London Mathematical Society ISSN 1461–1570

PRIMES IN ELLIPTIC DIVISIBILITY SEQUENCES

MANFRED EINSIEDLER, GRAHAM EVEREST AND THOMAS WARD

Abstract

Morgan Ward pursued the study of elliptic divisibility sequences, originally initiated by Lucas, and Chudnovsky and Chudnovsky subsequently suggested looking at elliptic divisibility sequences for prime appearance. The problem of prime appearance in these sequences is examined here, from both a theoretical and a practical viewpoint. We show calculations, together with a heuristic argument, to suggest that these sequences contain only finitely many primes.

1. *Introduction*

For $0 \leqslant n \in \mathbb{N}$, let u_n denote the nth term in an integral divisibility sequence (u_n). This means that each u_n is an integer, and that

$$m \mid n \text{ implies that } u_m \mid u_n. \tag{1}$$

The oldest non-trivial example of a divisibility sequence is probably the Fibonacci sequence. Other examples are the Mersenne sequence, $M_n = 2^n - 1$, and the generalized Mersenne sequences studied by Pierce and Lehmer (see [8, 11, 13]). All of these sequences satisfy a linear recurrence relation. Bézivin, Pethö and van der Poorten have characterized all such sequences in [1]. An important class of divisibility sequences satisfies a non-linear recurrence relation: these are the *elliptic divisibility sequences*, so named by Morgan Ward, and first studied by Lucas.

Definition 1. An integral divisibility sequence (u_n) is an *elliptic divisibility sequence* if, for all $m \geqslant n \geqslant 1$, it satisfies the recurrence relation

$$u_{m+n}u_{m-n} = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2. \tag{2}$$

The same recurrence relation is satisfied by the elliptic division polynomials associated to an elliptic curve. Morgan Ward wrote several papers detailing the arithmetic theory of elliptic divisibility sequences, starting with [20]. Recently, Shipsey [15] has used elliptic divisibility sequences to study the discrete logarithm problem for elliptic curves over finite fields. She has found an elegant algorithm for computing high-order values, using a kind of repeated doubling.

The question of prime appearance in divisibility sequences has received much attention when the sequence satisfies a linear recurrence relation. It seems plausible that such sequences will contain infinitely many primes after taking account of any generic divisibility. For example, reciprocal Lehmer–Pierce sequences are all squares, and have all terms divisible by the first. The result of [1] allows one to characterize precisely when there will be generic divisibility.

The first author acknowledges the support of EPSRC postdoctoral award GR/M49588.
Received 8 September 2000, revised 29 December 2000*; published 5 February 2001*.
2000 Mathematics Subject Classification 11Y11, 11G07

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

One other kind of generic divisibility can occur, as evidenced by the sequence $4^n - 1$: for $n > 1$, the terms will have non-trivial factors $2^n + 1$ and $2^n - 1$. Essentially the same kind of argument explains Ribenboim's example in [**14**, p. 64]. He points out that the Lucas sequence $0, 1, 3, 8, 21, 55, \ldots$ (the even terms of the Fibonacci sequence) has only one prime term. This kind of generic divisibility occurs in elliptic divisibility sequences also, as detailed in Proposition 7.

So far, there is a shortage of proofs for prime appearance in linear recurrence sequences, but there are some heuristic arguments and some compelling data. See [**18**] for heuristic arguments concerning the Mersenne sequence, and [**5**] for recent work on other classical sequences. The heuristics agree with the data, although there is not a lot of data for the Mersenne sequence, only 38 Mersenne primes being known. In [**8**] we provide a large amount of data for related sequences, first defined by Pierce and Lehmer, which generalize the Mersenne sequence.

Although Morgan Ward wrote many papers about elliptic divisibility sequences, including one on repetition of prime factors [**19**], he did not touch on the question of prime appearance. In [**3**] and [**4**], the Chudnovskys consider this question, and they make the suggestion that elliptic divisibility sequences should contain very large primes. In this paper, we are going to argue, from heuristics and from calculations, that an elliptic divisibility sequence should contain only finitely many primes. In their paper, the Chudnovskys also note that some of the sequences that they consider are highly divisible by small primes. We showed in [**6**] how this is a manifestation of singular reduction on the underlying elliptic curve. The sequence which arises as the division sequence associated to a rational point on an elliptic curve (see equation (6)) is trying to tell us all the local heights for that point, and the high divisibility is accounted for by singular reduction at the dividing primes. After appropriately dividing out by these primes, we obtain a new sequence, which can be tested for primality.

