n is divisible by m, then the *rank of appearance* of m, denoted $r_m = r_m(D)$, is the minimal integer $r \geq 1$ with $m \mid D_r$.

For primes p of good reduction, r_p is also the smallest integer $r \geq 1$ such that $[r]P \equiv \mathcal{O} \pmod{p}$, so this number does exist for all such primes, since $E(\mathbb{F}_p)$ is a finite group for such primes. Define $v_p(n) = k$, where $p^k \parallel n$. While we will only use the rank of appearance of primes, it can be generalized to all odd positive integers n using Lemma 5 of [14], which says that $v_p(D_{mn}) \geq v_p(mD_n)$, with equality holding unless $p = 2$, $2 \mid m$, $v_2(D_n) = 1$, and E has either ordinary or multiplicative reduction at 2. Hence we can sometimes use this to derive r_{p^a} for p odd, and use the lcm of the various $p^a \parallel n$ to derive r_n for n odd.

Definition 1.3. An *anomalous prime* for an elliptic curve E is a prime p of good reduction such that $\#E(\mathbb{F}_p) = p$.

The term anomalous prime comes from a work of Mazur [10] in which he studied rational points of elliptic curves in towers of number fields.

It is well known that due to a result of Hasse, the size of the group $E(\mathbb{F}_p)$ is $p + 1 - a_p$, where $|a_p| \leq 2\sqrt{p}$. Assuming $r_p > 1$, an equivalent definition for an anomalous prime $p > 5$ for an elliptic curve E is a prime for which $r_p = p$, since $r_p \mid \#E(\mathbb{F}_p)$, and $\#E(\mathbb{F}_p) < 2p$ for $p > 5$. For the general case, numbers n whose large prime factors are anomalous primes prove to potentially be the largest subset of $n \mid D_n$. There are certain properties of elliptic curves which lead to a smaller number of anomalous primes; these properties allow us to find a better bound.

Definition 1.4. An elliptic curve E is *c-nomalous* if

$$S(x) = \#\{p \leq x : p \text{ is anomalous}\}$$

can be bounded by $O_E(x^{1-c})$.

The Lang–Trotter conjecture says that for an elliptic curve E with no CM and nonzero trace, the number of primes $p \leq x$ with $a_p = k$ should be asymptotic to $\frac{c_{E,k}\sqrt{x}}{\log x}$ for each possible k in the Hasse bound. If the conjecture is correct, this would be true for $a_p = 1$ in particular, so all elliptic curves are $\frac{1}{2}$-nomalous. Assuming the GRH for the Dedekind zeta functions of the division fields of E, a result of Serre ([13]) gives us

$$\#\{p \leq x : p \nmid N, a_p = 1\} \ll_N \frac{x^{5/6}}{(\log x)^{1/3}},$$

where N is the conductor of E. A more recent paper of Murty, Murty, and Saradha that also assumes the GRH gives a better bound in [11], namely

$$\#\{p \leq x : p \nmid N, a_p = 1\} \ll_N \frac{x^{4/5}}{(\log x)^{1/5}},$$

Under this assumption, all elliptic curves are $\frac{1}{5}$-nomalous.

If E has nontrivial torsion over $\mathbb{Q}$, the torsion subgroup over $\mathbb{Q}$ can be injected into $E(\mathbb{F}_p)$ for primes of good reduction. Hence such an E can have at most one anomalous prime, so such a curve is 1-nomalous. The same is

true of any elliptic curve E which is $\mathbb{Q}$-isogenous to an elliptic curve E' which has nontrivial torsion or to an elliptic curve E'' for which $E''(\mathbb{Q}(\sqrt{\Delta_{E''}}))$ has nontrivial torsion, by remarks A9, A11 of Nathan Jones' appendix to [2]. Here, $\Delta_{E''}$ is the discriminant of E''.

If E is a CM elliptic curve, it has been shown [5] that the Lang–Trotter bound holds in this case, that is:

$$\#\{p < x : p \nmid N, a_p = 1\} \ll_N \sqrt{x}/\log x$$

where N is the conductor of E (only a finite number of primes divide N). Hence such a curve is $\frac{1}{2}$-nomalous.

