NUMBER THEORY PROBLEMS FROM THE HARMONIC ANALYSIS OF A FRACTAL

DORIN ERVIN DUTKAY AND JOHN HAUSSEMANN

Abstract. We study some number theory problems related to the harmonic analysis (Fourier bases) of the Cantor set introduced by Jorgensen and Pedersen in [JP98].

Contents

1. Introduction 1
2. Proofs and other results 6
3. Examples 15
References 16

1. Introduction

In [JP98], Jorgensen and Pedersen made a surprising discovery: they constructed a fractal measure on a Cantor set which has an orthonormal Fourier series. This Cantor set is obtained from the interval [0, 1], dividing it into four equal intervals and keeping the first and the third, [0, 1/4] and [1/2, 3/4], and repeating the procedure infinitely many times. It can be described in terms of iterated function systems: let

\[ \tau_0(x) = x/4 \text{ and } \tau_2(x) = (x + 2)/4, \quad (x \in \mathbb{R}). \]

The Cantor set \( X_4 \) is the unique compact set that satisfies the invariance condition

\[ X_4 = \tau_0(X_4) \cup \tau_2(X_4). \]

The set \( X_4 \) is described also in terms of the base 4 decomposition of real numbers:

\[ X_4 = \left\{ \sum_{k=1}^{n} 4^{-k} b_k : b_k \in \{0, 2\}, n \in \mathbb{N} \right\}. \]

On the set \( X_4 \) one considers the Hausdorff measure \( \mu \) of dimension \( \log_4 2 = \frac{1}{2} \). In terms of iterated function systems, the measure \( \mu \) is the invariant measure for the iterated function system, that is, the unique Borel probability measure that satisfies the invariance equation

\[ \mu(E) = \frac{1}{2} \left( \mu(\tau_0^{-1} E) + \mu(\tau_2^{-1} E) \right), \text{ for all Borel sets } E \subset \mathbb{R}. \]

2010 Mathematics Subject Classification. 11A07,11A51,42C30.
Key words and phrases. Cantor set, Fourier basis, prime decomposition, spectral measure.
Equivalently, for all continuous compactly supported functions \( f \),

\[
\int f \, d\mu = \frac{1}{2} \left( \int f \circ \tau_0 \, d\mu + \int f \circ \tau_2 \, d\mu \right).
\]

We denote, for \( \lambda \in \mathbb{R} \):

\[
e^{2\pi i \lambda x}, \quad (x \in \mathbb{R}).
\]

Jorgensen and Pedersen proved in that the Hilbert space \( L^2(\mu) \) has an orthonormal basis formed with exponential functions, i.e., a Fourier basis, \( E(\Gamma_0) := \{e_\lambda : \lambda \in \Gamma_0\} \) where

\[
(1.3) \quad \Gamma_0 := \left\{ \sum_{k=0}^{n} 4^k l_k : l_k \in \{0, 1\}, n \in \mathbb{N} \right\}.
\]

Later, Strichartz \cite{Str06} proved that these Fourier series have better convergence properties than their classical counterparts on the unit interval; for example, the Fourier series of a continuous function converge uniformly.

**Definition 1.1.** We say that the subset \( \Gamma \) of \( \mathbb{R} \) is a spectrum for the measure \( \mu \) if the corresponding family of exponential functions \( E(\Gamma) := \{e_\lambda : \lambda \in \Gamma\} \) is an orthonormal basis for \( L^2(\mu) \). We say that \( \Gamma \) is complete/incomplete if the set \( E(\Gamma) \) is as such in \( L^2(\mu) \).

Other spectra for the measure \( \mu \) were constructed later in \cite{LW02, Str00, DJ06, DHS09, DHL13}, using some other digits for the spectrum. As we can see in (1.3), the spectrum \( \Gamma_0 \) corresponds to the digits \( \{0, 1\} \).

The main question that we address in this paper is the following:

**Question.** For what digits \( \{0, m\} \) with \( m \in \mathbb{N} \) odd is the set

\[
\Gamma(m) := m\Gamma_0 = \left\{ \sum_{k=0}^{n} 4^k l_k : l_k \in \{0, m\}, n \in \mathbb{N} \right\}
\]

a spectrum for \( L^2(\mu) \)?

**Definition 1.2.** Let \( m \in \mathbb{N} \) be an odd number. We say that \( m \) is complete if the set \( \Gamma(m) \) is a spectrum for the measure \( \mu_4 \). We say that \( m \) is incomplete if it is not complete.

As it was shown in \cite{DJ06}, that the set \( E(\Gamma(m)) \) is always orthonormal in \( L^2(\mu) \), but sometimes it is incomplete. For example, for \( m = 3 \), the set \( \Gamma(3) \) is not complete. Applying the results from \cite{LW02} or the refinement obtained in \cite{DJ06}, we can characterize the numbers \( m \) that give spectra (i.e., complete orthonormal bases) in terms of extreme cycles.

**Definition 1.3.** Let \( m \in \mathbb{N} \) be an odd number. We say that a finite set \( \{x_0, x_1, \ldots, x_{r-1}\} \) is an extreme cycle (for the digits \( \{0, m\} \)) if there exist \( l_0, \ldots, l_{r-1} \in \{0, m\} \) such that

\[
x_1 = \frac{x_0 + l_0}{4}, \quad x_2 = \frac{x_1 + l_1}{4}, \quad \ldots, \quad x_{r-1} = \frac{x_{r-2} + l_{r-2}}{4}, \quad x_0 = \frac{x_{r-1} + l_{r-1}}{4},
\]

and

\[
(1.4) \quad \left| \frac{1 + e^{2\pi i 2x_k}}{2} \right| = 1, \quad (k \in \{0, \ldots, r-1\}).
\]

The points \( x_i \) are called extreme cycle points.
Theorem 1.4. [LVW02, DJ06] Let \( m \in \mathbb{N} \) be odd. The number \( m \) is complete if and only if the only extreme cycle for the digit set \( \{0, m\} \) is the trivial one \( \{0\} \).

For example, for \( m = 3 \), the set \( \{1\} \) is an extreme cycle: \( (1 + 3)/4 = 1 \) and \( e^{2\pi i/2} = 1 \), so \( \Gamma(3) \) is incomplete.

In [DJ09] it was proved that the sets \( \Gamma(5^k) \) are complete for any \( k \), which shows the surprising fact that spectra have arbitrarily low densities. In [DHL13] it was shown that there are spectra for this fractal measure which have zero Beurling dimension. The result from [DJ09] was used by Jorgensen et al. to construct some scaling operators on the Cantor set, operators that exhibit an interesting fractal structure [JKS12, JKS14].

Theorem 1.4 turns our question into a number theory question: for what odd numbers \( m \) are there no (non-trivial) extreme-cycles? Any odd number \( m \) satisfying this criterion is complete; any odd number \( m \) not satisfying this criterion is incomplete.

We state here the main results of the paper and we provide the proofs in the next section.

Proposition 1.5. Let \( m \) and \( k \) be some odd natural numbers. If \( m \) is incomplete then \( km \) is incomplete.

Because of Proposition 1.5, we define primitive numbers:

Definition 1.6. We say that an odd number \( m \) is primitive if \( m \) is incomplete and, for all proper divisors \( d \) of \( m \), \( d \) is complete. In other words, there exist extreme cycles for the digits \( \{0, m\} \) and there are no extreme cycles for the digits \( \{0, d\} \) for any proper divisor \( d \) of \( m \).

Of course, a number \( m \) will be incomplete if and only if it is divisible by a primitive number. A computer check shows that the first primitive numbers are: 3, 85, 341, 455, 1285, 4369, 5461, 6355, 9709, 28679, 60787, 327685, 416179. See Table 1 for more primitive numbers. So, in particular, the numbers \( 3k, 85k, 341k, 455k, 1285k \) etc. are incomplete for any odd natural number \( k \). The primitive numbers seem to become more and more sparse, but we were able to prove that:

Theorem 1.7. There are infinitely many primitive numbers.

