PRIMES IN DIVISIBILITY SEQUENCES

GRAHAM EVEREST AND THOMAS WARD

ABSTRACT. We give an overview of two important families of divisibility sequences: the Lehmer–Pierce family (which generalise the Mersenne sequence) and the elliptic divisibility sequences. Recent computational work is described, as well as some of the mathematics behind these sequences.

1. INTRODUCTION

An old problem in number theory concerns the sequence $1, 3, 7, 15, \ldots$ of numbers given by the formula $M_n = 2^n - 1$. These were studied by many people, but the French monk MARIN MERSENNE in the religious order of the Minims made the most important investigations.

MERSENNE wanted to use this sequence to find a formula that would represent primes. He did not succeed in this, but the numbers $M_p = 2^p - 1$ for p prime have proved to be of lasting interest in number theory. To honour his work, the sequence $M_n = 2^n - 1$ is now called the MERSENNE sequence. If a term in the sequence is a prime, it is known as a MERSENNE prime.

Lemma 1. *If $M_n = 2^n - 1$ is prime, then n must be a prime.*

Proof. If $n = ab$ with $a, b > 1$ then $M_a = 2^a - 1$ is a non-trivial factor of $2^n - 1$. □

Of course this does not say that if n is prime, then $2^n - 1$ is prime! In fact $2^{11} - 1 = 2047 = 23 \times 89$. What it does say is that if we want to search for primes in the sequence $2^n - 1$ we should restrict attention to the sequence $3, 7, 31, 127, 2047, 8191, \ldots$ given by the formula $N_n = 2^{p(n)} - 1$ where $p(n)$ is the nth prime number. The proof of Lemma 1 points to another important property of the MERSENNE sequence: it is a *divisibility sequence*. In other words,

$$\text{for all } m \geq 1, m|n \text{ implies } M_m|M_n. \tag{1}$$

The problem we mentioned at the start is this: does the MERSENNE sequence contain infinitely many primes? The so-called MERSENNE

The authors acknowledge the support of EPSRC award GR/M49588.

Prime Conjecture asserts the answer is 'yes', and it is an open problem to this day.

A more refined problem to study is this: how do the primes in the sequence (N_n) appear? That is, if $2^{n_1}-1, 2^{n_2}-1, \ldots$ is the sequence of MERSENNE primes we find, how fast does the sequence $n_1, n_2, \ldots$ grow? Of course this question does not really make sense until we know that there are infinitely many MERSENNE primes!

2. Heuristics

One approach to this problem is to use a *heuristic* argument. That is, rather than trying to prove that there are infinitely many MERSENNE primes, we argue that if certain plausible things happen, then there must be infinitely many MERSENNE primes. This gives an approach from probability that suggests the following: if $M_{n_1} = 2^{n_1}-1, M_{n_2} = 2^{n_2}-1, \ldots$ are the MERSENNE primes, then

$$\frac{\log\log M_{n_j}}{j} \longrightarrow \frac{\log 2}{e^{\gamma}},$$

where $\gamma = 0.577\ldots$ is the classical EULER-MASCHERONI constant. Numerical evidence to support this conjectured growth rate comes from simply testing the numbers $3, 7, 31, 127, 2047, 8191, \ldots$ for primality: the problem is these numbers grow very fast, so it is difficult to test them. A huge network of thousands of computers have been used together on this problem, and 38 MERSENNE primes have been found. Although the data set is not large, the observed growth rate does fit the expected rate very closely, see [2].

3. Sequences associated to polynomials

Another way to approach the MERSENNE Prime Conjecture is to examine sequences which arise in an analogous way to see whether the numerical evidence supports the natural analogous conjecture. Consider a monic polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with integer coefficients, which factorizes over $\mathbb{C}$ as

$$f(x) = (x-\alpha_1)\ldots(x-\alpha_d). \tag{2}$$

Following PIERCE [11] and LEHMER [9], we can associate a sequence of integers to f by defining

$$\Delta_n(f) = \prod_{i=1}^{d} |\alpha_i^n - 1| \text{ for } n \geq 1. \tag{3}$$

To see that all the terms are integers, let A_f denote the companion matrix of f. Then one can check that for all $n \geq 1$,

$$\Delta_n(f) = |\det(A_f^n - I_d)|. \tag{4}$$

We have found the formula (4) to be the most useful for computing terms of the sequence $\Delta_n(f)$, since it involves only integer arithmetic.

