RATIONAL POINTS IN CANTOR SETS

Judit Nagy
Dept. of Analysis of Eötvös Lorand University, Kecskemeti u. 10-12, 1053 Budapest, Hungary
e-mail: nmm@cs.elte.hu
(Submitted April 1999-Final Revision December 1999)

1. INTRODUCTION

The idea for this article was given by a problem in real analysis. We wanted to determine the one-dimensional Lebesgue-measure of the set $f^{-1}(C)$, where C stands for the classical triadic Cantor set and f is the Cantor-function, which is also known as "devil's staircase." We could see immediately that to determine the above measure we needed to know which dyadic rationals were contained in C. We soon found that the solution is well known; namely, there are only two such fractions: $\frac{1}{4}$ and $\frac{3}{4}$. This inspired a question: Are there any other primes such that only finitely many fractions are contained in the classical triadic Cantor set, where the denominator is a power of p? The aim of this paper is to verify the surprising result: every $p \neq 3$ prime fulfills the condition. Charles R. Wall showed in [2] that the Cantor set contains only 14 terminating decimals. His article gave very important information regarding the proof. We may ask if the quality of containing "very few" rational numbers and that of having zero Lebesgue measure are in close connection for a Cantor set. The answer seems to be "yes" at first sight, but in [1] Duane Boes, Richard Darst, and Paul Erdös showed a symmetric Cantor set family which, for each $\lambda \in [0, 1]$, has a member of Lebesgue measure $1-\lambda$, but the sets of the family typically do not contain "any" rational numbers.

2. DEFINITIONS, NOTATIONS, AND LEMMAS

Definition 1: Let n be a positive integer and m a positive integer relatively prime to n. The order of n modulo m is the smallest positive exponent g such that $n^g \equiv 1 \pmod{m}$.

Notation 1: Since our proofs require only the case $n = 3$, for the reason of simplicity we omit n and denote the order of 3 modulo m by $\text{ord}(m)$.

Lemma 1: If l and m are relatively prime to 3 and l divides m, then $\text{ord}(l)$ divides $\text{ord}(m)$.

Proof: This follows immediately from the definition of the order. □

Lemma 2: Let $p > 3$ be prime and $\text{ord}(p) = d$. If $\text{ord}(p^b) = d$ for an integer b, then $\text{ord}(p^{b+1})$ either equals d, or p divides $\text{ord}(p^{b+1})$.

Proof: (We denote a divides b in the usual way by $a|b$ and denote a does not divide b by $a \nmid b$.) We observe that $d|p-1$. It is enough to verify that if $p \nmid \text{ord}(p^{b+1})$ then $\text{ord}(p^{b+1}) = d$.

It is well known that if m is relatively prime to 3 then $\text{ord}(m)$ divides $\phi(m)$, where ϕ is Euler's function; hence, $\text{ord}(p^{b+1}) | \phi(p^{b+1}) = (p-1) \cdot p^b$ and, furthermore, $\text{ord}(p^{b+1}) | p-1$, since $p \nmid \text{ord}(p^{b+1})$.

From Lemma 1, it follows that $d | \text{ord}(p^{b+1})$; hence, there exists a positive integer t such that $\text{ord}(p^{b+1}) = d \cdot t$.

Now, $3^d \equiv 1 \pmod{p^b}$ gives $3^{d\cdot p} \equiv 1 \pmod{p^{b+1}}$, which implies that $d\cdot t \mid d\cdot p$. But, since $d\cdot t$ divides both $p-1$ and $d\cdot p$, it also divides their greatest common divisor d. Therefore $t=1$, which completes the proof. □

Lemma 3: Let $p>3$ be a prime. If $\text{ord}(p)=d$, then there exists a unique positive integer n, for which $\text{ord}(p^k)=d$ whenever $1\le k\le n$ and $\text{ord}(p^{n+t})=d\cdot p^t$ whenever t is a positive integer.

Proof: By Lemma 1 and Lemma 2, there exists a maximal exponent n such that $\text{ord}(p^n)=d$. We use mathematical induction on t.

Let $t=1$. We show that $\text{ord}(p^{n+1})=d\cdot p$.

From $3^d \equiv 1 \pmod{p^n}$, it follows that $3^{d\cdot p} \equiv 1 \pmod{p^{n+1}}$; hence, $\text{ord}(p^{n+1}) \mid d\cdot p$. On the other hand, using the first two lemmas, $d \mid \text{ord}(p^{n+1})$ and $p \mid \text{ord}(p^{n+1})$; therefore, $d\cdot p \mid \text{ord}(p^{n+1})$. Next, supposing $\text{ord}(p^{n+t})=d\cdot p^t$, we prove that $\text{ord}(p^{n+t+1}) \mid d\cdot p^{t+1}$ for any positive integer t.