First, we give a criterion that ensures that a number \( m \) is complete. It is based on the multiplicative group generated by the number 4 in \( \mathbb{Z}_m \).

Definition 1.8. Let \( m \) be an odd natural number. We will denote by \( \mathbb{Z}_m \) the finite ring of integers modulo \( m \), \( \mathbb{Z}/m\mathbb{Z} \). We use the notation \( \mathbb{Z}_m^\times \) to indicate the multiplicative structure on \( \mathbb{Z}_m \). We denote by \( U(\mathbb{Z}_m) \) the set of elements in \( \mathbb{Z}_m \) that have a multiplicative inverse. We denote by \( G_m \) the group generated by 4 in \( U(\mathbb{Z}_m) \),

\[
G_m = \{ 4^j \pmod{m} : j = 0, 1, \ldots \}.
\]

The order of 4 in the group \( U(\mathbb{Z}_m) \) is the smallest positive integer \( a \) such that \( 4^a \equiv 1 \pmod{m} \). We denote \( a \) by \( \alpha_4(m) \) and \( \alpha_4(m) = |G_m| \).

We denote by \( \text{lcm}(a_1, \ldots, a_n) \) the lowest common multiple of the numbers \( a_1, \ldots, a_n \).

Theorem 1.9. Let \( m > 3 \) be an odd number not divisible by 3. If any of the numbers \( -1(\pmod{m}), -2(\pmod{m}), 2(\pmod{m}), \) or \( 3(\pmod{m}) \) is in \( G_m \), then \( m \) is complete.

Theorem 1.10. Let \( m > 12 \) be an odd number not divisible by 3. If any of the numbers \( 5(\pmod{m}), 6(\pmod{m}), 7(\pmod{m}), 8(\pmod{m}), 9(\pmod{m}), 10(\pmod{m}), 11(\pmod{m}) \) or \( 12(\pmod{m}) \) is in \( G_m \), then \( m \) is complete.
Table 1. Primitive numbers up to $5 \times 10^6$, their prime decompositions and $o_4$ for the primes in the prime decomposition.

| $m$ | Prime decomposition | $o_4$ for the primes |
|-----|---------------------|----------------------|
| 3   | 3                   | 1                    |
| 85  | 5,17                | 2,4                  |
| 341 | 11,31               | 5,5                  |
| 455 | 5,7,13              | 2,3,6                |
| 1285| 5,257               | 2,8                  |
| 4369| 17,257              | 4,8                  |
| 5461| 43,127              | 7,7                  |
| 6355| 5,31,41             | 2,5,10               |
| 9709| 7,19,73             | 3,9,9                |
| 28679| 7,17,241           | 3,4,12               |
| 60787| 89,683              | 11,11                |
| 327685| 5,65537           | 2,16                 |
| 416179| 29,113,127         | 14,14,7              |
| 549791| 11,151,331         | 5,15,15              |
| 755915| 5,19,73,109       | 2,9,9,18             |
| 1114129| 17,65537          | 4,16                 |
| 1472045| 5,37,73,109       | 2,18,9,18            |
| 1549411| 31,151,331        | 5,15,15              |
| 1912111| 31,61681           | 5,20                 |
| 2060863| 7,37,73,109       | 3,18,9,18            |
| 3335735| 5,13,19,37,73     | 2,6,9,18,9           |
| 6973057| 7,13,19,37,109    | 3,6,9,18,18          |

Then we prove that any prime power is a complete number:

**Theorem 1.11.** If $p$ is a prime number, $p > 3$ and $n \in \mathbb{N}$, then $p^n$ is complete.

The rest of the paper is devoted to the study of which composite numbers are primitive or complete.

**Definition 1.12.** For a prime number $p \geq 3$, we denote by $\iota_4 (p)$ the largest number $l$ such that $o_4 (p^l) = o_4 (p)$. We say that $p$ is simple if $o_4 (p) < o_4 (p^2)$, i.e., $\iota_4 (p) = 1$.

**Remark 1.13.** The first non-simple prime number is 1093 and $o_4 (1093) = o_4 (1093^2) = 182$.

The main techniques that we will use are contained in the following two lemmas:

**Lemma 1.14.** Let $a, b \geq 1$ be odd numbers. Assume that $o_4 (ab) \geq \frac{2a+15}{12} o_4 (b)$. Then $ab$ is not primitive.

**Lemma 1.15.** Let $a, b \geq 1$ be odd numbers. Assume that $o_4 (ab) \geq 2^{\log_2 \sqrt{41}} o_4 (b)$. Then $ab$ is not primitive.
Remark 1.16. The estimate in Lemma 1.15 is almost always better than the estimate in Lemma 1.14 as we have $2^{\left\lfloor \log_2 \sqrt{\frac{m}{3}} \right\rfloor} < \frac{2a+15}{12}$ for all odd numbers $a$ except $a = 13$ and $a = 15$, and for $a = 18$, since $a$ is divisible by 3 we know that $ab$ is not complete and not primitive. Despite this, we include this lemma since the arguments in the proof are different and they might be improved.

Remark 1.17. We will use Lemmas 1.14 and 1.15 inductively to prove that some numbers are complete: start with a prime power. We know these are complete, from Theorem 1.11. Then, multiply by some number in such a way that one of the lemmas applies. Repeat this inductively.

Theorem 1.18. Let $p_1, \ldots, p_r$ be distinct odd primes. For $i \in \{1, \ldots, r\}$, let $j_i \geq 0$ be the largest number such that $p_i^{j_i}$ divides $\text{lcm}(o_4(p_1), \ldots, o_4(p_r))$. Assume that $p_1^{j_1 + j_1} \cdots p_r^{j_r + j_r}$ is complete. Then $p_1^{k_1} \cdots p_r^{k_r}$ is complete for any $k_1, \ldots, k_r \geq 0$.

We performed a computer check to find all the primitive numbers less than $10^7$. The results are listed in Table 1. Using this and Theorem 1.18 we get the next Corollary.

Corollary 1.19. Let $p_1, \ldots, p_r$ be distinct odd primes. For $i \in \{1, \ldots, r\}$, let $j_i \geq 0$ be the largest number such that $p_i^{j_i}$ divides $\text{lcm}(o_4(p_1), \ldots, o_4(p_r))$. Assume that $p_1^{j_1 + j_1} \cdots p_r^{j_r + j_r} < 10^7$ and that the set $\{p_1, \ldots, p_r\}$ does not contain any of the lists in the second column of Table 1. Then $p_1^{k_1} \cdots p_r^{k_r}$ is complete for any $k_1, \ldots, k_r \geq 0$.

The next results show that if the order of 4 in $U(\mathbb{Z}_m)$ is large, then $m$ cannot be primitive.

Theorem 1.20. Let $m$ be an odd number. Assume the following conditions are satisfied:

(i) For every proper divisor $d|m$, $d < m$, the number $d$ is complete.

(ii) There exists $n \geq 0$ such that

$$o_4(m) > \min_n \left\{ 2^n \left\lceil \frac{m}{3 \cdot 4^n} \right\rceil \right\}.$$  

Then $m$ is complete. If only condition (ii) is satisfied, then $m$ is not primitive. Here $\lceil x \rceil$ is the smallest integer larger than or equal to $x$.

Corollary 1.21. Let $m$ be an odd number. If

$$o_4(m) > 2^{\left\lfloor \log_2 \sqrt{\frac{m}{3}} \right\rfloor},$$

or in particular, if

$$o_4(m) > \sqrt{\frac{4m}{3}},$$

then $m$ is not primitive.