If $f(x) = x - 2$, then $\Delta_n(f) = 2^n - 1$ is the MERSENNE sequence. Just like the MERSENNE sequence, $\Delta_n(f)$ is a divisibility sequence. We assume for simplicity that no α_i is a root of unity, so $\Delta_n(f)$ is never equal to zero. If we can obtain evidence for prime occurrence in these sequences then it will strengthen our belief in the MERSENNE Prime Conjecture. To give ourselves the best chance of finding primes, we will assume f is irreducible because if we can write $f = f_1 f_2$ in a non-trivial way then

$$\Delta_n(f) = \Delta_n(f_1)\Delta_n(f_2).$$

The question of how fast the sequence $\Delta_n(f)$ grows – which determines how difficult it is going to be to search for primes in the sequence – is not simple. It is clear that

$$\frac{1}{n}\log|2^n - 1| \to \log 2,$$

and for the same reason, if $|\alpha_i| > 1$, then

$$\frac{1}{n}\log|\alpha_i^n - 1| \to \log|\alpha_i|.$$

For zeros α_i with $|\alpha_i| < 1$ there is no problem: in this case

$$\frac{1}{n}\log|\alpha_i^n - 1| \to 0.$$

All that remains is the possibility that we may have zeros α_i with $|\alpha_i| = 1$ that are not roots of unity. It turns out – though this is not trivial – that in this case also

$$\frac{1}{n}\log|\alpha_i^n - 1| \to 0.$$

Putting all the three possibilities together and using some transcendence theory to give error estimates, the following can be obtained (see [6] or [8]).

Theorem 2. *There are constants $m_f \geq 0$, and $A = A(f) > 0$, such that*

$$\frac{1}{n}\log\Delta_n(f) = m_f + O((\log n)^A/n).$$

The constant m_f is given by the formula,

$$m_f = \sum_{i=1}^{d} \log \max\{1, |\alpha_i|\}.$$

The quantity m_f is called the (logarithmic) MAHLER measure of f and it is common to denote e^{m_f} by M_f. It is a very important and subtle measure of the 'size' of f. Theorem 2 means that $\Delta_n(f)$ is approximately M_f^n when n is large. This gives rise to a version of Lemma 1 for LEHMER–PIERCE sequences.

Corollary 1. For only finitely many composite n's can $\Delta_n(f)$ be prime.

Proof. Notice firstly that Theorem 2 shows that $\Delta_n(f) \to \infty$ as $n \to \infty$. So there can only be finitely many n for which $\Delta_n(f) = 1$. If the statement of the corollary is false then there must be infinitely many pairs $1 < m < n$ with $\Delta_{mn}(f)$ prime as $n \to \infty$. But $\Delta_n(f)|\Delta_{mn}(f)$ and, by the previous remark, $\Delta_n(f)$ for only finitely many n. This forces $\Delta_{mn}(f) = \Delta_n(f)$ for infinitely many n. Thus, as $n \to \infty$, we obtain a contradiction because $\Delta_{mn}(f)$ grows like M_f^{mn} while $\Delta_n(f)$ grows like M_f^n. □

We would like to find a monic polynomial f with very small MAHLER measure, and see how many primes appear in the sequence $\Delta_n(f)$, which will grow very slowly. There is a problem though: How do we find such a polynomial? The following statement is sometimes known as Kronecker's Lemma. For a proof see [8, p.27].

Lemma 3. *If $m(f) = 0$, then f has a zero that is a root of unity. If f is irreducible and $m(f) = 0$ then the sequence $\Delta_n(f)$ is periodic.*

So the polynomials we are interested in all have strictly positive MAHLER measure. LEHMER [9] noticed that

$$g(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

has $m_g = 0.162\ldots$, and no smaller positive measure has been found since! This remarkable polynomial has 8 of its 10 roots lying on the unit circle, so these 8 roots have absolute value 1. It is not known whether polynomials with positive MAHLER measure can have arbitrarily small measure – this is known as LEHMER'S problem. The book [8] discusses what is known about this problem and shows how it relates to other parts of mathematics.