2. *Elliptic divisibility sequences*

The recurrence relation (2) is less straightforward than a linear recurrence. In order to calculate terms, notice firstly that the single relation (2) gives rise to two relations

$$u_{2n+1} = u_{n+2}u_n^3 - u_{n-1}u_{n+1}^3 \tag{3}$$

and

$$u_{2n}u_2 = u_{n+2}u_n u_{n-1}^2 - u_n u_{n-2} u_{n+1}^2. \tag{4}$$

The relation (3) comes about by setting $m = n + 1$, whilst relation (4) comes about by setting $m = n + 2$ and then replacing n by $n - 1$. The relations (3) and (4) can then be subsumed into the single relation

$$u_n u_{\lfloor n/\lfloor (n+1)/2 \rfloor \rfloor} = u_{\lfloor (n+4)/2 \rfloor} u_{\lfloor n/2 \rfloor} u^2_{\lfloor (n-1)/2 \rfloor} - u_{\lfloor (n+1)/2 \rfloor} u_{\lfloor (n-3)/2 \rfloor} u^2_{\lfloor (n+2)/2 \rfloor},$$

where '$\lfloor \cdot \rfloor$' denotes, as usual, the integer part. Following Morgan Ward, say that a solution $u = (u_n)_{n \geqslant 0}$ of condition (2) is *proper* if $u_0 = 0$, $u_1 = 1$, and $u_2 u_3 \neq 0$. Such a proper solution will be an elliptic divisibility sequence if and only if u_2, u_3 and u_4 are integers with $u_2 \mid u_4$, and relations (3) and (4) are satisfied for all n. Hence the terms u_i, for $0 \leqslant i \leqslant 4$, uniquely determine an elliptic divisibility sequence.

This last remark forms the basis for one of the approaches taken by the Chudnovskys: specify the first five terms, and then consider the resulting sequence. There are problems with this approach. Firstly, there are elliptic divisibility sequences that satisfy a linear recurrence relation. Examples of these include the integers $u_n = n$ and the sequence $0, 1, -1, 0, 1 \ldots$ of Legendre symbols $u_n = (n/3)$. Our interest lies with sequences that do not satisfy a linear recurrence. Secondly, it is difficult to guess at the growth rate for an elliptic divisibility sequence when you see only the first five terms, and rapidly growing sequences become problematical when it comes to checking terms for primality. Finally, there is a subtle problem, which the Chudnovskys observed: in certain instances, all of the terms can be divisible by very high powers of small primes. Theorem 4 below gives an explanation for this in terms of the arithmetic of the underlying elliptic curves.

The other approach taken by the Chudnovskys is better suited to our purpose. All the examples of elliptic divisibility sequences that are non-linear arise from elliptic division polynomials, analogues of the classical cyclotomic polynomials from arithmetic. We shall now give a short account of this material. All of the theory of elliptic curves needed here can be found in Silverman's volumes [**16**] and [**17**].

Consider an elliptic curve defined over the rational numbers, determined by a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5}$$

with coefficients $a_1, \ldots, a_6$ in $\mathbb{Z}$.

Definition 2. With the notation of equation (5), let

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}$$

Define a sequence of polynomials in $\mathbb{Z}[x, y]$ as follows:

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4 &= \psi_2\big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2\big).
\end{aligned}$$

Now define inductively, for $n \geqslant 2$,

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$$

and

$$\psi_{2n}\psi_2 = \psi_n\big(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\big).$$

It is straightforward to check that each $\psi_n \in \mathbb{Z}[x, y]$. Write $\psi_n(Q)$ for ψ_n evaluated at the point $Q = (x, y)$. The basic properties of elliptic division polynomials can be found in [**16**], [**17**] and [**20**].

Proposition 3. *The sequence* (ψ_n) *satisfies the recurrence* (2)*. Also,*

$$\psi_n^2(Q) = n^2x^{n^2-1} + \ldots \quad \in \mathbb{Z}[x]$$

is a primitive integral polynomial in x alone, whose roots are the x-coordinates of the finite torsion points on the curve whose order divides n.

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

The proposition guarantees that the evaluated sequence $(\psi_n(Q))$ satisfies condition (2) for any integral point Q. It is readily checked that if (u_n) is any rational sequence that satisfies equation (2) and c is a non-zero rational, then $v_n = c^{n^2-1}u_n$ also satisfies condition (2). Given any rational point Q, the shape of the equation (5) guarantees that the denominator of the x-coordinate is a square, say $x(Q) = a/b^2$. Thus, from the point Q and the curve, we can produce the terms of an elliptic divisibility sequence $b^{n^2-1}\psi_n(Q)$ by clearing the denominator. Define the sequence $(E_n) = (E_n(Q))$ by

$$E_n = b^{n^2-1}\psi_n(Q) \quad \in \mathbb{Z}. \tag{6}$$

In [3], the Chudnovskys suggested looking at elliptic divisibility sequences for prime appearance. In one approach, they specified the first five terms, and then examined the first 100 terms of the resulting sequence. These did indeed exhibit some primes, and some of them are quite large. The largest prime that they found has 469 decimal digits: it appears in the third sequence from the end in Table 1.

Our heuristics predict that any given sequence should contain only finitely many primes. We ran the Chudnovskys' sequences to the first 500 terms, and in every case found no new primes. In their other approach, they specified an elliptic curve and a non-torsion integral point Q, and examined the terms of the resulting division sequence for primality. Below, we shall explain how good choices for the curve and the point may be made. We did this for many curves and points, and again our calculations suggest that a given sequence will contain only a finite number of primes. In Section 3 of the paper, we present a heuristic argument to explain why we should expect only finitely many primes. The key to our approach is contained in Theorem 4 below, which was proved in [7] (see also [9]).