Corollary 1.22. Let $p_1, \ldots, p_r$ be distinct simple prime numbers strictly larger than 3. Assume the following conditions are satisfied:

(i) For any proper subset $F \subset \{1, \ldots, r\}$ and any powers $k_i \geq 0$, $i \in F$, the number $\prod_{i \in F} p_i^{k_i}$ is complete.

(ii) None of the numbers $o_4(p_1), \ldots, o_4(p_r)$ is divisible by any of the numbers $p_1, \ldots, p_r$.

(iii) The following equation is satisfied:

$$\text{lcm}(o_4(p_1), \ldots, o_4(p_r)) > 2^{\left\lfloor \log_2 \sqrt{\frac{m}{3}} \right\rfloor}.$$
Then $p_1^{k_1} \ldots p_r^{k_r}$ is complete.

**Corollary 1.23.** Let $p_1, \ldots, p_r$ be distinct simple prime numbers strictly larger than 3. Assume the following conditions are satisfied:

(i) The numbers $o_4(p_1), \ldots, o_4(p_r), p_1, \ldots, p_r$ are mutually prime.

(ii) $o_4(p_j) > \sqrt{\frac{4}{3}} p_j$ for all $j$.

Then the number $p_1^{k_1} \ldots p_r^{k_r}$ is complete for any $k_1 \geq 0, \ldots, k_r \geq 0$.

**Corollary 1.24.** Let $a$ be a complete odd number. Let $p > 3$ be a simple prime number. Assume that

(i) $p$ does not divide $a$;

(ii) $o_4(p)$ and $o_4(a)$ are mutually prime;

(iii) $o_4(p) > 2^{\lceil \log_2 \sqrt{\frac{4}{3}} \rceil}$ (in particular if $o_4(p) = \frac{p-1}{2}$, $p > 5$).

Then $p^k a$ is complete for all $k \geq 0$.

In the last section of our paper, we illustrate the theory with some examples and we formulate some conjectures.

2. Proofs and other results

We begin with some preliminary lemmas.

**Lemma 2.1.** If $x_0$ is an extreme cycle point then $x_0 \in \mathbb{Z}$, $x_0$ has a periodic base 4 expansion

$$x_0 = \frac{a_0}{4} + \frac{a_1}{4^2} + \cdots + \frac{a_{r-1}}{4^r} + \frac{a_0}{4^{r+1}} + \cdots + \frac{a_{r-1}}{4^{2r}} + \cdots,$$

with $a_k \in \{0, m\}$, and $0 \leq x_0 \leq \frac{m}{3}$. Hence

$$x_0 = \frac{4^{r-1} a_0 + 4^{r-2} a_1 + \cdots + 4 a_{r-2} + a_{r-1}}{4^r - 1}.$$

Moreover

$$\{x_0 : x_0 \text{ is an extreme cycle point} \} = X_L \cap \mathbb{Z},$$

where $X_L$ is the attractor of the iterated function system

$$\sigma_0(x) = \frac{x}{4}, \quad \sigma_m(x) = \frac{x + m}{4},$$

so

$$X_L = \cup_{l \in \{0,m\}} \sigma_l(X_L),$$

$$X_L = \left\{ \sum_{n=1}^{\infty} \frac{l_n}{4^n} : l_n \in \{0, m\} \text{ for all } n \in \mathbb{N} \right\}.$$  

**Proof.** Let $l_0, \ldots, l_{r-1}$ as in Definition 1.3. Then

$$x_0 = \frac{x_{r-1}}{4} + \frac{l_{r-1}}{4} = \frac{x_{r-2}}{4^2} + \frac{l_{r-2}}{4^2} + \frac{l_{r-1}}{4} = \cdots = \frac{x_0}{4^r} + \frac{l_0}{4^r} + \frac{l_1}{4^r} + \cdots + \frac{l_{r-1}}{4^r}.$$
Iterating this equality to infinity we obtain the base 4 decomposition of \( x_0 \). Also

\[
0 \leq x_0 \leq \sum_{k=1}^{\infty} \frac{m}{4^k} = \frac{m}{3}.
\]

From (2.1), using the triangle inequality we see that we must have \( e^{2\pi x_0} = 1 \) so \( x_0 \in \mathbb{Z}/2 \). If \( x_0 = (2m + 1)/2 \) with \( m \in \mathbb{Z} \) then \( x_1 = (x_0 + l_0)/2 = \frac{2m + 1 + 2l_0}{4} \), but since \( 2m + 1 + 2l_0 \) is odd it follows that \( x_1 \not\in \mathbb{Z}/2 \). This contradicts the fact that \( x_1 \) is also an extreme cycle point so it satisfies (2.1). Thus \( x_0 \in \mathbb{Z} \).

These statements show that \( x_0 \) is contained in \( X_L \cap \mathbb{Z} \). Conversely, if \( x_0 \in X_L \cap \mathbb{Z} \) then, if \( x_0 \in \sigma_0(X_L) \), we have that there exists \( x_{-1} \in X_L \) such that \( x_0 = \frac{x_{-1} + m}{4} \), and we get that \( x_{-1} = 4x_0 \in \mathbb{Z} \cap X_L \). If \( x_0 \in \sigma_m(X_L) \) then there exists \( x_{-1} \in X_L \) such that \( x_0 = \frac{x_{-1} + m}{4} \). Then \( x_{-1} = 4x_0 - m \equiv x_0(\text{mod } m) \). By induction, we obtain \( x_{-1}, x_{-2}, \ldots \) and digits \( d_0, d_1, \ldots \), in \( \{0, m\} \) such that \( x_{-i} = \frac{x_{-i} + d_i}{4} \). Moreover, \( x_0 \equiv 4^t x_{-1}(\text{mod } m) \). Since 4 is mutually prime with \( m \), it has a finite order \( a \) in the multiplicative group of invertible elements in \( U(\mathbb{Z}_m) \), so \( 4^a \equiv 1(\text{mod } m) \). Then \( x_0 \equiv x_{-a}(\text{mod } m) \). But since \( x_0 \) and \( x_{-a} \) are contained in \( X_L \subset [0, \frac{m}{4}] \), we get that \( x_0 = x_{-a} \) and thus \( x_0 \) is a point in an extreme cycle in \( X_L \cap \mathbb{Z} \).

\[\square\]

**Remark 2.2.** Using Lemma 2.1 one can develop an algorithm to determine the existence of non-trivial cycles. Take all the integers \( k \) between 1 and \( p/3 \). Define \( x = k \). If \( x \equiv 0 \text{mod } 4 \) then set \( x = x/4 \). If \( x + p \equiv 0 \text{mod } 4 \) then set \( x = (x + p)/4 \). If none of these two conditions are satisfied then move to \( k + 1 \). Do this as long as it is possible or until the point \( x \) that has already been checked. If such a point is reached then stop; there is a non-trivial extreme cycle. If not, move on to the next integer \( k + 1 \) and repeat these steps.

**Lemma 2.3.** Assume \( m > 3 \) is odd and \( x_j \) is an extreme cycle point for the digit set \( \{0, m\} \). Then \( x_j \equiv 0(\text{mod } 4) \) or \( x_j \equiv -m(\text{mod } 4) \).

**Proof.** We have

\[
x_{j+1} = \frac{x_j + l_j}{4},
\]

where \( l_j \in \{0, m\} \). Then

\[
4x_{j+1} = x_j + l_j.
\]

Considering the above modulo 4, we have

\[
0 \equiv x_j + m(\text{mod } 4)
\]

or

\[
0 \equiv x_j(\text{mod } 4).
\]

\[\square\]

**Lemma 2.4.** Let \( m > 3 \) be an odd number not divisible by 3 and \( x_t \) be the largest extreme cycle point in the non-trivial extreme cycle \( X \) for the digit set \( \{0, m\} \). Then \( x_t \) is divisible by 4.
Proof. Assume for contradiction’s sake that \( x_t \) is odd. Then, with Lemma 2.3, the next cycle point is
\[
\frac{x_t + m}{4}.
\]
Since \( x_t < m/3 \) we get that
\[
\frac{x_t + m}{4} > x_t.
\]
This is a contradiction to the maximality of \( x_t \).
Since \( x_t \) is not odd, it is divisible by 4 by the previous lemma.