Theorem 1.5. *Let E be a c-nomalous elliptic curve, $0 < c \leq 1$, P a nontorsion rational point on E. Then as $x \to \infty$,*

$$\#N(x) \leq \frac{x}{L(x)^{1/\sqrt{8}+o_P(1)}},$$

where $L(x) = \exp(\sqrt{\log x \log\log x})$.

2. Counting $N(x)$

Throughout we let the variable p denote a prime number.

Lemma 2.1. *For $y \geq 2$, $0 < \gamma \leq 1$, the estimates*

$$\#\{p : r_p \text{ exists and } r_p \leq y\} \ll y^3, \ \#\{p < x : r_p \text{ exists and } r_p \leq p^\gamma\} \ll x^{3\gamma}$$

hold, where the implied constants depend only on the elliptic curve E and the point P.

Proof. The first inequality implies the second, so we will only show the first. We will use Ward's definition of a divisibility sequence here. From Remark 28 of [14], our sequence $\{D_n\}$ is related to some $\{W_n\}$, which can be determined using the division polynomials of E. In particular, $D_n \mid W_n$. It is known that W_n grows like e^{cn^2} (see, e.g., Lemma 2 of [9]), where c depends on the point P used. It is easy to show that a number of size e^{cn^2} has at most $O_P(n^2)$ prime factors by comparing it to 2^{n^2}. Thus, each W_n has at most $O_P(n^2)$ prime factors. Summing, we see that at most $O(y^3)$ primes divide the first y terms of the division sequence, so only that many primes can have $r_p \leq y$. Since $D_n \mid W_n$, this bound holds for D_n as well. □

Lemma 2.2. *For a given choice of E and P, with p a prime, for any real $x \geq 1$, if $R(x,p)$ is the number of solutions of the congruence*

$$D_n \equiv 0 \pmod{p} \text{ with } 1 \leq n \leq x,$$

then

$$R(x,p) \leq \frac{x}{r_p}.$$

Proof. Lemma 4 in [14] states that $p \mid D_n$ if and only if $r_p \mid n$, which follows from the definitions of r_p. There are at most $\frac{x}{r_p}$ such integers n that are at most x. □

Lemma 2.3. *Let S be a set of primes with*

$$B(x) := \sum_{\substack{p \in S \\ p \le x \\ j \ge 1}} \frac{1}{p^j}.$$

Let $S_1(x)$ be the set of powers of primes in S (including the primes themselves) that are at most x, and assume $\#S_1(x) \le \frac{xf(x)}{(\log x)^c}$, where $c \ge 1$ and $f(x) > 0$ is a nondecreasing function. For all $x > 2$, let $S_\infty(x)$ be the set of $n \le x$ where all prime factors of n are elements of S. Then

$$\#S_\infty(x) \le e^{2^c B(x)} \frac{xf(x)}{(\log x)^c}.$$

Proof. Let $\omega(n)$ count the number of prime factors of n without repetition; define $S_k = \{n \in \mathbb{Z}^+ : \omega(n) = k,\ p \mid n \Rightarrow p \in S\}$; define $S_k(x) = \{n \le x : n \in S_k\}$. We will prove that $\#S_k(x) \le \frac{(2^c B(x))^{k-1} xf(x)}{(k-1)!(\log x)^c}$; this holds for $k = 1$. Assume it holds at k. Let $n \in S_{k+1}(x)$. Then n has $k+1$ prime powers as factors, at most one of which can be greater than $\sqrt{x}$. We will count $\#S_{k+1}(x)$ by counting these smaller factors. We have:

$$\begin{aligned}
\#S_{k+1}(x) &\le \frac{1}{k} \sum_{q \in S_1(\sqrt{x})} \#S_k(\frac{x}{q}) \\
&\le \frac{1}{k} \sum_{q \in S_1(\sqrt{x})} \frac{(2^c B(x))^{k-1}}{(k-1)!} \frac{(x/q) f(x/q)}{(\log(x/q))^c} \\
&\le \frac{1}{k} \frac{(2^c B(x))^{k-1}}{(k-1)!} \frac{2^c x f(x)}{(\log x)^c} \sum_{q \in S_1(\sqrt{x})} \frac{1}{q} \\
&\le \frac{(2^c B(x))^k}{k!} \frac{xf(x)}{(\log x)^c},
\end{aligned}$$

using the fact that f is an increasing function and the definition of $B(x)$. Summing over k, we get that $\#S_\infty(x) \le e^{2^c B(x)} \frac{xf(x)}{(\log x)^c}$. □