To every prime p, associate the p-adic valuation in the usual way, and associate the Archimedean valuation to the 'prime' infinity. Recall that any rational point has a canonical global height $\hat{h}(Q)$. This global height is non-negative, and vanishes if and only if Q is a torsion point. It has the functoriality property that $\hat{h}(kQ) = k^2\hat{h}(Q)$ for every rational point Q and every $k \in \mathbb{Z}$. Moreover, the global height is a sum of canonical local heights, one for each prime:

$$\hat{h}(Q) = \sum_{p \leqslant \infty} \lambda_p(Q). \tag{7}$$

The canonical local heights can be given by explicit formulæ. For finite primes, these involve only the discriminant Δ of the curve (see equation (8) below), the coordinates of Q, and $\psi_2(Q)$ or $\psi_3(Q)$; see Exercises 6.7 and 6.8 in [17]. Usually, local canonical heights are defined up to a constant, and then normalized to make them isomorphism-invariant. In this paper, we shall always use non-normalized local heights.

Write

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{8}$$

for the discriminant of the curve (5). Primes p that divide Δ are precisely the primes for which the elliptic curve reduces to a singular curve mod p. Normalized local heights contain a factor $(1/12)\log|\Delta|_p$ to make them isomorphism-invariant; it is important to stress that the local heights represented in Theorem 4 are not normalized to make them isomorphism-invariant. Of course, the sum of the local heights is always the global height, whether the local heights are normalized or not.

The theorem that follows was proved in [7]; it relates the non-normalized heights directly to elliptic divisibility sequences. A more general version, together with numerical examples, appears in [9].

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

Theorem 4. *Assume that equation (5) is in global minimal form. Let Q denote a non-torsion rational point on the curve. Then for $p = \infty$ or a finite prime of singular reduction, there are positive constants A and B, with $B < 2$, for which*

$$1/n^2 \log|\psi_n(Q)|_p = \lambda_p(Q) + \begin{cases} O\left((\log n)^A/n^2\right) & \text{if } p = \infty, \\ O\left(1/n^B\right) & \text{if } p < \infty. \end{cases} \tag{9}$$

The constant A depends upon the curve and the point Q only, whilst B depends upon the curve, the point Q and the prime p. The method of proof uses elliptic transcendence theory. It is a surprising feature of the underlying bounds in elliptic transcendence theory that the bound for the finite primes is inferior to that for the infinite prime.

For a prime of singular reduction (or for $p = \infty$), the canonical local height of a rational point can be negative. It follows from equation (9) that if p is a prime of singular reduction for the curve, and the canonical local height of Q at that prime is negative, then $E_n = E_n(Q)$ must ultimately be divisible by very high powers of p. Thus, Theorem 4 explains the examples of sequences (E_n), which the Chudnovskys discovered, where all the terms E_n are divisible by certain primes. Of course, sequences with this property will yield very few prime values. Rather than ignore such sequences, however, one can divide out the singular primes from each term of E_n by writing

$$F_n = |E_n| \prod_{p|\Delta} |E_n|_p. \tag{10}$$

We feel that the sequence (F_n) still deserves to be called 'an elliptic divisibility sequence' even though it might not satisfy condition (2). Note that one could also consider removing the prime divisors belonging to an arbitrary finite set of primes that contains the divisors of Δ. Based on our results here, we believe that the resulting sequence would still be prime only finitely often.

The next result also comes from [7].

Theorem 5. *If Q is a rational point with $x(Q) = a/b^2$, and F_n is defined as in equation (10), then*

$$F_n = \hat{H}(Q)^{n^2 + O(n^{2-C})}, \tag{11}$$

where $\log \hat{H}(Q) = \hat{h}(Q)$, and $0 < C < 2$ is a constant.

The asymptotic formula (11) is important because we can use it to restrict our search for primes. A prime of the form $F_n = F_n(Q)$ is an *anomalous prime* if the index n is not a prime.

Proposition 6. *There can be only finitely many anomalous primes in the sequence (F_n).*

Proof. Since (F_n) is a divisibility sequence with $F_n > 1$ for all large n, the only way in which large anomalous primes can appear is if they are of the form $F_{mn} = F_n$ with $1 < m, n$. If there are infinitely many anomalous primes, then this relation will hold with $mn \to \infty$. Then equation (11) implies that

$$n^2 = (mn)^2 + o\left((mn)^2\right),$$

which is clearly impossible. □

Another important application of equation (11) is as follows. For a non-torsion rational point Q, compare $F_n(Q)$ with $F_n(kQ)$ when $1 < k \in \mathbb{N}$. We know that $\hat{h}(kQ) = k^2\hat{h}(Q)$.

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

It follows from equation (11) that the terms of the sequence $(F_n(kQ))$ are all larger than those in the sequence $(F_n(Q))$ from some point onwards. Proposition 7 below shows that for prime $n > k$, $F_n(Q) \mid F_n(kQ)$. Since only finitely many terms of $F_n(Q)$ are equal to 1, this means that, from some point, every term $F_n(kQ)$ has a non-trivial factor, and therefore that only finitely many terms of $F_n(kQ)$ are primes. This is an elliptic analogue of the generic divisibility dicussed in Section 1.