We mention also a way to determine if a coset of the group \( G_m \) is an extreme cycle

**Proposition 2.5.** Assume \( m > 3 \) is odd. If a co-set \( C \) of \( G_m \) in \( U(\mathbb{Z}_m) \) has the property that for all \( x_j \in C, x_j < \frac{m}{2} \), then \( C \) is an extreme cycle for the digit set \( \{0, m\} \).

**Proof.** Let \( C \) be such a co-set. Label the elements in \( C \) such that \( x_j \equiv 4x_{j+1}(\mod m) \), and if \( a \) is the number of elements in \( G_m \), \( x_a-1 \equiv 4x_0(\mod m) \). Then, since \( 0 < x_{j+1} < \frac{m}{2} \), we have \( 0 < 4x_{j+1} < 2m \), so
\[
(2.7) \quad x_j = 4x_{j+1} - km,
\]
where \( k \in \{0, 1\} \), and similarly for \( x_0 \) and \( x_a-1 \). Rearranging, we find that
\[
(2.8) \quad \frac{x_j + l_j}{4} = x_{j+1},
\]
where \( l_j \in \{0, m\} \), and similarly for \( x_0 \) and \( x_a-1 \). Since \( C \) contains only integers, by Lemma 2.1, \( C \) is an extreme cycle.

**Proof of Proposition 1.2.** If \( m \) is incomplete, then by Theorem 1.4 there exists a non-trivial extreme cycle \( \{x_0, \ldots, x_r-1\} \) for the digits \( \{0, m\} \). Multiplying the relations in Definition 1.3 by \( k \) we see that \( \{kx_0, \ldots, kx_{r-1}\} \) is a cycle for the digits \( \{0, km\} \). With Lemma 2.1 we have that \( x_i \in \mathbb{Z} \), so \( kx_i \in \mathbb{Z} \) and therefore \( 1.4 \) is satisfied for the points \( kx_i \), and therefore we have a non-trivial extreme cycle for the digits \( \{0, km\} \).

**Proof of Theorem 1.4.** Assume for contradiction’s sake that \( m \) is incomplete. Then there is a non-trivial extreme cycle \( X = \{x_0, \ldots, x_r-1\} \) for the digit set \( \{0, m\} \). From the relation between the cycle points,
\[
(2.9) \quad x_{j+1} = \frac{x_j + b_j}{4},
\]
where \( b_j \in \{0, m\} \), we have that \( 4x_{j+1} \equiv x_j(\mod m) \). Thus,
\[
(2.10) \quad 4^{r-k}x_0 \equiv x_0(\mod m, k \in \{0, \ldots, r\}),
\]
so, for all \( k \in \mathbb{N} \), the number \( 4^kx_0 \) is congruent modulo \( m \) with an element of the extreme cycle \( X \). But then, the hypothesis, implies that there is a number \( c \in \{-1, 2, -2, 3\} \), the number \( cx_0 \) is congruent modulo \( m \) with an element in \( X \), and since \( x_0 \) is arbitrary in the cycle, we get that \( cx_j \) is congruent to an element in \( X \) for any \( j \).

In the following arguments we use the fact that since \( m \) is not divisible by 3, the condition on cycle points \( 0 < x_j < \frac{m}{3} \) implies \( 0 < x_j < \frac{m}{3} \).

If \( c = -1 \), then \( -x_0(\mod m) \in X \). Since \( 0 < x_0 < \frac{m}{3}, -x_0(\mod m) > \frac{m}{3} \), a contradiction.
If \( c = -2 \), then \(-2x_0 \pmod{m} \in X\). Since \(0 < x_0 < \frac{m}{3}\), \(-2x_0 \pmod{m} > \frac{m}{3}\), a contradiction.

If \( c = 2 \), then \(2x_j \pmod{m} \in X\) for all \(j\). Let \(x_N\) be the largest element of the extreme cycle. Since \(0 < x_N < \frac{m}{2}\), \(2x_N \pmod{m} = 2x_N\). This number is in \(X\), a contradiction to the maximality of \(x_N\).

If \( c = 3 \), then \(3x_j \pmod{m} \in X\) for all \(j\). Let \(x_N\) be the largest element of the extreme cycle. Since \(0 < x_N < \frac{m}{2}\), \(3x_N \pmod{m} = 3x_N\). This number is in \(X\), a contradiction to the maximality of \(x_N\).

\(\square\)

**Proof of Theorem 1.10.** Assume for contradiction’s sake that \(m\) is incomplete. Then there is a non-trivial extreme cycle \(X = \{x_0, \ldots, x_{r-1}\}\) for the digit set \(\{0, m\}\). As in the proof of Theorem 1.9, for all \(k \in \mathbb{N}\), the number \(4^k x_0\) is congruent modulo \(m\) with an element of the extreme cycle \(X\). But then, the hypothesis, implies that there is a number \(c \in \{5, 6, 7, 8, 9, 10, 11, 12\}\), the number \(cx_0\) is congruent modulo \(m\) with an element in \(X\), and since \(x_0\) is arbitrary in the cycle, we get that \(cx_j\) is congruent to an element in \(X\) for any \(j\).

In the following arguments we use the fact that since \(m\) is not divisible by 3, the condition on cycle points \(0 \leq x_j \leq \frac{m}{2}\) implies \(0 \leq x_j < \frac{m}{2}\). Let \(x_t\) be the largest element in the extreme cycle. We have

\[0 < x_t < \frac{m}{3} .\]

By the Lemma 2.4, \(x_t\) is divisible by four. Therefore, dividing by four, we get the next element in the extreme cycle, called \(x_N\), and we have

\[x_N < \frac{m}{12} .\]

For \(c \in \{5, 6, 7, 8, 9, 10, 11, 12\}\), \(x_t < cx_N < m\), so \(cx_N \pmod{m} = cx_N\) is a point in \(X\) bigger than \(x_t\), a contradiction to the maximality of \(x_t\).

\(\square\)

**Corollary 2.6.** For \(n \geq 1\) the numbers \(4^n + 1, 4^n - 3, 2 \cdot 4^n - 1\) and \(2 \cdot 4^n + 1\) are complete. For \(n \geq 3\), the numbers \(4^n - 5, 4^n - 7, 4^n - 9, 4^n - 11, 2 \cdot 4^n - 3, 2 \cdot 4^n - 5\) are complete.

**Proof.** If \( m = 4^n + 1 \) then \(4^n = -1 \pmod{m}\). Then use Theorem 1.9. Similarly for \(4^n - 3, 4^n - 5, 4^n - 7, 4^n - 9, 4^n - 11\) using also Theorem 1.10.

If \( m = 2 \cdot 4^n - 1 \), then \(4^{n+1} - 2 = 2(2 \cdot 4^n - 1)\) so \(4^{n+1} = 2 \pmod{m}\). Then use Theorem 1.9. Similarly for \(2 \cdot 4^n + 1, 2 \cdot 4^n - 3, 2 \cdot 4^n - 5\).

\(\square\)

**Proof of Theorem 1.11.** It is well known (see e.g. [IR90 page 45]), that the equation \(x^2 \equiv b \pmod{p^n}\) has 0 or two solutions. Let \(a\) be the smallest positive integer such that \(4^a \equiv 1 \pmod{p^n}\). If \(a\) is even, then we have \((4^{a/2})^2 \equiv 1 \pmod{p^n}\) so \(4^{a/2} \equiv \pm 1 \pmod{p^n}\). Since \(4^{a/2} \neq 1 \pmod{p^n}\) we get \(4^{a/2} \equiv -1 \pmod{p^n}\).