Theorem 2.4. *For $x \ge 20$, let $N(x) = N_{E,P}(x)$ be the set of integers $n \le x$ with $n \mid D_n$. Then the estimate*

$$\#N(x) \le O_{E,P}\left(\frac{x(\log\log x)^{5/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}\right)$$

holds.

Proof. We assume x is large. We will divide the set $N(x)$ into four subsets. Let $P(n)$ be the largest prime factor of n, and let $y = (\log x)^6$. Let

$$\begin{aligned}
N_1(x) :=& \{n \leq x : P(n) \leq y\} \\
N_2(x) :=& \big\{n \leq x : n \notin N_1(x), \text{ there exists a prime } p > y \text{ dividing } n \\
& \qquad \text{such that } \ r_p < p^{\frac{1}{4}}\big\} \\
N_3(x) :=& \{n \leq x : n \notin N_1(x), p \mid n \Rightarrow p \leq y \text{ or } p \text{ is anomalous}\} \\
N_4(x) :=& N(x) \setminus \bigcup_{i=1}^{3} N_i.
\end{aligned}$$

We will now bound the sizes of each of these sets.

For $N_1(x)$, we need the number of y-smooth numbers (n such that $P(n) \leq y$) less than x, $\psi(x, y)$. For our value of y, we can use $\psi(x, y) = x^{1-1/k+o(1)}$ as $x \to \infty$ when $y = (\log x)^k$ (Theorem 1 from [3]), so $\psi(x, y) \leq x^{5/6+o(1)}$ here. Hence $N_1(x) \leq x^{5/6+o(1)}$.

Now let $n \in N_2(x)$. Then $n = pm$, where $p > y$ is some prime with $r_p < p^{1/4}$. Note that any $p \mid D_1$ would be counted in this way; there are only finitely many such primes for any P. We know $p \leq \frac{x}{m}$, so $y \leq \frac{x}{m}$, and this implies that $m \leq \frac{x}{y}$. By Lemma 2.1, the number of such primes $p \leq x/m$ with $r_p < p^{1/4}$ is $O_P((x/m)^{3/4})$, where the implied constant depends on E and P. Summing over all possible values of $m \leq x/y$, we get

$$\begin{aligned}
\#N_2(x) &\ll_P \sum_{1 \leq m \leq x/y} \frac{x^{3/4}}{m^{3/4}} \leq x^{3/4} \sum_{1 \leq m \leq x/y} \frac{1}{m^{3/4}} \\
&\ll x^{3/4} \int_1^{x/y} \frac{dt}{t^{3/4}} \ \ll \frac{x}{\sqrt[4]{y}} = \frac{x}{(\log x)^{3/2}}.
\end{aligned}$$

Now let $n \in N_4(x)$. We may write $n = pm$, where $p > y$ is some nonanomalous prime dividing n with $r_p \geq p^{1/4}$ Such a prime exists because n is not contained in one of the other N_i. Because $n \in N(x)$, $p \mid n \mid D_n$, so by Lemma 4 of [14], $r_p \mid n$ as well. For p not an anomalous prime, $p \geq 7$, $\gcd(p, r_p) = 1$ because $r_p \mid \#E(\mathbb{F}_p)$, as mentioned previously. Therefore $pr_p \mid n$; there are at most $\frac{n}{pr_p}$ such numbers less than n for each p. We can count $\#N_4(x)$ by summing over p:

$$\begin{aligned}
\#N_4(x) &\leq \sum_{y \leq p \leq x} \frac{x}{pr_p} \leq \sum_{y \leq p \leq x} \frac{x}{p^{5/4}} \\
&\ll x \int_y^x \frac{dt}{t^{5/4}} \ \ll \frac{x}{\sqrt[4]{y}}.
\end{aligned}$$

This is the same magnitude as our bound for $\#N_2(x)$. In addition, this bound overestimates the number of n in this set since the integral is over all integers between y and x, not just the primes in this range.