Because the polynomial g is symmetric, the roots pair off, each with its inverse. This forces the numbers $\Delta_n(g)$ to be perfect squares when n is odd. See [6] for a more detailed proof. Thus the correct analogue

of the MERSENNE problem is to ask: how often is the sequence $\Gamma_n = \sqrt{\Delta_n(g)}$ prime? Since there will be at most finitely many composite n for which Γ_n is prime, the same kind of heuristic argument as before may be applied to this problem. This heuristic predicts that if $n_1 < n_2 < \dots$ are the primes for which Γ_{n_j} are prime, then

$$\frac{\log\log\Gamma_{n_j}}{j} \to \frac{m_g}{2e^\gamma} = 0.0455\dots$$

4. Experimental results for Lehmer-Pierce sequences

As part of a broader investigation [6], the primes in the sequence Γ_n were found for $n \le 200,000$. The results are shown in Figure 1, which gives a good agreement with the conjectured behaviour. In the graph, n_j is the sequence of primes for which Γ_{n_j} was found to be prime. We found 208 such primes in a few weeks on a single PC. This compares with the 38 MERSENNE primes found using many thousands of computers over many years – the difference is that the sequence grows more slowly. The predicted growth rate compared very well with that observed.

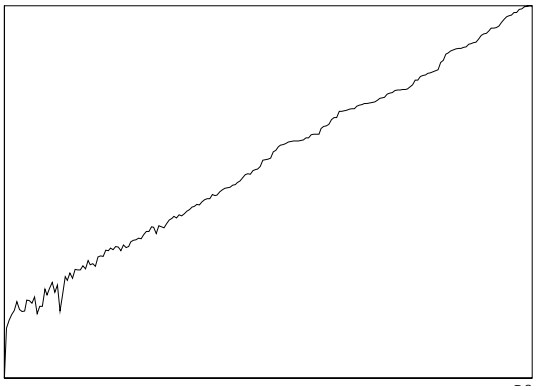

FIGURE 1. *Graph of* $\log\log\Gamma_{n_j}$ *against* j *for* $n \le 200,000$

5. Recurrence Relations

It is easily proved by induction that the MERSENNE sequence satisfies the linear recurrence relation

$$u_{n+2} = 3u_{n+1} - 2u_n \text{ for all } n \ge 1. \tag{5}$$

The LEHMER–PIERCE sequences we studied before also satisfy linear recurrence relations, but involving more terms. This reminds us of a

sequence studied several centuries before MERSENNE, the FIBONACCI sequence $1, 1, 2, 3, 5, \ldots$. Here the relation is the well-known

$$u_{n+2} = u_{n+1} + u_n \text{ for all } n \geq 1. \tag{6}$$

We will write F for the Fibonacci sequence with the nth term denoted F_n. It is widely believed — but not known — that the FIBONACCI sequence contains infinitely many prime terms F_n. There are other well-known sequences which satisfy (6). For example the LUCAS Sequence satisfies the same recurrence but starts $1, 3, 4, 7 \ldots$. We call this sequence L with the nth term denoted L_n. The reference [3] gives up-to-date information about primes in these sequences.

It seems plausible that a divisibility sequence which satisfies a linear recurrence relation should always contain infinitely many primes, provided one takes account of *generic factorization*. By this term, we mean there is something about the structure of the sequence that compels it to be composite for all sufficiently large n. For example, the LEHMER–PIERCE sequences coming from reciprocal polynomials take values which are squares. For another example, consider the sequence $3^n - 1$: All of the terms are even so at most one, when $n = 1$, can be prime. Nonetheless, we expect that the sequence $3^n - 1/2$ will be prime infinitely often. More generally, any divisibility sequence u_n will have all its terms divisible by the first so we look for prime values of u_n/u_1. There is another kind of generic factorization that you see, for example, with the sequence $4^n - 1$. Whenever $n > 1$, the terms will have non-trivial factors $2^n - 1$ and $2^n + 1$. Essentially the same kind of argument explains the example given by RIBENBOIM in [12, p. 64]. He notes that the sequence $0, 1, 3, 8, 21, 55 \ldots$ (the even terms of the FIBONACCI sequence) contains only one prime, even though it is a divisibility sequence with $u_1 = 1$ and it satisfies a linear recurrence relation. Using the characterization given in [1], it is possible to explain precisely when a linear divisibility sequence will have generic factorization. What we are saying is that provided this generic factorization is taken into account, one expects infinitely many primes to appear.