If \(a\) is odd, then \((4^{a+1})^2 \equiv 4 \pmod{p^n}\). Therefore \(4^{a+1} \equiv \pm 2 \pmod{p^n}\).

In both cases, the result follows from Theorem 1.9.

\(\square\)

**Remark 2.7.** The proof of Theorem 1.11 indicates that it is enough to have exactly two solutions for both equations \(x^2 \equiv 1 \pmod{m}\) and \(x^2 \equiv 4 \pmod{m}\), to obtain that \(m\) is complete. But the only odd numbers for which this condition holds are the prime powers. Indeed, if \(m = p_1^{n_1} \ldots p_r^{n_r}\), with \(r \geq 2\) and \(n_1, \ldots, n_r > 0\), then, by the Chinese Remainder Theorem, there exists an integer \(x\) such
that \( x \equiv -1 (\text{mod } p_1^{r_1}) \), \( x \equiv 1 (\text{mod } p_2^{r_2}) \), \ldots \( x \equiv 1 (\text{mod } p_n^{r_n}) \). This implies that \( x^2 \equiv 1 (\text{mod } p_k^{r_k}) \) for all \( k \), and therefore \( x^2 \equiv 1 (\text{mod } m) \). Also, it is clear that \( x \neq \pm 1 (\text{mod } m) \).

The next proposition gives us some information about the structure of extreme cycles for primitive numbers.

**Proposition 2.8.** Let \( m \) be a primitive number and let \( C = \{x_0, \ldots, x_{p-1}\} \) be an extreme cycle. Then:

(i) The length \( p \) of the cycle is equal to \( o_4(m) \).

(ii) Every element of the cycle \( x_i \) is mutually prime with \( m \).

(iii) The extreme cycle \( C \) is a coset of the group \( G_m \) in \( U(\mathbb{Z}_m) \), \( C = x_0G_m \).

**Proof.** Suppose \( x_0 \) and \( m \) have a common divisor \( d > 1 \). Then, since \( x_1 = \frac{x_0 + dm}{4} \) we have that \( 4x_1 \) is divisible by \( d \) and since \( d \) is odd it follows that \( d \) divides \( x_1 \). By induction \( d \) divides all elements of the cycle. But then \( \{x_0/d, x_1/d, \ldots, x_{p-1}/d\} \) is an extreme cycle for the digits \( \{0, m/d\} \). But this contradicts the fact that \( m \) is primitive.

We have \( 4x_i \equiv x_{i-j (\text{mod } p)} (\text{mod } m) \) for all \( i, j \in \{0, \ldots, p-1\} \). Therefore \( 4p x_0 \equiv x_0 (\text{mod } m) \).

Since \( x_0 \) is in \( U(\mathbb{Z}_m) \), we get that \( 4p \equiv 1 (\text{mod } m) \), so \( p \) divides \( o_4(m) =: a \). Also, we have \( x_0 \equiv 4^a x_0 \equiv x_{-a (\text{mod } p)} (\text{mod } m) \) so, since all the elements of the cycle are in \( \{0, m/3\} \) we get that \( x_0 = x_{-a (\text{mod } p)} \). Therefore \( a \) is divisible by \( p \). Thus \( p = a = o_4(m) \).

Since \( x_0G_m \) is the order of the group \( G \), and since \( 4x_0 \) (mod \( m \)) = \( x_{-j (\text{mod } p)} \), we get that \( x_0G_m = C \).

□

As we have seen in Proposition 2.8, the order of 4 in \( U(\mathbb{Z}_m) \) plays an important role in our investigation. We enumerate some properties of \( o_4(m) \) which will help us in our study.

**Proposition 2.9.** Let \( m \) and \( n \) be mutually prime odd integers. Then \( o_4(mn) = \text{lcm}(o_4(m), o_4(n)) \).

**Proof.** We have \( a = o_4(mn) \) is the smallest integer such that \( 4^a \equiv 1 (\text{mod } mn) \). So \( a \) is the smallest integer such that \( 4^a \equiv 1 (\text{mod } m) \) and \( 4^a \equiv 1 (\text{mod } n) \), which means that \( a \) is the smallest integer that is divisible by \( o_4(m) \) and \( o_4(n) \) so it is the lowest common multiple of these two numbers. □

**Proposition 2.10.** Let \( p \) be an odd prime number. Then \( o_4(p^k) = o_4(p) \) for \( k \leq \iota_4(p) \) and \( o_4(p^k) = \frac{p^{k-\iota_4(p)} o_4(m)}{o_4(p) o_4(m)} \) for all \( k \geq \iota_4(p) \).

**Proof.** For \( k \leq \iota_4(p) \), the statement is trivial. Assume by induction that, for \( k \geq \iota_4(p) \), \( a_k := o_4(p^k) = p^{k-\iota_4(p)} o_4(p) \) and \( o_4(p^k) < o_4(p^{k+1}) \). Then there exists \( q \) not divisible by \( p \) such that \( 4^{a_k} = 1 + qp^k \). Raise this to power \( p \) using the binomial formula:

\[
4^{pa_k} = 1 + p \cdot qp^k + q'p^{k+2},
\]

for some integer \( q' \). This implies that \( a_{k+1} = o_4(p^{k+1}) \) divides \( pa_k \) and also that \( pa_k \) is not \( o_4(p^{k+2}) \).

Since \( 4^{a_{k+1}} \equiv 1 (\text{mod } p^{k+1}) \) we have also \( 4^{a_{k+1}} \equiv 1 (\text{mod } p^k) \) so \( a_k \) divides \( a_{k+1} \). Thus \( a_{k+1} \) is a number that divides \( pa_k \) and is divisible by \( a_k \), and by the induction hypothesis \( a_{k+1} > a_k \). Thus \( a_{k+1} = pa_k = p^{k+1-\iota_4(p)} o_4(p) \). Also, \( o_4(p^{k+1}) = pa_k \neq o_4(p^{k+2}) \) so \( o_4(p^{k+1}) < o_4(p^{k+2}) \). Using induction we obtain the result. □
Proposition 2.11. Let $p_1, \ldots, p_r$ be distinct odd primes and $k_1, \ldots, k_r \geq 0$. For $i \in \{1, \ldots, r\}$, let $j_i \geq 0$ be the largest integer such that $p_i^{j_i}$ divides $\text{lcm}(o_4(p_1), \ldots, o_4(p_r))$. Then

\begin{equation}
(2.11) \quad o_4(p_1^{j_1} \cdots p_r^{j_r}) = \left( \prod_{i=1}^{r} p_i^{\max\{k_i - j_i - \ell_i(p_i), 0\}} \right) \text{lcm}(o_4(p_1), \ldots, o_4(p_r)).
\end{equation}

Proof. With Propositions 2.9 and 2.10, we have

If $k_i - \ell_i(p_i) \leq j_i$, then $p_i^{\max\{k_i - \ell_i(p_i), 0\}}$ already divides $\text{lcm}(o_4(p_1), \ldots, o_4(p_r))$, so it does not contribute to the right-hand side. If $k_i - \ell_i(p_i) > j_i$, then $p_i^{\max\{k_i - \ell_i(p_i), 0\}}$ contributes with $p_i^{k_i - \ell_i(p_i) - j_i}$ to the right-hand side. Then (2.11) follows. \hfill \Box

Proof of Theorem 7.4. Suppose there are only finitely many primitive numbers and let $m_1, \ldots, m_s$ be all the primitive numbers strictly bigger than 3. Let $n$ be a common multiple for the numbers $o_4(9), o_4(m_1), \ldots, o_4(m_s)$. Then

\[ 4^{n+1} - 1 \equiv 4 - 1 = 3 \pmod{9, \text{mod } m_1, \ldots, \text{mod } m_s}. \]

Let $m = \frac{4^n + 1}{3}$. We have that $m$ is not divisible by 3, $m_1, \ldots, m_s$, otherwise $4^{n+1} - 1$ is divisible by 9, $m_1, \ldots, m_s$. So $m$ is not divisible by any primitive number, therefore it must be complete.