All that remains to deal with is $N_3(x)$, the case involving anomalous primes. Recall that for this case, for each prime $p \mid n$, either $p < y$ or p is anomalous. A result of Serre's [13] shows that for E a non-CM curve (the bound is better if E has CM, addressed in the introduction), N the conductor of E,

$$\#\{p < x : p \nmid N, a_p = 1\} \ll_N \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}.$$

For a number n currently uncounted, let $n = m_1 m_2$, where m_1 is y-smooth and m_2 is composed entirely of anomalous primes. We divide these numbers into two cases, one where $m_1 \le x^{9/10}$, and one where $m_1 \ge x^{9/10}$. We will denote these counts by $A_1(x)$ and $A_2(x)$, respectively. Looking at nontrivial powers of anomalous primes, there are at most $\sqrt{x}\log x$ that are less than x, so the number of anomalous primes and powers of anomalous primes less than x is bounded by $O\left(\frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}\right)$ as well. Lemma 2.3 gives that

$$\#\{n \le x : n \text{ is the product of anomalous primes}\} \ll_E \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}$$

where the implied constant depends on the curve E as in Lemma 2.3 and on the conductor of E by Serre's result. Note that Serre's result implies that our $B(x)$ is $O(1)$ by partial summation.

Counting the first case, we have

$$\begin{aligned}
A_1(x) &\le \sum_{m_1 \le x^{9/10}} \sum_{m_2 \le \frac{x}{m_1}} 1 \\
&\ll_E \sum_{m_1 \le x^{9/10}} \frac{\frac{x}{m_1}(\log\log(x/m_1))^{2/3}(\log\log\log(x/m_1))^{1/3}}{(\log(x/m_1))^{4/3}} \\
&\ll \sum_{m_1 \le x^{9/10}} \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{m_1(\log x)^{4/3}} \\
&= \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}} \sum_{m_1 \le x^{9/10}} \frac{1}{m_1} \\
&\le \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}} \sum_{P(m) \le y} \frac{1}{m}.
\end{aligned}$$

Dealing with the latter sum separately, we see that

$$\sum_{P(m)\leq y}\frac{1}{m}=\prod_{p<y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\prod_{p<y}\left(1-\frac{1}{p}\right)^{-1}\sim e^{\gamma}\log y$$

by Mertens' Theorem. So

$$\begin{aligned}A_1(x)&\ll_E\frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}\log y}{(\log x)^{4/3}}\\&\ll\frac{x(\log\log x)^{5/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}.\end{aligned}$$

In the second case, we use the previously cited bound for the number of y-smooth numbers less than x, $\psi(x,y)$, here. We have

$$\begin{aligned}A_2(x)&\leq\sum_{m_1\geq x^{9/10}}\sum_{m_2\leq\frac{x}{m_1}}1\leq\sum_{m_2\leq x^{1/10}}\sum_{m_1\leq\frac{x}{m_2}}1\\&\leq\sum_{m_2\leq x^{1/10}}\psi(\frac{x}{m_2},y)\leq\sum_{m_2\leq x^{1/10}}\psi(x,y)\\&\leq\sum_{m_2\leq x^{1/10}}x^{5/6+o(1)}\leq x^{1/10}x^{5/6+o(1)}=x^{14/15+o(1)}\end{aligned}$$

as $x\to\infty$.

Hence $N_3(x)$ is the dominant case, with size bounded above by

$$\frac{x(\log\log x)^{5/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}.$$

This is our unconditional bound. □

3. Elliptic curves that are *c*-nomalous

In this section we prove Theorem 1.5. Recall Definition 1.4 of a c-nomalous elliptic curve.