Proposition 7. *Suppose that Q is a non-torsion rational point, and that $1 \leqslant k \in \mathbb{N}$ is fixed. Then, for all primes $n > k$,*

$$F_n(Q) \mid F_n(kQ).$$

Proof. Let K_n denote the algebraic number field obtained by adjoining to $\mathbb{Q}$ all the x-coordinates of the n-torsion points. Suppose that p is a prime of non-singular reduction, and that $p \mid F_n(Q)$. Let P denote a prime ideal above p in K_n. From Proposition 3, we know that

$$E_n^2 = n^2 \prod_{T:nT=O} \left|b^2T - a\right|. \tag{12}$$

Suppose that we have a relation $P^i \mid b^2T - a$, for some n-torsion point T and some $i \geqslant 1$. Clearly, $(p, b) = 1$, and it follows that $x(Q) \equiv x(T) \bmod P^i$. If p is a prime of non-singular reduction, we can find $kQ \bmod P^i$. Also, $(n, k) = 1$, so kT must be a finite point, and we have $x(kQ) \equiv x(kT) \bmod P^i$. Thus P^i certainly appears in some factor of $F_n(kQ)$ because kT is also an n-torsion point. The map $T \mapsto kT$ permutes the n-torsion points when $(n, k) = 1$. Thus, every factor of $F_n(Q)$ that is divisible by P^i yields a distinct factor of $F_n(kQ)$ that is divisible by P^i. Since this is true for all $P \mid p$ in K_n, we deduce that every power of p in $F_n(Q)$ appears also in $F_n(kQ)$. □

In summary, in order to find primes, we start with non-torsion rational points which are of small height and, preferably, which are not multiples of other rational points. One expects small-height points to be integral, so we confined our search to those. In practice, a point that is found to be of small height is unlikely to be a multiple of any other point. For definiteness, we began with the point $Q = (0, 0)$ on the curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x. \tag{13}$$

By applying isomorphisms of the form $y \mapsto y + mx$, a_1 may be taken to be 0 or 1 without loss of generality. All curves with the other coefficients in the range -100 to 100 were searched to find the canonical global height of Q on each curve. Of course, these curves are not necessarily in global minimal form, so they were changed to that form (which leaves the global height invariant). The resulting sequences (F_n) were tested for prime appearance for a selection of curves. The results are summarized in Table 2. The calculations were performed using GP-Pari, see [**12**]. Note that 'a prime' in this context means 'a probable prime', in the sense that it is a pseudo-prime to ten randomly chosen bases. There now follows a heuristic argument that suggests that only finitely many terms of (F_n) should be primes.

3. *Heuristics on prime appearance*

The essence of what follows may be summarized in the following way. Since $\log F_n$ is quadratic in n, the prime number theorem predicts that only a finite number of the F_n will

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

be prime (if they behave randomly). This contrasts with, say, the terms of the Mersenne sequence, whose logarithms grow linearly in n.

Wagstaff gave a heuristic argument for the appearance of primes in the Mersenne sequence [18]. Roughly speaking, the prime number theorem implies that the probability that a large integer N is prime is $1/\log N$. The Euler–Fermat theorem implies that if n is prime, then any prime divisor q of $2^n - 1$ is forced to be greater than $2n$. Thus, the probability that $2^n - 1$ is prime needs to be adjusted by Euler factors for primes less than $2n$. We may expect

$$\sum_{\text{prime } n<x} 1/\log(2^n - 1) \prod_{q<2n} \left(1 - \tfrac{1}{q}\right)^{-1} \tag{14}$$

Mersenne primes $2^n - 1$ with $n < x$. Using Merten's theorem, the expression in (14) is asymptotically $\rho \log x$, where $\rho = e^{\gamma}/\log 2$, and γ denotes Euler's constant. This rough argument does actually fit the data, although it should be added that only 38 Mersenne primes are known. On the other hand, this kind of argument can be extended to provide a reasonably satisfactory explanation (see [8]) of prime appearance in the Lehmer–Pierce sequences which generalize the Mersenne sequence. The Lehmer–Pierce sequences provide much more data against which to compare the heuristic argument.

Clearly, the growth rate of the underlying sequence plays a key role in the argument. Hardy and Wright [10, footnote to p. 15] argued somewhat earlier that this kind of reasoning gives a heuristic explanation for the conjectured finiteness of the number of primes in the Fermat sequence defined by $a_n = 2^{2^n} + 1$. Once again, the large growth rate of this sequence means a paucity of data against which to test such hypotheses. This is behind the Chudnovskys' suggestion that small-height rational points on elliptic curves would provide more data against which to test hypotheses of prime appearance.