1. Let y denote $3^{d\cdot p^t}$. Then

$$3^{d\cdot p^{t+1}} - 1 = (3^{d\cdot p^t})^p - 1 = y^p - 1 = A\cdot B, \tag{1}$$

where $A=y-1$ and $B=y^{p-1}+y^{p-2}+\cdots+y+1$. From $y\equiv 1 \pmod{p^{n+t}}$, it follows that $p^{n+t}\mid A$ and $p\mid B$, since $y\equiv 1 \pmod{p}$. Thus, $3^{d\cdot p^{t+1}} \equiv 1 \pmod{p^{n+t+1}}$, which implies $\text{ord}(p^{n+t+1}) \mid d\cdot p^{t+1}$

2. Next, we prove $d\cdot p^{t+1} \mid \text{ord}(p^{n+t+1})$. First, $d\cdot p^t \mid \text{ord}(p^{n+t+1})$ and $\text{ord}(p^{n+t+1}) \mid d\cdot p^{t+1}$ by Lemma 1 and the previous result. So $\text{ord}(p^{n+t+1})$ can only be $d\cdot p^t$ or $d\cdot p^{t+1}$.

We now show that $d\cdot p^t$ is impossible, that is, $p^{n+t+1} \nmid 3^{d\cdot p^t}-1$. Let z denote $3^{d\cdot p^{t-1}}$. Then

$$3^{d\cdot p^t} - 1 = (3^{d\cdot p^{t-1}})^p - 1 = z^p - 1 = A_*\cdot B_*, \tag{2}$$

where $A_*=z-1$ and $B_*=z^{p-1}+z^{p-2}+\cdots+z+1$. From the condition $\text{ord}(p^{n+t})=d\cdot p^t$ follows $p^{n+t}\nmid A_*$, so it is enough to show that $p^2 \nmid B_*$. To obtain this, we write B_*-p as a product:

$$\begin{aligned} B_*-p &= (z^{p-1}-1)+(z^{p-2}-1)+(z^{p-3}-1)+\cdots+(z-1) \\ &= (z-1)\cdot(z^{p-2}+2\cdot z^{p-3}+\cdots+(p-2)\cdot z+(p-1)). \end{aligned}$$

We have $z\equiv 1 \pmod{p}$ and thus $z^{p-2}+2\cdot z^{p-2}+\cdots+(p-2)\cdot z+(p-1) \equiv (1+2+\cdots+p-1) \pmod{p}$. Since $1+2+\cdots+p-1 = p\cdot\frac{p-1}{2}$ and $\frac{p-1}{2}$ is an integer, we obtain

$$p \mid z^{p-2}+2\cdot z^{p-2}+\cdots+(p-2)\cdot z+(p-1). \tag{3}$$

On the other hand, we have $p\mid z-1$; hence, $p^2 \mid B_*-p$. Then p^2 cannot divide B_*. □

Notation 2: Given a positive integer L relatively prime to 3, let

$$N(L)=\{K : 1\le K\le L-1 \text{ and } (K,L)=1\}. \tag{4}$$

Remark 1: Observe that $N(L)$ consists of all the possible numerators of simplified fractions in $[0,1]$ with denominator L. It is also clear that $N(L)$ has exactly $\phi(L)$ many elements. Recall from Charles Wall's article [2] that $N(L)$ decomposes into $\frac{\phi(L)}{\text{ord}(L)}$ equivalence classes, each of which has $\text{ord}(L)$ many elements. These can be written in the form

$$[k(L)] = \{k, k\cdot 3, \ldots, k\cdot 3^{\text{ord}(L)-1} : \bmod L\}, \tag{5}$$

where k is an element of $N(L)$.

Definition 2: We call the $[k(L)]$ equivalence classes briefly the classes of $N(L)$.

Remark 2: In addition, we recall that, for each $k \in N(L)$, either all the elements of a $[k(L)]$ class, or none of them, are numerators of fractions in the Cantor set, so it is enough to find a $k' \in [k(L)]$ such that $\frac{k'}{L} \notin C$, that is, $\frac{k'}{L}$ was eliminated during the construction of the Cantor set. This guarantees that all the elements of $[k(L)]$ are numerators of eliminated fractions.

Definition 3: We call the class $[k(L)]$ "eliminated" if there exists a $k' \in [k(L)]$ such that $\frac{k'}{L} \notin C$.

Remark 3: Now, let n be the positive integer determined in Lemma 3. Then $N(p^n)$ has

$$\frac{\phi(p^n)}{\text{ord}(p^n)} = \frac{(p-1)\cdot p^{n-1}}{d}$$

classes and, for each positive integer t, the set $N(p^{n+t})$ has

$$\frac{\phi(p^{n+t})}{\text{ord}(p^{n+t})} = \frac{(p-1)\cdot p^{n+t-1}}{d\cdot p^t} = \frac{(p-1)\cdot p^{n-1}}{d}$$

classes.