6. Elliptic Divisibility Sequences

We are now going to discuss divisibility sequences which satisfy a different kind of recurrence relation. These come from *elliptic curves*, and have many interesting and subtle properties. There are two approaches: one is very formal and elementary but hides the geometry, the other shows how the curve is used but is more sophisticated.

For the first approach, say that a divisibility sequence u_n $n \geq 0$ is an *elliptic divisibility sequence* if

$$u_{m+n}u_{m-n} = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2 \tag{7}$$

for all $m \geq n \geq 1$. For technical reasons, we restrict attention to sequences that have $u_0 = 1$, $u_1 = 1$, $u_2u_3 \neq 0$ and $u_2|u_4$; call these sequences *proper*. Morgan Ward studied many properties of proper elliptic divisibility sequences in [14]. Later on, we will explain in what sense these sequences are 'elliptic' – it might seem surprising since there do not seem to be any ellipses on show!

The recurrence relation (7) is less straightforward than a linear recurrence, and you might wonder what the terms of such a sequence look like. The first thing to say is that there are familiar examples. For example, the sequence $u_n = n$ satisfies (7) and so does the sequence $0, 1, -1, 0, 1, -1, 0 \ldots$. But these are trivial examples so we go on to talk about the important non-trivial examples.

In order to calculate terms, notice firstly that the single relation (7) gives rise to two relations

$$u_{2n+1} = u_{n+2}u_n^3 - u_{n-1}u_{n+1}^3, \quad \text{and} \tag{8}$$

$$u_{2n}u_2 = u_{n+2}u_nu_{n-1}^2 - u_nu_{n-2}u_{n+1}^2. \tag{9}$$

The relation (8) comes about by setting $m = n + 1$ whilst (9) comes about by setting $m = n + 2$ then replacing n by $n - 1$. The relations (8) and (9) can be subsumed into the single relation

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

where $\lfloor\cdot\rfloor$ denotes, as usual, the integer part.

If you just specify the terms $u_0, \ldots, u_4$ of a proper sequence then you can use the relation to compute all the other terms in the sequence. It is remarkable that you always end up with a divisibility sequence.

7. Primes in elliptic divisibility sequences

Our theme has to do with primes in divisibility sequences which satisfy recurrence relations. For the Lehmer-Pierce sequences, we studied the growth rates to decide whether checking for prime appearance was feasible. Thus, the first natural question which occurs is to decide the growth rate for a proper elliptic divisibility sequence. We answered this question in [7].

Theorem 4. *Suppose u_n denotes the nth term of a non-trivial proper elliptic divisibility sequence. There are constants $\kappa \geq 0$ and B such that*

$$\log |u_n| = \kappa n^2 + O\left((\log n)^B\right).$$

If $\kappa = 0$ then the sequence is periodic with finite period.

Thus the only interesting sequences from our point of view are those with $\kappa > 0$. This means the nth term is approximately $e^{\kappa n^2}$ for large n, so the sequences grow very rapidly indeed. From Theorem 4 we can make a familiar deduction.

Corollary 2. There are only finitely many composite indices n for which u_n is prime.

If we wish to examine particular sequences for prime occurrence, we will need to choose a sequence whose growth rate κ is small. Thus we find ourselves asking a similar sort of problem to the one LEHMER faced. Can we find sequences with arbitrarily small growth rate? We are going to discuss this elliptic analogue of LEHMER'S problem later.

In the papers [4] and [5], CHUDNOVSKY and CHUDNOVSKY considered the arithmetic of elliptic divisibility sequences. The following examples are taken from [4]. The first 5 terms are specified, then the first 100 terms are calculated. Table 1 shows prime appearance for prime indices up to $n = 100$. Also shown are the corresponding growth rates κ.

Initial terms	Growth rate κ	Prime incidence up to $n = 100$
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

TABLE 1. Elliptic divisibility sequences from the paper [4] of CHUDNOVSKY & CHUDNOVSKY.

Some of the primes in this table are very large. For example, the term u_{79} in the third sequence from the end is a prime with 469 decimal digits. It might look as though we should be able to keep computing terms and find larger and larger primes: This was thought to be the

case for some time. But if you run the sequences out to $n = 500$ you find no new primes. In [7] we provide a heuristic explanation of why we believe these sequences should stop producing primes beyond a certain point.