Using Hasse's theorem, we can give a kind of elliptic analogue of the approach of Wagstaff. If q is a non-singular prime which divides F_n, then it follows that nQ must reduce to the point at infinity on the reduced curve mod q. If n is prime, it follows that the order of the group of $\mathbb{F}_q$-points on this curve must be bounded below by n. By Hasse's theorem, the order of this group is $q + O(\sqrt{q})$ uniformly. Inverting this inequality gives an upper bound for q of the form $n + O(\sqrt{n})$ uniformly. Thus, in the elliptic analogue of estimate (14), we adjust by the Euler factors for non-singular primes q bounded by $n + O(\sqrt{n})$. We should also include the Euler factors for the singular primes, but for a different reason. The construction of F_n guarantees that each term is free of singular primes, so the probability that F_n is prime must be adjusted by these Euler factors, just as it is for each of the non-singular primes. This gives the following estimate for the number of prime values of F_n with prime $n < x$:

$$\sum_{\text{prime } n<x} 1/\log F_n \prod_{q<n+O(\sqrt{n})} \left(1 - \tfrac{1}{q}\right)^{-1}. \tag{15}$$

Merten's theorem and the quadratic growth rate of $\log F_n$ shows that the expression in (15) converges. This suggests that, for any large x, the number of prime indices $n < x$ for which F_n is prime is constant. In other words, there should be a finite number of non-anomalous primes. In Proposition 6 we showed there can be only a finite number of anomalous primes also. This argument may be slightly refined, using the known uniform constant in Hasse's theorem (see [2, Theorem 8.3]). This changes estimate (15) to the following: the expected number of non-anomalous primes in the sequence (F_n) is bounded above by

$$\sum_{\text{prime n}<\infty} 1/\log F_n \prod_{q<n+1+2\sqrt{n}} \left(1 - \tfrac{1}{q}\right)^{-1} \sim 1.9/\hat{h}(Q).$$

Note that an exact calculation was made, to avoid using Merten's theorem in this context, since the error term in estimating the product would swamp the other terms. There does not seem to be a reasonable heuristic for a lower bound, since the early terms (small values of the prime n) dominate the sum, so asymptotic estimates are inappropriate.

The elliptic analogue of the Lehmer problem suggests that the canonical height of a non-torsion rational point should be uniformly bounded below. Combining this with our heuristics suggests that the number of primes appearing should be uniformly bounded above. A more refined conjecture of Lang suggests that the height is bounded below by $c \log |\Delta|$. This suggests that the number of primes should decrease as the discriminant increases. The experimental evidence suggests that the constant c must be very small; known points of small height are used in [**16**] to give an upper bound of around 10^{-4} for c. Thus we cannot use this conjecture to give a reasonable upper bound for the number of primes appearing in an elliptic divisibility sequence in terms of the discriminant.

4. *Computational evidence*

The heuristics in Section 3 suggest two things. Firstly, a sequence $(F_n(Q))$ of the form (10) is expected to be eventually composite. Secondly, the number of non-anomalous primes in the sequence is expected to be less than $1.9/\hat{h}(Q)$. For a selection of points on curves found with canonical heights in the range 0.01 to 0.1, the sequence (F_n) was tested for primality for $n \leqslant 600$. The selection was made by simply choosing some curves from a short list, so as to provide a reasonable cover of the range of heights.

There are major impediments to such experiments. On the practical side, there are very few points with small height, and the quadratic growth of $\log F_n$ means that primality testing had to be carried out on many thousands of numbers with logarithms in the range 3,000 to 30,000. On the theoretical side, the fact that the curve and the point both vary means that even the most optimistic heuristic argument leaves one expecting the experimental data to lie on many different lines. Also, it is in the nature of these sequences not to have small prime factors; therefore, proving that late terms of the sequence are composite is a slower process than would be the case for a 'typical' number of comparable size.

An additional test was made of the basic heuristic (that the number of primes is finite) by testing each of the elliptic divisibility sequences considered in [**3**] out to index 500. In each case, no additional primes were found beyond those found by the Chudnovskys in their search to index 100. These results are presented in Table 1, where the first five terms of the sequence satisfying condition (2) are given, followed by the observed growth rate, and finally the prime values of n for which the sequence was found to be prime. Note that in every example, the sequence comes from an integral point on an elliptic curve that reduces to a non-singular point for every prime p. Thus the growth rate that is shown is an approximation to the global canonical height of that point, which is entirely concentrated at the infinite prime.

The other results are presented in two forms. Table 2 records the curve (in the form used by GP-Pari), the point Q, the canonical height $\hat{h}(Q)$, the number $N(Q)$ of non-anomalous primes found for $n \leqslant 600$, the logarithmic error size $e(Q) = \log_{10} \epsilon_{600}(Q)$ from equation (16), and the set S of singular primes for the curve. The only exception is the first entry in Table 2, where the prime search was carried out for $n \leqslant 1500$; this is indicated with an asterisk on the value of $N(Q)$. For this curve, a prime was found at $n = 739$. The format for elliptic curves used by GP-Pari means that the vector $[a_1, a_2, a_3, a_4, a_6]$ corresponds to the curve in (global minimal) Weierstrass form (5).

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

Table 1: Elliptic divisibility sequences from the paper [3] of Chudnovsky and Chudnovsky.