On the other hand, in Lemma 2.1 let $r = n$, $a_{n-1} = a_{n-2} = a_{n-3} = m$, $a_0 = \cdots = a_{n-4} = 0$. We have

\[ x_0 = \frac{m(16 + 4 + 1)}{4^{n+1} - 1} = \frac{4^{n+1} - 1}{4} \cdot 21 = 7 \in X_L \cap \mathbb{Z}. \]

Thus $x_0$ is a non-trivial extreme cycle point, so $m$ cannot be complete. \hfill \Box

Proof of Lemma 1.14. Suppose that $ab$ is primitive. Since $a > 1$, $b$ is a proper divisor of $b$ so $b$ is complete. By Proposition 2.8, there exists an extreme cycle $C$ and it is equal to a coset $x_0G_{ab}$ of the multiplicative group generated by $4$ in $U(\mathbb{Z}_{ab})$. Consider the map $h : G_{ab} \to G_b$, $h(x) = x \pmod{b}$. Then, $h$ is a homomorphism and it is onto. Let $|G_{ab}| = o_4(ab) = M o_4(b) = M |G_b|$, so that $h$ is an $M$-to-1 map, where $M \geq \frac{2a+15}{12}$. Then the map $h' : x_0G_{ab} \to (x_0 \pmod{b})G_b$, $h'(x_0x) = (x_0x) \pmod{b}$, is also an $M$-to-1 map ($x_0$ is invertible in $\mathbb{Z}_{ab}^\times$ by Proposition 2.8, hence also in $\mathbb{Z}_b^\times$).

So, in particular, there are exactly $M$ elements in $x_0G_{ab}$ which are mapped into $x_0 \pmod{b}$. These elements can be written $x_0 \pmod{b} + kb \pmod{ab}$ for $M$ different values of $k$, each in the set $\{0, \ldots, a-1\}$. Since $b$ is complete, by Proposition 2.5, the coset $(x_0 \pmod{b})G_b$ contains an element $> \frac{b}{2}$. Therefore we can assume $y_0 := x_0 \pmod{b} > \frac{b}{2}$.

From Lemma 2.3, we know that the points in the cycle are congruent to 0 or $-ab$ modulo 4. So $y_0 + kb \equiv 0 \pmod{4}$ or $-ab \pmod{4}$, for all $M$ values of $k$ such that this point is in the extreme cycle. Since $b$ is odd, it has an inverse, $c$ in $\mathbb{Z}_b^\times$, and we have that $k \equiv -cy_0 \pmod{4}$ or $k \equiv c(-ab - y_0) \pmod{4}$. Therefore the values of $k$ here belong to only two equivalence classes modulo 4, so in each set $\{4n, 4n + 1, 4n + 2, 4n + 3\}$ there are at most 2 values of $k$. Therefore, if we take the largest such $k$, if $M$ is even, then $k \geq 4(\frac{M}{2} - 1) + 1 = 2M - 3$. If $M$ is odd, then the largest $k$ is at least
and this contradicts the fact that an extreme cycle is contained in \([0, \frac{ab}{3}]\), by Lemma 2.1.

\[4(\frac{M-1}{2} - 1) + 4 = 2M - 2.\] So in both cases \(k \geq 2M - 3\). Then

\[y_0 + kb > \frac{b}{2} + (2M - 3)b \geq \frac{ab}{3},\]

Proof of Theorem 1.18 Suppose there are some numbers \(k_1, \ldots, k_r \geq 0\) such that \(m = p_1^{k_1} \cdots p_r^{k_r}\) is not complete. Therefore, a divisor of this number has to be primitive, relabeling the powers \(k_i\), we can assume \(m\) is complete. If not, then it has to be divisible by some primitive number \(m\). Since \(m < 10^7\), we have that \(m' < 10^7\) so \(m'\) has to be one of the numbers in Table 1. Then the list of primes in the prime decomposition of \(m'\) is contained in the list of primes in the prime decomposition of \(m\), and this contradicts the hypothesis. Therefore \(m\) is complete.

\[\Box\]

Proof of Corollary 1.19 By Theorem 1.18 it is enough to check that \(m := p_1^{\ell_4(p_1) + j_1} \cdots p_r^{\ell_4(p_r) + j_r}\) is complete. If not, then it has to be divisible by some primitive number \(m'\). Since \(m < 10^7\), we have that \(m' < 10^7\) so \(m'\) has to be one of the numbers in Table 1. Then the list of primes in the prime decomposition of \(m'\) is contained in the list of primes in the prime decomposition of \(m\), and this contradicts the hypothesis. Therefore \(m\) is complete.

\[\Box\]

Lemma 2.12. The number of non-trivial cycle points for an odd number \(m\) not divisible by 3 is less than

\[\min_n \left\{ 2^n \left\lfloor \frac{m}{3 \cdot 4^n} \right\rfloor \right\} .\]

Proof. The phrasing in the statement of the above lemma, ”number of non-trivial cycle points,” refers to the total number of points among all non-trivial cycles.

We know from Lemma 2.11 that the cycle points are contained in the intersection of the attractor \(X_L\) with \(\mathbb{Z}\). Also \(X_L \subset [0, \frac{m}{3}]\). Therefore

\[X_L \subset \bigcup_{a_0, a_1, \ldots, a_{n-1} \in \{0, m\}} \sigma_{a_{n-1}} \cdots \sigma_{a_0} \left[0, \frac{m}{3}\right]\]

\[= \bigcup_{a_0, a_1, \ldots, a_{n-1} \in \{0, m\}} \left[\frac{a_0 + 3a_1 + \cdots + 4^{n-1}a_{n-1}}{4^n} \cdot \frac{m}{3 \cdot 4^n} + \frac{a_0 + 3a_1 + \cdots + 4^{n-1}a_{n-1}}{4^n}\right].\]

The intervals in this union can be written as

\[\left[\frac{m \sum_{k=0}^{n-1} l_k 4^k}{4^n}, \frac{m \left(1 + 3 \sum_{k=0}^{n-1} l_k 4^k\right)}{3 \cdot 4^n}\right],\]

with \(l_0, \ldots, l_{n-1} \in \{0, 1\}\).

Because \(m\) is not divisible by 3 or 4, the right endpoint is never an integer. Examining the left endpoint, we find

\[\sum_{k=0}^{n-1} l_k 4^k < 4^n,\]
and thus, since \( m \) is odd the left endpoint is an integer only if it is 0. Since the only cycle containing 0 is the trivial one, we have that the only non-trivial cycle points for \( m \) are the interior points of the above intervals; there are \( 2^n \) such intervals at each iteration, and each one contains at most \( \left\lfloor \frac{m}{3 \cdot 4^n} \right\rfloor \) integers in its interior.

\[\Box\]

**Proof of Lemma 1.13** We proceed as in the proof of Lemma 2.12. We take \( n = \left\lfloor \log_2 \sqrt{\frac{m}{3}} \right\rfloor \). Then \( \frac{ab}{3 \cdot 4^n} \leq b \), so the length of the intervals in (2.12) is at most \( b \). As we have seen in the proof of Lemma 2.12 the endpoints of these intervals cannot be non-trivial cycle points. If \( ab \) is primitive, then, by Proposition 2.8, there exists a cycle of length \( \frac{m}{3} \), by Proposition 2.8.