Finally, suppose that the terms u_2 and u_3 in a proper elliptic divisibility sequence are not coprime, say the prime p divides both terms. Then $p|u_4$, one of the conditions for being a proper sequence. Now one can show, by induction, using the formulæ (8) and (9), that all the terms will be divisible by p. Thus, in these cases, we can see that we will never obtain infinitely many primes in the sequence.

Suppose we write $d = \gcd(u_2, u_3)$ and let S denote the set of primes which divide d. Write v_n to be the same as u_n except with the primes in S removed. Of course this is still a divisibility sequence, although it might not satisfy (7). Now that we have removed generic factorization from u_n, we can examine the sequence v_n for prime appearance. In [7], the growth rate of v_n was considered.

Theorem 5. *For some $0 < K < 2$, and $\lambda \geq 0$*

$$\log |v_n| = \lambda n^2 + O(n^K).$$

If we wish to examine these sequences v_n for prime appearance then we need to find examples where the growth rate λ is small. It is helpful then to supply some of the background from the theory of elliptic curves. We will do this in the next section before supplying some examples of sequences v_n with small λ. The Elliptic Lehmer Problem states that the non-zero values of λ are bounded below uniformly away from zero. It is a very difficult problem.

8. Elliptic Curves

Another approach to elliptic divisibility sequences is to start with an elliptic curve

$$y^2 = x^3 + ax + b \tag{10}$$

with coefficients a, b in $\mathbb{Z}$. An excellent reference for this topic is Silverman's book [13]. We must always suppose that the quantity $4a^3 + 27b^2 \neq 0$. This condition is equivalent to the cubic polynomial $x^3 + ax + b$ having no repeated zeros. If $Q = (x, y)$ is an integer point on the curve then we can use it to begin an elliptic divisibility sequence. Define

$$\begin{aligned}
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5ax^2 - 4abx - 8b^2 - a^3).
\end{aligned}$$

Now the formulæ (8) and (9) can be used to generate all the other terms of an elliptic divisibility sequence $u_n = \psi_n$. This might seem an incredibly complicated way to generate an elliptic divisibility sequence! Before we explain why we do things this way we will exhibit a table to show the prime appearance and growth rates for various sequences v_n. The table shows the coefficients a, b in (10) together with the starting point $Q = (x, y)$, the growth rate h for the sequence v_n, N, the number of prime values of v_n with n prime up to 500, and the set S consisting of the primes which divide $\gcd(u_2, u_3)$.

a	b	Q	h	N	S
-12	20	(-2,6)	0.015621	8	$\{2,3\}$
-4	4	(2,2)	0.020132	7	$\{2\}$
-1	1	(1,1)	0.024904	8	$\{2\}$
-67	226	(-3,20)	0.027047	9	$\{2,5\}$
-187	991	(7,5)	0.027921	5	$\{2,5\}$
-3	34	(5,12)	0.029759	6	$\{2,3\}$
-21	61	(5,9)	0.038373	4	$\{2,3\}$
-145	1825	(5,35)	0.038793	7	$\{2,5,7\}$

TABLE 2. Prime appearance and growth rate.

The formulæ in (11) come about because our elliptic curve has an *algebraic structure*. The points on the curve (10) actually form a group in the following sense. Suppose we draw the tangent to our starting point Q, then this tangent will meet the curve again at a point (we must allow the possibility that this is the point 'at infinity'). This point might not be an integral point, but its coefficients will certainly be rationals. We write $2Q$ for the reflection of this new point in the x-axis. Now join this new point $2Q$ to Q by a straight line which will meet the curve at a new point, again rational. The reflection of this new point in the x-axis we call $3Q$. By induction, we form a sequence of points on the curve nQ and each of them have rational coordinates. What is going on here is that we are using the natural group operation on the curve. If we wrote this operation using a '+' sign then the point nQ really is the result of adding Q to itself $n-1$ times using the operation '+'. The general case is illustrated in Figure 2, where points P and Q are added to make R.