Proof. We will use the same notation for the $N_i(x)$ as before, although now we will let $y=\exp(\sqrt{2\log x\log\log x})=L(x)^{\sqrt{2}}$, to minimize $N(x)$.

We will need a new bound for $\psi(x,y)$, namely $x\exp((-1+o(1))v\log v)$, which holds as long as we have $v=\frac{\log x}{\log y}$ going to infinity, with $y>(\log x)^2$ (see [4], for example). These bounds hold for our new choice of y, so we get as $x\to\infty$,

$$\begin{aligned}v\log v&=\frac{\log x}{\sqrt{2\log x\log\log x}}\log\frac{\log x}{\sqrt{2\log x\log\log x}}\\&=\sqrt{\frac{\log x}{2\log\log x}}\log\sqrt{\frac{\log x}{2\log\log x}}\end{aligned}$$

$$= \frac{1}{2}\sqrt{\frac{\log x}{2\log\log x}}(\log\log x - \log(2\log\log x))$$
$$= \left(\frac{1}{\sqrt{8}} + o(1)\right)\sqrt{\frac{\log x}{\log\log x}}(\log\log x)$$
$$= \left(\frac{1}{\sqrt{8}} + o(1)\right)\sqrt{\log x \log\log x}.$$

Plugging this in to our bound for $\psi(x, y)$, we get

$$\begin{aligned}\#N_1(x) &\leq x\exp((-1+o(1))v\log v)\\ &\leq x\exp\left(\left(\frac{-1}{\sqrt{8}} + o(1)\right)\sqrt{\log x\log\log x}\right)\\ &= \frac{x}{L(x)^{1/\sqrt{8}+o(1)}}.\end{aligned}$$

Using the derivation of our bound for $\#N_2(x)$ in Theorem 2.4 with our new value of y, we see that

$$\#N_2(x) \ll_P \frac{x}{\sqrt[4]{y}} = \frac{x}{L(x)^{1/\sqrt{8}}}.$$

Similarly, $\#N_4(x)$ is also bounded above by $O\big(\frac{x}{\sqrt[4]{y}}\big)$ using its previous derivation in Theorem 2.4, so it too does not significantly contribute to the size of $N(x)$.

We will now show that under the c-nomalous condition, the contribution from $N_3(x)$ is within our bound for the size of $N(x)$. For each $n \in N_3(x)$, as in the proof of Theorem 2.4 let $n = m_1m_2$, where m_1 is y-smooth and m_2 is composed entirely of anomalous primes p with $p > y$. We will divide these n into three subcases: one where $m_2 \leq y^{1/c^2}$, one where m_2 is divisible by a prime of size at least $y^{1/c}$, and one where $m_2 > y^{1/c^2}$ and is composed entirely of primes of size at most $y^{1/c}$. Call the counts in these cases $A_1(x)$, $A_2(x)$, and $A_3(x)$, respectively. We will use the S_∞ notation from Lemma 2.3 to denote the set $\{n \leq x : p \mid n \Rightarrow p > y, p \text{ is anomalous}\}$.

For the first case, we can bound the number of such n by looking at the y-smooth portions. Note that m_2 can have at most $\frac{1}{c^2}$ prime factors, since each anomalous prime is at least y. We have, as $x \to \infty$,

$$\begin{aligned}A_1(x) &\leq \sum_{\substack{k\leq y^{1/c^2}\\ k\in S_\infty}} \psi\left(\frac{x}{k}, y\right) \leq \sum_{\substack{k\leq y^{1/c^2}\\ k\in S_\infty}} \frac{x/k}{L(x/k)^{1/\sqrt{8}+o(1)}}\\ &\leq \sum_{\substack{k\leq y^{1/c^2}\\ k\in S_\infty}} \frac{x}{kL(x)^{1/\sqrt{8}+o(1)}} = \frac{x}{L(x)^{1/\sqrt{8}+o(1)}} \sum_{\substack{k\leq y^{1/c^2}\\ k\in S_\infty}} \frac{1}{k}\end{aligned}$$

$$\leq \frac{x}{L(x)^{1/\sqrt{8}+o(1)}} \sum_{j \leq 1/c^2} \frac{1}{j!} \left(1 + \sum_{\substack{p \leq y^{1/c^2} \\ p \text{ anomalous}}} \frac{1}{p-1} \right)^j$$

$$\leq \frac{x}{L(x)^{1/\sqrt{8}+o(1)}} \left(1 + \sum_{\substack{p \leq y^{1/c^2} \\ p \text{ anomalous}}} \frac{1}{p-1} \right)^{1/c^2}.$$