Now, as in the proof of Lemma 1.14 define the map \( h : x_0G_{ab} \to x_0G_b, \ x_0x \mapsto (x_0x)(\mod b) \).

We saw that this is an \( M \)-to-1 map, with \( M > 2^n \). Therefore there are \( M \) values of \( k \) such that \( x_0(\mod b) + kb \) is in the cycle \( C \). However, the intervals in (2.12) contain at most one such point, since their length is \( b \) and the endpoints are not extreme cycle points. We have \( 2^n < M \) such intervals, and this leads to a contradiction.

\[\Box\]

**Proof of Theorem 1.20** If \( m \) is primitive, then, by Proposition 2.8 there exists a cycle of length \( o_1(m) \). The contradiction follows from Lemma 2.12.

\[\Box\]

**Proof of Corollary 1.21** Let \( n = \left\lfloor \log_2 \sqrt{\frac{m}{3}} \right\rfloor \). Then \( 4^n \geq \frac{m}{3} \) so \( \left\lceil \frac{m}{3 \cdot 4^n} \right\rceil = 1 \). Furthermore,

\[
(2.14) \quad 2^n \left\lceil \frac{m}{3 \cdot 4^n} \right\rceil = 2^n \leq 2^{\log_2 \sqrt{\frac{4m}{3}}} = \sqrt{\frac{4m}{3}}.
\]

The rest follows from Theorem 1.20.

\[\Box\]

**Proof of Corollary 1.22** Suppose there exists \( k_1, \ldots, k_r \) such that \( p_1^{k_1} \cdots p_r^{k_r} \) is not complete. Then pick \( k_1, \ldots, k_r \) such that \( \sum_{i=1}^r k_i \) is as small as possible, with this property. Clearly, by (i) we can assume all \( k_i \geq 1 \). Then all the proper divisors of \( p_1^{k_1} \cdots p_r^{k_r} \) are complete. So \( m := p_1^{k_1} \cdots p_r^{k_r} \) is primitive. By Propositions 2.9 and 2.10 we have

\[
o_4(m) = \lcm(o_4(p_1^{k_1}), \ldots, o_4(p_r^{k_r})) = \lcm(p_1^{k_1-1}o_4(p_1), \ldots, p_r^{k_r-1}o_4(p_r)) = p_1^{k_1-1} \cdots p_r^{k_r-1} \lcm(o_4(p_1), \ldots, o_4(p_r)).
\]

From (iii), we get

\[
p_1^{k_1-1} \cdots p_r^{k_r-1} \lcm(o_4(p_1), \ldots, o_4(p_r)) > 2^n \left\lceil \frac{p_1 \cdots p_r}{3 \cdot 4^n} \right\rceil \geq 2^n \left\lceil \frac{p_1 \cdots p_r}{3 \cdot 4^n} \right\rceil.
\]

(we used the fact that for \( a > 0, N \in \mathbb{N}, \left\lfloor a \right\rfloor N \) is an integer \( \geq aN \), so it is bigger than \( aN \)). Since \( m \) is primitive, Corollary 1.21 gives us a contradiction.

\[\Box\]

**Corollary 2.13.** Let \( p_1, \ldots, p_r \) be distinct simple prime numbers strictly larger than 3. Assume the following conditions are satisfied:

(i) None of the numbers \( o_4(p_1), \ldots, o_4(p_r) \) is divisible by any of the numbers \( p_1, \ldots, p_r \).

(ii) For any subset \( \{i_1, \ldots, i_s\} \) of \( \{1, \ldots, r\} \), with \( s \geq 2 \) the following inequality holds:

\[
(2.15) \quad \lcm(o_4(p_{i_1}), \ldots, o_4(p_{i_s})) > \sqrt[4]{\frac{4}{3}p_{i_1} \cdots p_{i_s}}.
\]
Then the number \( p_{k_1}^{r_{k_1}} \cdots p_{k_r}^{r_r} \) is complete for any \( k_1 \geq 0, \ldots, k_r \geq 0 \).

**Proof.** We proceed by induction on \( r \). Theorem 1.11 shows that we have the result for \( r = 1 \). Assume, the result holds for \( r - 1 \) primes. Then the conditions (i),(ii) in Corollary 1.22 are satisfied and we check condition (iii). Let \( m := p_1 \cdots p_r \).

We have:

\[
\sqrt{\frac{4m}{3}} < o_4(m).
\]

Thus condition (iii) is satisfied and Corollary 1.22 gives us the result. \( \square \)

**Proof of Corollary 1.23.** We use Corollary 2.13. For any subset \( \{i_1, \ldots, i_s\} \) of \( \{1, \ldots, r\} \) with \( s \geq 2 \) we have

\[
o_4(p_{i_1}) \cdots o_4(p_{i_s}) > \sqrt{\frac{4}{3} p_{i_1} \cdots \sqrt{\frac{4}{3} p_{i_s}}} \geq \sqrt{\frac{4}{3} p_{i_1} \cdots p_{i_s}}.
\]

\( \square \)

**Proof of Corollary 1.24.** Since \( p \) does not divide \( a \), \( p^k \) is prime with \( a \). With Propositions 2.9, 2.10 we have

\[
o_4(p^k a) = p^{k-1} o_4(p) o_4(b).
\]

Also we have, for \( k \geq 2 \), since \( p \geq 5 \),

\[
[\log_2 \sqrt{\frac{p}{3}}] + \log_2 p^{k-1} \geq [\log_2 \sqrt{\frac{p}{3}}] + \log_2 p^{k-1} + 1 \geq [\log_2 \sqrt{\frac{p}{3}}] + [\log_2 p^{k-1}]
\]

\[
\geq [\log_2 \sqrt{\frac{p}{3}} + \log_2 p^{k-1}] = [\log_2 \sqrt{\frac{p^k}{3}}].
\]

Therefore,

\[
p^{k-1} o_4(p) > 2^{[\log_2 \sqrt{\frac{p^k}{3}}]},
\]

for \( k \geq 2 \) and also, from the hypothesis , for \( k = 1 \). By Lemma 1.15 \( p^k a \) cannot be primitive, for \( k \geq 1 \) and, because \( a \) is complete and \( p \) is prime, this means that \( p^k a \) is complete.

Note that \( \frac{p^{k-1}}{2} \geq 2^{[\log_2 \sqrt{\frac{p^k}{3}}]} \) for \( p > 5 \), so this is indeed a peculiar case. \( \square \)

**Corollary 2.14.** Let \( m \) be an odd number. If the index \( x \) of \( G_m \) in \( U(\mathbb{Z}_m) \) satisfies \( \frac{\phi(m)}{\sqrt{\frac{4}{3} m}} > x \), where \( \phi \) is Euler’s totient function, then \( m \) is not primitive.