The connection with our complicated definitions at the start of this section is that the x-coordinate of nQ can be expressed in terms of the coordinates of Q and a and b as ϕ_n/ψ_n^2 with ψ_n defined as above. Here ϕ_n is another polynomial which can also be defined by a recursion formula. The arithmetic of elliptic curves has been studied very

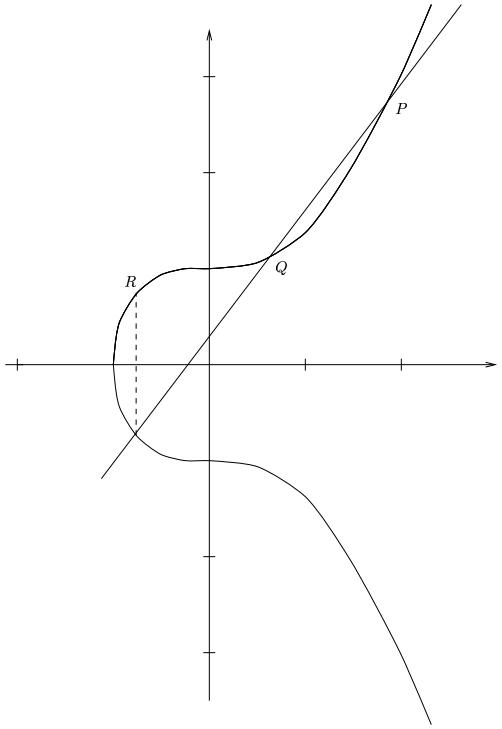

FIGURE 2. *$R = P + Q$ on an elliptic curve*

intensely and a great deal of knowledge now exists that can be used in the study of elliptic divisibilty sequences. At the same time, problems such as the Elliptic LEHMER Problem can be stated simply in terms of elliptic divisibilty sequences. The growth rates we discussed earlier can be understood in terms of quantities related to points on the curves: The quantity λ is usually known as the *global canonical height*. We used knowledge of elliptic curves to find sequences with small growth rates. Table 2 is taken from [7].

9. PERIODIC POINTS

Suppose X denotes a set and $T : X \to X$ a map on X. We define, for every $n > 0$

$$\mathrm{Per}_n(T) = |\{x \in X : T^n(x) = x\}|. \tag{11}$$

This is the number of periodic points of order n for the map T on X. In dynamical systems the properties of iterates of maps are studied. Often, the set X will come equipped with some topological structure and T will be a map which preserves that structure. For example, X could be a topological space and T could be a continuous map. The

following examples show the connection between these ideas and our earlier ones about sequences.

Example 6. Let $X = [0,1)$ denote the additive circle, actually a group. Let $T : X \to X$ denote the map $T(x) = 2x \bmod 1$. This is a continuous map of the compact group X and it is easy to check that

$$\mathrm{Per}_n(T) = 2^n - 1.$$

Thus the MERSENNE sequence appears again, this time in connection with a simple dynamical system.

We say a sequence of positive integers is *realizable* if it agrees with $\mathrm{Per}_n(T)$ for any map T on any set X. The next example shows that the LEHMER-PIERCE sequences are realizable.

Example 7. Let $f(x) = x^d + \cdots + a_0$ denote an integral polynomial, and $X = [0,1)^d$ the d-dimensional torus. The companion matrix of f acts by multiplication on X (and reducing mod 1) to give our map T. The number of periodic points is given by the formula

$$\mathrm{Per}_n(T) = \Delta_n(f).$$

A different kind of example realizes the Lucas sequence.

Example 8. Let X be the space of all sequences of 0's and 1's in which a 1 is always followed by a 0. This has a natural topology which turns it into a compact space. If T now denotes the map which shifts any sequence along one place to the left then

$$\mathrm{Per}_n(T) = L_n.$$

Notice that in this example, the map is not an endomorphism of a group as it was with the first two examples. When the map is a group endomorphism, we always get a divisibility sequence for the sequence of periodic points. This is because, the equation $T^n(x) = x$ can be written $(T^n - I)(x) = 0$, where I denotes the identity map on X and thus the solutions x lie in the kernel of an endomorphism. If $n|m$ then the solutions of $T^n(x) = x$ form a subgroup of the group of solutions of $T^m(x) = x$ and LEGENDRE'S Theorem implies the statement about divisibility.

It seems a natural question to ask whether the FIBONACCI sequence itself can represent the periodic points of a dynamical system and the answer is no. In fact, the following was proved recently (see [10]).