We use a multinomial identity to change from a sum over k to one over j and p. This expression involving a sum on anomalous p is $O_c(1)$ since we sum only over anomalous primes, so $A_1(x)$ is at most the same size as our bound for $\#N_2(x)$.

We now find the size of $A_2(x)$ using partial summation:

$$A_2(x) \leq \sum_{\substack{y^{1/c} \leq p \leq x \\ p \text{ anomalous}}} \frac{x}{p} \ll x \left[\frac{1}{x}(x^{1-c}) + \int_{y^{1/c}}^{x} \frac{1}{t^2} t^{1-c}\, dt \right]$$

$$= x^{1-c} + x \int_{y^{1/c}}^{x} \frac{1}{t^{1+c}}\, dt \leq \frac{x}{cy} \ll \frac{x}{L(x)^{\sqrt{2}}}.$$

Thus the contribution of $A_2(x)$ is negligible.

We will now find the size of $A_3(x)$. Note that since each factor of m_2 is at most $y^{1/c}$, m_2 has at least $k = \lfloor \frac{1}{c} \rfloor$ prime factors (with multiplicity). Suppose m is composed of k anomalous primes in $(y, y^{1/c}]$. Then

$$A_3(x) \leq x \sum_{m \leq x} \frac{1}{m} \leq x \left(\sum_{\substack{y < p \leq y^{1/c} \\ p \text{ anomalous}}} \frac{1}{p} \right)^k.$$

Dealing with the reciprocal sum of these anomalous primes separately,

$$\sum_{\substack{y \leq p \leq y^{1/c} \\ p \text{ anomalous}}} \frac{1}{p} \leq \sum_{\substack{p \geq y \\ p \text{ anomalous}}} \frac{1}{p} \ll \int_{y}^{\infty} \frac{1}{t^2} t^{1-c}\, dt = \int_{y}^{\infty} \frac{1}{t^{1+c}}\, dt \ll \frac{1}{y^c}.$$

Raising this to the kth power, we see that our reciprocal sum of large anomalous primes to the kth power is $O\big(\frac{1}{y}\big)$. Thus, $A_3(x) = O\big(\frac{x}{y}\big) = O\big(\frac{x}{L(x)^{\sqrt{2}}}\big)$, which is negligible compared to the other cases.

Hence for c-nomalous curves, $\#N(x) \leq \frac{x}{L(x)^{1/\sqrt{8}+o_P(1)}}$, as $x \to \infty$. $\square$

Acknowledgements. We thank Carl Pomerance for his help with various calculations, as well as an anonymous referee for their helpful comments.

References

[1] André-Jeannin, Richard. Divisibility of generalized Fibonacci and Lucas numbers by their subscripts. *Fibonacci Quart.* **29** (1991), no. 4, 364–366. MR1131414 (92i:11018), Zbl 0737.11003.

[2] Bandman, Tatiana; Grunewald, Fritz; Kunyavskiĭ, Boris. Geometry and arithmetic of verbal dynamical systems on simple groups. With an appendix by Nathan Jones. *Groups Geom. Dyn.* **4** (2010), no. 4, 607–655. MR2727656 (2011k:14020), Zbl pre05880956, arXiv:0809.0369v2.

[3] de Bruijn, N. G. On the number of positive integers $\leq x$ and free of prime factors $\geq y$, II. *Nederl. Akad. Wetensch. Proc. Ser. A. Indag. Math.* **28** (1966), 239–247. MR0205945 (34 #5770), Zbl 0139.27203.