3. THE MAIN RESULTS

Theorem 1: Let $p > 3$ be a prime such that 3 is a primitive root modulo p^2. Then there are no fractions $\frac{a}{b} \in C$ (where a and b are relatively prime numbers) such that b is a power of p.

Proof: First, $\text{ord}(p^2) = p\cdot(p-1)$ immediately implies $\text{ord}(p) = p-1$. Thus, Lemma 3 with $d = p-1$ gives $n = 1$, so $\text{ord}(p^{t+1}) = (p-1)\cdot p^t$ for each positive integer t. Then $\phi(p^t) = \text{ord}(p^t)$, so $N(p^t)$ consists of one class, for example, $N(p^t) = [1(p^t)]$. Therefore, $N(p^t)$ has $(p-1)\cdot p^{t-1}$ elements and, for each prime $p > 3$ and positive integer t,

$$(p-1)\cdot p^{t-1} > 2\cdot\left[\frac{p^t}{3}\right], \tag{6}$$

$\left(\text{where } \left[\frac{p^t}{3}\right] \text{ denotes the integer part of the real number } \frac{p^t}{3}\right)$. Thus, there exists an $i \in [1(p^t)]$ such that $\frac{1}{3} < \frac{i}{p^t} < \frac{2}{3}$, hence, $N(p^t)$ is eliminated. □

Next, we show that if n is the largest integer for which $\text{ord}(p) = \text{ord}(p^n)$ then n is also the largest exponent such that the n^{th} power of p can be the denominator of a fraction in C.

Theorem 2: For each prime $p > 3$, there are finitely many fractions $\frac{a}{b} \in C$ such that b is a power of p.

Proof: Let $k \in N(p^{n+t})$ for any positive integer t. We show that $[k(p^{n+t})]$ is eliminated. Suppose

$$[k(p^{n+t-1})] = \{x_1, \ldots, x_{\text{ord}(p^{n+t-1})}\}. \tag{7}$$

Then

$$[k(p^{n+t})] = \{x_i + j\cdot p^{n+t-1} : i = 1, \ldots, \text{ord}(p^{n+t-1}),\ j = 0, 1, \ldots, p-1\}. \tag{8}$$

This can be seen easily concerning the following. For each number of the form $k \cdot 3^y$, there exists a $1 \le i \le \text{ord}(p^{n+t-1})$ such that $k \cdot 3^y \equiv x_i \pmod{p^{n+t-1}}$. Hence, there is a $j \in \{0, 1, \ldots, p-1\}$ such that $k \cdot 3^y \equiv x_i + j \cdot p^{n+t-1} \pmod{p^{n+t}}$. This implies

$$[k(p^{n+t})] \subseteq \{x_i + j \cdot p^{n+t-1} : i = 1, \ldots, \text{ord}(p^{n+t-1}),\ j = 0, 1, \ldots, p-1\}. \tag{9}$$

On the other hand, the two sets have the same number of elements, so they are equal.

What does this mean?

Take any element x_i of $[k(p^{n+t-1})]$ and observe the situation of the fractions

$$\frac{x_i}{p^{n+t}} < \frac{x_i + p^{n+t-1}}{p^{n+t}} < \frac{x_i + 2 \cdot p^{n+t-1}}{p^{n+t}} < \cdots < \frac{x_i + (p-1) \cdot p^{n+t-1}}{p^{n+t}} \tag{10}$$

in the interval [0, 1]. Writing them, respectively, in the form

$$\frac{x_i}{p^{n+t}} < \frac{x_i}{p^{n+t}} + \frac{1}{p} < \frac{x_i}{p^{n+t}} + \frac{2}{p} < \cdots < \frac{x_i}{p^{n+t}} + \frac{p-1}{p}, \tag{11}$$

we can see that the difference of each neighboring fraction is $\frac{1}{p}$ and, as $p > 3$, there must be at least one of them in the middle open third of [0, 1]. Therefore, $[k(p^{n+t})]$ is eliminated. □

REFERENCES

1. D. Boes, R. Darst, & P. Erdös. "Fat, Symmetric, Irrational Cantor Sets." *Amer. Math. Monthly* **88.5** (1981):340-41.
2. C. R. Wall. "Terminating Decimals in the Cantor Ternary Set." *The Fibonacci Quarterly* **28.2** (1990):98-101.
3. Solution to Problem H-339. *The Fibonacci Quarterly* **21.3** (1983):239.

AMS Classification Numbers: 11A41, 28A80

❖❖❖