Initial terms	Growth rate	Prime incidence up to $n = 500$
$0, 1, 1, 1, -2$	0.0560	5, 7, 11, 13, 23, 61, 71
$0, 1, 1, 1, 6$	0.1107	5, 7, 13, 23, 43, 47
$0, 1, 2, 1, 4$	0.1262	5, 7, 71
$0, 1, 1, 2, 7$	0.1311	11, 17, 73
$0, 1, 1, 1, -9$	0.1383	7, 47, 79
$0, 1, 1, 1, 10$	0.1432	7, 13, 41, 61
$0, 1, 1, 4, 1$	0.1730	71, 79
$0, 1, 1, 4, 3$	0.1737	5, 7, 13, 53, 71
$0, 1, 1, 5, 2$	0.2010	7, 43

Write

$$\epsilon_n(Q) = \left| \frac{1}{n^2} \log F_n(Q) - \hat{h}(Q) \right|. \tag{16}$$

One might have thought that the constants in equation (9) could be so large as to make $(1/n^2) \log F_n(Q)$ an unreliable estimate for $\hat{h}(Q)$, except for very large n. However $\epsilon_n(Q)$ seems to be approximately $1/n^2$ even for quite modest n (compare Table 2, which shows $e(Q) = \log_{10} \epsilon_{600}(Q)$). This suggests that the bounds used from transcendence theory are rather pessimistic, especially for finite primes.

Figure 1 plots the number of non-anomalous primes found against the reciprocal height, with the upper heuristic line indicated. Data points from Table 2 are recorded as solid dots, while the nine data points in Table 1 are recorded as hollow circles.

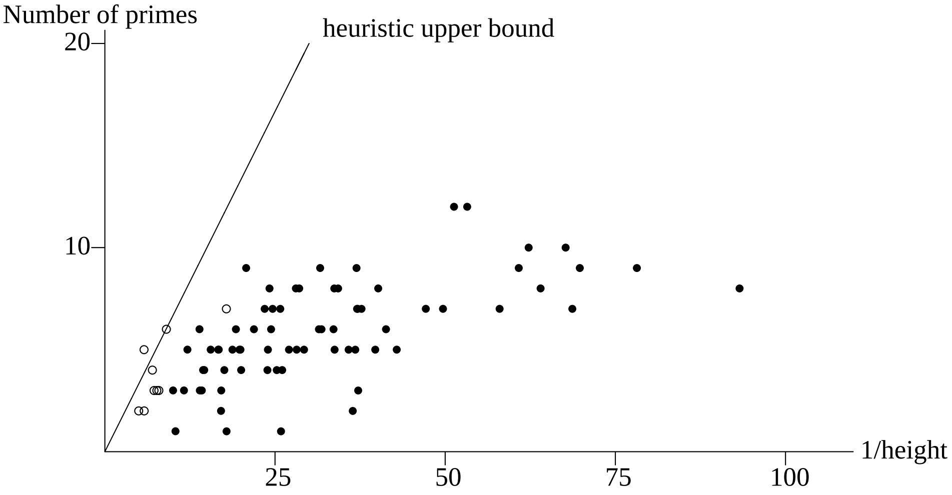

Figure 1: Number of primes found, against reciprocal height.