**Proof.** We have \( o_4(m) = |G_m| \) and \( \phi(m) = |U(\mathbb{Z}_m)|. \) Thus, from

\[
o_4(m) = \frac{|U(\mathbb{Z}_m)|}{x} = \frac{\phi(m)}{x} > \sqrt{\frac{4}{3} m}.
\]

The result follows from Corollary 1.21. \( \square \)
Table 2. The primes less than 1049 and their $o_4$.

| $p$ | $o_4(p)$ | $p$ | $o_4(p)$ | $p$ | $o_4(p)$ | $p$ | $o_4(p)$ | $p$ | $o_4(p)$ |
|-----|----------|-----|----------|-----|----------|-----|----------|-----|----------|
| 3   | 1        | 5   | 2        | 7   | 3        | 11  | 5        | 13  | 6        |
| 5   | 2        | 7   | 3        | 11  | 5        | 13  | 6        | 17  | 4        |
| 7   | 3        | 11  | 5        | 13  | 6        | 17  | 4        | 19  | 9        |
| 11  | 5        | 13  | 6        | 17  | 4        | 19  | 9        | 23  | 11       |
| 13  | 6        | 17  | 4        | 19  | 9        | 23  | 11       | 29  | 14       |
| 17  | 4        | 19  | 9        | 23  | 11       | 29  | 14       | 31  | 5        |
| 19  | 9        | 23  | 11       | 29  | 14       | 31  | 5        | 37  | 18       |
| 23  | 11       | 29  | 14       | 31  | 5        | 37  | 18       | 41  | 10       |
| 29  | 14       | 31  | 5        | 37  | 18       | 41  | 10       | 43  | 7        |
| 31  | 5        | 37  | 18       | 41  | 10       | 43  | 7        | 47  | 23       |
| 37  | 18       | 41  | 10       | 43  | 7        | 47  | 23       | 53  | 26       |
| 41  | 10       | 43  | 7        | 47  | 23       | 53  | 26       | 59  | 29       |
| 43  | 7        | 47  | 23       | 53  | 26       | 59  | 29       | 61  | 30       |
| 47  | 23       | 53  | 26       | 59  | 29       | 61  | 30       | 67  | 33       |
| 53  | 26       | 59  | 29       | 61  | 30       | 67  | 33       | 71  | 35       |
| 59  | 29       | 61  | 30       | 67  | 33       | 71  | 35       | 73  | 9        |
| 61  | 30       | 67  | 33       | 71  | 35       | 73  | 9        | 79  | 39       |
| 67  | 33       | 71  | 35       | 73  | 9        | 79  | 39       | 83  | 41       |
| 71  | 35       | 73  | 9        | 79  | 39       | 83  | 41       | 89  | 11       |
| 73  | 9        | 79  | 39       | 83  | 41       | 89  | 11       | 97  | 24       |
| 79  | 39       | 83  | 41       | 89  | 11       | 97  | 24       | 101 | 50       |

3. Examples

Example 3.1. We want to prove that $5^k \cdot 7^l$ is complete for any $k, l$. We have $o_4(5) = 2$, $o_4(7) = 3$ so

$$\operatorname{lcm}(o_4(5), o_4(7)) = 6 > 2\left\lceil \log_2 \sqrt{\frac{35}{3}} \right\rceil = 4.$$ 

Since 5 and 7 are simple primes, the result follows immediately from Corollary 1.22.

Example 3.2. Let us prove that $5^k \cdot 19^l$ is complete for any $k, l$. We have that $5^k$ is complete and $o_4(19) = 9 = \frac{19-1}{2}$ is prime with $o_4(5) = 2$. So Corollary 1.24 applies. The same argument applies to show that $7^k \cdot 11^l$ are complete. We can use this argument also for $7^k \cdot 11^l \cdot 23^m$, but we have to start with $17^k$, since $o_4(17) = 4$. Then $17^m \cdot 7^k$ is complete and $17^m \cdot 7^k \cdot 11^l$ is complete.

Example 3.3. Let us check that $5^k \cdot 11^l$ is complete for any $k, l$. We have $o_4(5) = 2$, $o_4(11) = 5$. We have a small problem since $o_4(11)$ is divisible by 5, which is one of the primes. In Theorem 1.18 or Corollary 1.19 we have $t_4(5) = 1$, $t_4(11) = 1$, $\operatorname{lcm}(o_4(5), o_4(11)) = 10$, so $j_1$, the largest power of 5
that divides the lcm 10, is 1, and \( j_2 = 0 \). So we have to check that \( 5^2 \cdot 11 \) is complete, or that it does not contain any of the lists in the second column of Table \([1]\). And that is clear.

We could also try to use Theorem \([1.20]\) or Corollary \([1.21]\). For that, since we know that 5 and 11 are complete (because they are prime), we have to check that \( 5 \cdot 11 \) and \( 5^2 \cdot 11 \) are not primitive. We can use Corollary \([1.21]\) to check that \( 5 \cdot 11 \) is complete

\[
o_4(5 \cdot 11) = \text{lcm}(o_4(5), o_4(11)) = 10 > 2^{\lceil \log_2 \sqrt{\frac{5 \cdot 11}{3}} \rceil} = 8.
\]

However, we cannot use this for \( 5^2 \cdot 11 \), because

\[
o_4(5^2 \cdot 11) = 10 < 2^{\lceil \log_2 \sqrt{\frac{5 \cdot 11}{3}} \rceil} = 16.
\]

The minimum in Theorem \([1.20]\) gives the same value, 16.

Looking at Table \([1]\) we formulate the following conjecture:

**Conjecture 3.4.** Let \( m \) be a primitive number. Then

(i) \( m \) is square-free.

(ii) If \( m = p_1 \ldots p_r \) is the prime decomposition of \( m \), then there exists \( i \) such that

\[
\text{lcm}(o_4(p_1), \ldots, o_4(p_r)) = o_4(p_i).
\]

A weaker conjecture is the following:

**Conjecture 3.5.** Let \( m \) be an odd number not divisible by 3 and let \( m = p_1^{k_1} \ldots p_r^{k_r} \) be its prime decomposition. If the numbers \( o_4(p_1), \ldots, o_4(p_r), p_1, \ldots, p_r \) are mutually prime then \( m \) is complete.

It is easy to see that Conjecture 3.4 implies Conjecture 3.5 for if \( m \) is not complete, then it is divisible by some primitive number, and by Conjecture 3.4 the orders cannot be mutually prime.

**Acknowledgements.** This work was partially supported by a grant from the Simons Foundation (#228539 to Dorin Dutkay).

**References**

[DHL13] Xin-Rong Dai, Xing-Gang He, and Chun-Kit Lai. Spectral property of Cantor measures with consecutive digits. *Adv. Math.*, 242:187–208, 2013.

[DHS09] Dorin Ervin Dutkay, Deguang Han, and Qiyu Sun. On the spectra of a Cantor measure. *Adv. Math.*, 221(1):251–276, 2009.

[DJ06] Dorin Ervin Dutkay and Palle E. T. Jorgensen. Iterated function systems, Ruelle operators, and invariant projective measures. *Math. Comp.*, 75(256):1931–1970 (electronic), 2006.

[DJ09] Dorin Ervin Dutkay and Palle E. T. Jorgensen. Fourier duality for fractal measures with affine scales. preprint, 2009.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[JKS12] Palle E. T. Jorgensen, Keri A. Kornelson, and Karen L. Shuman. An operator-fractal. *Numer. Funct. Anal. Optim.*, 33(7-9):1070–1094, 2012.

[JKS14] Palle E. T. Jorgensen, Keri A. Kornelson, and Karen L. Shuman. Scalar spectral measures associated with an operator-fractal. *J. Math. Phys.*, 55(2):022103, 23, 2014.

[JP98] Palle E. T. Jorgensen and Steen Pedersen. Dense analytic subspaces in fractal \( L^2 \)-spaces. *J. Anal. Math.*, 75:185–228, 1998.

[LW02] Izabella Laba and Yang Wang. On spectral Cantor measures. *J. Funct. Anal.*, 193(2):409–420, 2002.

[Str00] Robert S. Strichartz. Mock Fourier series and transforms associated with certain Cantor measures. *J. Anal. Math.*, 81:209–238, 2000.
[Str06] Robert S. Strichartz. Convergence of mock Fourier series. *J. Anal. Math.*, 99:333–353, 2006.

[Dorin Ervin Dutkay] University of Central Florida, Department of Mathematics, 4000 Central Florida Blvd., P.O. Box 161364, Orlando, FL 32816-1364, U.S.A.,
*E-mail address*: Dorin.Dutkay@ucf.edu

[John Haussermann] University of Central Florida, Department of Mathematics, 4000 Central Florida Blvd., P.O. Box 161364, Orlando, FL 32816-1364, U.S.A.,
*E-mail address*: jhaussermann@knights.ucf.edu