[4] Canfield, E. R.; Erdős, Paul; Pomerance, Carl. On a problem of Oppenheim concerning "factorisatio numerorum". *J. Number Theory* **17** (1983), no. 1, 1–28. MR0712964 (85j:11012), Zbl 0513.10043.

[5] Cojocaru, Alina Carmen. Questions about the reductions modulo primes of an elliptic curve. *Number theory*, 61–79. CRM Proceedings and Lecture Notes, 36. *Amer. Math. Soc., Providence, RI*, 2004. MR2076566 (2005i:11075), Zbl 1085.11030.

[6] Cornelissen, Gunther; Zahidi, Karim. Elliptic divisibility sequences and undecidable problems about rational points. *J. Reine Angew. Math.* **613** (2007), 1–33. MR2377127 (2009h:11196), Zbl 1178.11076, arXiv:math/0412473.

[7] Eisenträger, Kirsten; Everest, Graham. Descent on elliptic curves and Hilbert's tenth problem. *Proc. Amer. Math. Soc.* **137** (2009), no. 6, 1951–1959. MR2480276 (2009k:11201), Zbl pre05558381, arXiv:0707.1485v5.

[8] González, J. J. Alba; Luca, Florian; Pomerance, Carl; Shparlinski, Igor E. On numbers n dividing the nth term of a linear recurrence. *Proc. Edinburgh Math. Soc. (Series 2)* **55** (2012), 271–289. doi: 10.1017/S0013091510001355.

[9] Gordon, Daniel; Pomerance, Carl . The distribution of Lucas and elliptic pseudoprimes. *Math. Comp.* **57** (1991), no. 196, 825–838. MR1094951 (92h:11081), Zbl 0744.11066.

[10] Mazur, Barry. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972), 183–266. MR0444670 (56 #3020), Zbl 0245.14015.

[11] Murty, M. Ram; Murty, V. Kumar; Saradha, N. Modular forms and the Chebotarev density theorem. *Amer. J. Math.* **110** (1988), no. 2, 253–281. MR0935007 (89d:11036), Zbl 0644.10018.

[12] Poonen, Bjorn. Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *J. Amer. Math. Soc.* **16** (2003), no. 4, 981–990 (electronic). MR1992832 (2004f:11145), Zbl 1028.11077, arXiv:math/0306277v1.

[13] Serre, Jean-Pierre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR0644559 (83k:12011), Zbl 0496.12011.

[14] Silverman, Joseph H.; Stange, Katherine E. Terms in elliptic divisibility sequences divisible by their indices. *Acta Arith.* **146** (2011), no. 4, 355–378. MR2747036 (2012c:11126), Zbl 1225.11079, arXiv:1001.5303v1.

[15] Smyth, Chris. The terms in Lucas sequences divisible by their indices. *J. Integer Sequences* **13** (2010), Article 10.2.4, 18 pp. MR2592551 (2011a:11036), Zbl 1210.11025, arXiv:0908.3832v1.

[16] Somer, Lawrence. Divisibility of terms in Lucas sequences by their subscripts. *Applications of Fibonacci numbers, Vol. 5* (St. Andrews, 1992), 515–525. *Kluwer Acad. Publ., Dordrecht*, 1993. MR1271392 (94m:11022), Zbl 0806.11013.

[17] Stange, Katherine E. The Tate pairing via elliptic nets. *Pairing-based cryptography — Pairing 2007*, 329–348. Lecture Notes in Comput. Sci., 4575. *Springer, Berlin*, 2007. MR2423649 (2009e:11233), Zbl 1151.94570.

[18] Ward, Morgan. The law of repetition of primes in an elliptic divisibility sequence. *Duke Math. J.* **15** (1948), 941–946. MR0027286 (10,283e), Zbl 0032.01403.

[19] Ward, Morgan. Memoir on elliptic divisibility sequences. *Amer. J. Math.* **70** (1948), 31–74. MR0023275 (9,332j), Zbl 0035.03702.

Department of Mathematics, Dartmouth College, Hanover, NH 03755
avram.m.gottschlich@dartmouth.edu
http://www.math.dartmouth.edu/~avram/

This paper is available via http://nyjm.albany.edu/j/2012/18-23.html.