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

Table 2: Number of primes found

Curve	Q	$\hat{h}(Q)$	$N(Q)$	$e(Q)$	S
$[0, 1, 1, -100, 406]$	$[5, 7]$	0.010724	$8*$	-4.7	$\{3, 5\}$
$[0, 0, 1, -75, 256]$	$[-5, 22]$	0.012794	9	-4.8	$\{3, 5\}$
$[0, 1, 0, -190, 1025]$	$[-10, 45]$	0.014331	9	-4.8	$\{2, 3, 5\}$
$[0, 1, 1, -42, 110]$	$[0, 10]$	0.014560	7	-5.2	$\{3, 7\}$
$[0, 0, 1, -3, 4]$	$[4, 7]$	0.014772	10	-4.8	$\{3, 5\}$
$[0, 0, 0, -12, 20]$	$[-2, 6]$	0.015621	8	-5.4	$\{2, 3\}$
$[0, 1, 0, -57, 171]$	$[3, 6]$	0.016061	10	-5.1	$\{2, 3\}$
$[1, 1, 1, -12, 45]$	$[1, 5]$	0.016445	9	-5.2	$\{2, 3\}$
$[0, 1, 1, -12, 2]$	$[-3, 4]$	0.017243	7	-6.0	$\{3\}$
$[0, -1, 1, -2, 2]$	$[2, 1]$	0.018787	12	-5.1	$\{3\}$
$[1, -1, 1, -9, 9]$	$[-1, 4]$	0.019495	12	-5.2	$\{2\}$
$[0, 0, 0, -4, 4]$	$[2, 2]$	0.020132	7	-5.5	$\{2\}$
$[1, -1, 0, -1, 1]$	$[0, 1]$	0.021210	7	-4.9	$\{2\}$
$[0, 1, 0, -2, 9]$	$[-2, 3]$	0.023322	5	-4.9	$\{2, 3\}$
$[0, 1, 0, -12, 549]$	$[-6, 21]$	0.024213	6	-5.1	$\{2, 3, 7\}$
$[0, 0, 0, -1, 1]$	$[1, 1]$	0.024904	8	-5.2	$\{2\}$
$[1, 0, 1, -7, 14]$	$[1, 2]$	0.025175	5	-4.6	$\{2, 3\}$
$[1, 0, 0, -19, 33]$	$[2, 1]$	0.026523	7	-6.7	$\{2\}$
$[0, -1, 0, -1230, 17025]$	$[20, 5]$	0.026870	3	-5.2	$\{2, 5\}$
$[0, 1, 0, -106, 281]$	$[2, 9]$	0.026923	7	-5.2	$\{2, 3\}$
$[0, 1, 1, 10, 44]$	$[1, 7]$	0.026989	7	-4.8	$\{3, 5\}$
$[0, 0, 0, -67, 226]$	$[-3, 20]$	0.027047	9	-3.7	$\{2, 5\}$
$[0, 1, 0, -81, 243]$	$[3, 6]$	0.027179	5	-4.8	$\{2, 3\}$
$[0, 1, 0, -22, 41]$	$[2, 3]$	0.027455	2	-4.8	$\{2, 3\}$
$[0, 0, 0, -187, 991]$	$[7, 5]$	0.027921	5	-4.7	$\{2, 5\}$
$[0, -1, 0, -77, 289]$	$[-3, 22]$	0.029177	8	-4.9	$\{2, 11\}$
$[1, 0, 1, -9, 28]$	$[-1, 6]$	0.029624	5	-4.7	$\{2, 3\}$
$[0, -1, 0, -6, 9]$	$[0, 3]$	0.029660	8	-4.9	$\{2, 3\}$
$[0, 0, 0, -3, 34]$	$[5, 12]$	0.029759	6	-5.2	$\{2, 3\}$
$[0, 1, 1, 0, 0]$	$[0, 0]$	0.031408	6	-5.3	$\varnothing$
$[0, 0, 1, -3, 0]$	$[-1, 1]$	0.031606	9	-5.7	$\{3\}$
$[0, 1, 0, -96, 333]$	$[6, 3]$	0.031788	6	-4.8	$\{2, 3\}$
$[0, 1, 1, -346, -2288]$	$[-10, 16]$	0.034164	5	-4.7	$\{3, 11\}$
$[0, 1, 0, -61, 191]$	$[5, 6]$	0.035013	8	-4.8	$\{2, 3\}$

Continued on the next page

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

Table 2: Number of primes found, *continued*

Curve	Q	$\hat{h}(Q)$	$N(Q)$	$e(Q)$	S
[1, −1, 1, 1, 39]	[−1, 6]	0.035622	8	−4.9	{2, 3}
[1, −1, 1, −11, 27]	[−1, 6]	0.036961	5	−5.2	{2, 3}
[0, 0, 0, −21, 61]	[5, 9]	0.038373	4	−4.7	{2, 3}
[0, 1, 0, −457, 3656]	[11, 9]	0.038635	1	−5.0	{2, 3}
[0, 0, 0, −145, 1825]	[5, 35]	0.038793	7	−4.6	{2, 5, 7}
[1, 0, 0, −2, 1]	[1, 0]	0.039593	4	−6.3	$\varnothing$
[0, 1, 0, −186, 1089]	[−6, 45]	0.040564	7	−4.7	{2, 3, 5}
[0, 0, 1, −117, 982]	[−8, 37]	0.040938	6	−5.5	{3, 5}
[1, 1, 1, −16, −15]	[−3, 5]	0.041328	8	−5.0	{2}
[1, 1, 1, −5, 0]	[−2, 3]	0.041731	5	−4.8	{5}
[1, −1, 1, −27, −21]	[−3, 6]	0.041854	4	−4.5	{2, 5}
[0, −1, 0, −36, 232]	[−6, 14]	0.042577	7	−4.8	{2, 7}
[0, 1, 1, −51, 380]	[−6, 22]	0.045642	6	−4.9	{3, 5}
[0, 0, 1, −97, −180]	[−7, 12]	0.047199	5	−6.7	{5}
[0, 1, 1, −112, −380]	[−7, 10]	0.048152	9	−4.9	{3, 7}
[1, 0, 0, −17, 9]	[−2, 7]	0.049920	4	−4.7	{2, 3}
[1, 1, 0, −12, 4]	[−2, 6]	0.050171	5	−4.6	{2, 5}
[0, −1, 0, −112, 416]	[−4, 28]	0.050523	5	−5.0	{2, 7}
[0, 1, 0, −60, 144]	[−6, 18]	0.051907	6	−4.9	{2, 3}
[0, 1, 0, −8, 13]	[−2, 5]	0.053310	5	−4.6	{2, 5}
[0, −1, 0, −60, 792]	[−6, 30]	0.055897	1	−4.5	{2, 3, 5}
[0, −1, 0, −220, 1432]	[−6, 50]	0.056934	4	−4.7	{2, 5}
[0, 1, 1, −442, −3338]	[−13, 19]	0.058442	3	−4.9	{3, 13}
[0, 1, 1, −50, −94]	[−5, 7]	0.058542	2	−4.4	{3, 5}
[0, 1, 1, −8, −6]	[−2, 2]	0.059722	5	−4.9	{5}
[0, 0, 1, −147, 306]	[−7, 31]	0.059992	5	−4.6	{3, 7}
[1, 0, 0, −40, −64]	[−4, 8]	0.064265	5	−5.2	{2, 3}
[0, 1, 0, −1342, −18271]	[−22, 33]	0.068435	4	−4.7	{2, 3, 11}
[0, 1, 0, −133, 1863]	[−7, 50]	0.069217	4	−4.7	{2, 5}
[0, 1, 1, −286, −1180]	[−11, 27]	0.070143	3	−4.4	{5, 11}
[0, 0, 1, −40, 48]	[−6, 8]	0.071586	3	−5.1	{17}
[0, 1, 1, −382, −2958]	[−12, 6]	0.071857	6	−4.9	{13}
[0, 1, 1, −1, −1]	[−1, 0]	0.082352	5	−5.3	$\varnothing$
[1, 0, 0, −43, −103]	[−4, 5]	0.085944	3	−4.7	{2, 3}
[0, 1, 1, −2728, −53576]	[−31, 46]	0.096258	1	−4.9	{3, 31}
[0, 1, 0, −413, −3009]	[−11, 18]	0.099665	3	−5.1	{2, 3}

Acknowledgement. The authors thank the anonymous referees for several helpful comments.

References

1. Jean-Paul Bézivin, Attila Pethö and Alfred J. van der Poorten, 'A full characterization of divisibility sequences', *Amer. J. Math.* 112 (1990) 985–1001. 1, 1

2. J. S. Chahal, *Topics in number theory* (Plenum Press, New York, 1988). 7

3. D. V. Chudnovsky and G. V. Chudnovsky, 'Sequences of numbers generated by addition in formal groups and new primality and factorization tests', *Adv. in Appl. Math.* 7 (1986) 385–434. 2, 4, 8, 9

4. D. V. Chudnovsky and G. V. Chudnovsky, 'Computer assisted number theory with applications', *Number theory* (*New York*, 1984 – 5) (Springer, Berlin, 1987) 1–68. 2

5. Harvey Dubner and Wilfrid Keller, 'New Fibonacci and Lucas primes', *Math. Comp.* 68 (1999) 417–427, S1–S12. 2

6. M. Einsiedler, G. Everest and T. Ward, 'Morphic heights and periodic points', *New York Number Th. Sem.*, to appear (2001). 2

7. M. Einsiedler, G. Everest and T. Ward, 'Entropy and the canonical height.' *J. Number Theory*, to appear (2001). 4, 4, 5

8. M. Einsiedler, G. Everest and T. Ward, 'Primes in sequences associated to polynomials (after Lehmer)', *LMS J. Comput. Math.* 3 (2000) 125–139; http://www.lms.ac.uk/jcm/3/lms2000-004/. 1, 2, 7

9. G. Everest and T. Ward, 'The canonical height of an algebraic point on an elliptic curve', *New York J. Math.* 6 (2000). 4, 4

10. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edn (Clarendon Press, Oxford, 1979). 7

11. D. H. Lehmer, 'Factorization of certain cyclotomic functions', *Ann. of Math.* 34 (1933) 461–479. 1

12. PARI-GP, http://www.parigp-home.de. 6

13. T. A. Pierce, 'Numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$', *Ann. of Math.* 18 (1917) 53–64. 1

14. Paulo Ribenboim, 'The Fibonacci numbers and the Arctic ocean', *Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics* (*Munich*, 1993) (de Gruyter, Berlin, 1995) 41–83. 2

15. R. Shipsey 'Elliptic divisibility sequences', PhD Thesis, Goldsmith's College (University of London), 2000. 1

16. J. H. Silverman, *The arithmetic of elliptic curves* (Springer, New York, 1986). 3, 3, 8

17. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves* (Springer, New York, 1994). 3, 3, 4

18. S. S. Wagstaff, 'Divisors of Mersenne numbers', *Math. Comp.* 40 (1983) 385–397. 2, 7

19. M. Ward, 'The law of repetition of primes in an elliptic divisibility sequence', *Duke Math. J.* 15 (1948) 941–946. 2

20. M. Ward, 'Memoir on elliptic divisibility sequences', *Amer. J. Math.* 70 (1948) 31–74. 1, 3

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press

Manfred Einsiedler Manfred.Einsiedler@univie.ac.at

Mathematical Institute
University of Vienna
Strudlhofgasse 4
A-1090 Wien
Austria

Graham Everest G.Everest@uea.ac.uk
Thomas Ward T.Ward@uea.ac.uk

School of Mathematics
University of East Anglia
Norwich NR4 7TJ

https://doi.org/10.1112/S1461157000000772 Published online by Cambridge University Press