Theorem 9. *Suppose $U = a, b \ldots$ denotes any sequence of positive integers which satisfies* (6)*. Then U is realizable if and only if $b = 3a$. In other words U is realizable if and only if it is a multiple of L, the* LUCAS *sequence.*

The method of proof for this theorem rests on an apparently simple, but very profound, observation. Let $r(n)$ denote a sequence of non-negative integers. Write $\hat{r}(n) = (r * \mu)(n)$ for the convolution of r with the MÖBIUS function,

$$\hat{r}(n) = \sum_{d|n} \mu(n/d) r(d).$$

Then $r(n)$ is realizable if and only if

$$n | \hat{r}(n) \text{ and } \hat{r}(n) \geq 0 \text{ for every } n \geq 1. \tag{12}$$

This condition can be used to rule out particular examples of sequences as being realizable. For example, the condition above says that if $n = p$ is a prime then

$$r(p) \equiv r(1) \bmod p. \tag{13}$$

Consider the elliptic divisibility sequences in Table 1. Each of the sequences of absolute values can be tested to see if they are realizable. For the sequence 0,1,1,1,-2, the next term is -3 and already this fails the condition (13) when $p = 5$. Similarly, the next term in the sequence $0, 1, 1, 1, 6$ is 5 and this also fails the condition (13) when $p = 5$. More generally, if we specify the terms $0, 1, 1, 1, c \geq 2$ then the formula (8) gives $u_5 = c - 1$. The only way this can be congruent to 1 mod 5 is if $c \equiv 2 \bmod 5$. In this way it is easy to generate many elliptic divisibility sequences which fail to be realizable. In fact, so far, we have not found a single elliptic divisibility sequence whose absolute values are realizable.

10. Dynamics and the Mersenne Prime Conjecture

In this last section we will draw together some of the threads in an attempt to suggest an approach to the MERSENNE Prime Conjecture. We have noticed that the sequences which are realizable also seem to contain infinitely many primes, having taken account of any generic factorization. By contrast, elliptic divisibilty sequences seem never to be realizable, nor to contain infinitely many primes. Of course one cannot press sequences neatly into two camps. For example, the FIBONACCI sequence is conjectured to have infinitely many primes but is not realizable.

However, this behaviour does cause us to speculate that a fruitful approach to the MERSENNE Prime Conjecture (and related conjectures for LEHMER-PIERCE and LUCAS sequences) might be through dynamical systems. Specifically, does the fact that they count periodic points (and therefore come from numbers of points on individual orbits) enable anything to be said about their arithmetic properties?

References

[1] Jean-Paul Bézivin, Attila Pethő and Alfred J. van der Poorten, 'A full characterisation of divisibility sequences.' *Amer. J. Math.* 112 (1990) 985–1001.
[2] Chris Caldwell, 'Prime Page' `http://www.utm.edu/research/primes`
[3] Harvey Dubner and Wilfrid Keller, 'New Fibonacci and Lucas primes.' *Math. Comp.* 68 (1999) 417–427, S1–S12.
[4] 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.
[5] D.V. Chudnovsky and G.V. Chudnovsky, 'Computer assisted number theory with applications.' 'Number theory (New York, 1984–1985),' (Springer, Berlin, 1987) pp. 1–68, pp. 1–68.
[6] M. Einsiedler, G. Everest and T. Ward, 'Primes in sequences associated to polynomials (after Lehmer).' *LMS J. Math. and Comp.* 3 (2000) 125–139.
[7] M. Einsiedler, G. Everest and T. Ward, 'Computational aspects of elliptic divisibility sequences' *Pre-print*
[8] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics* (Springer, London, 1999).
[9] D.H. Lehmer, 'Factorization of certain cyclotomic functions.' *Ann. of Math.* 34 (1933) 461–479.
[10] Yash Puri and Thomas Ward, 'A dynamical property unique to the Lucas sequence.' *Pre-print*
[11] 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.
[12] 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) pp. 41–83, pp. 41–83.
[13] Joseph H. Silverman *The Arithmetic of Elliptic Curves* (Springer, New York, 1986).
[14] M. Ward, 'Memoir on elliptic divisibility sequences.' *Amer. J. Math.* 70 (1948) 31–74.

E-mail address: `g.everest@uea.ac.uk`

E-mail address: `t.ward@uea.ac.uk`

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK.