Fractal projections and a number theory question

Alan Chang

Mathcamp 2021 Week 5

Contents

1 Introduction

1.1 Course blurb

Let $K_0 \subset \mathbb{R}^2$ be the unit square. Divide K_0 into 16 squares of equal size, and let $K_1 \subset K_0$ be the union of the four corner squares. Repeat the same procedure on each of the four squares of K_1 to get K_2 (a union of 16 squares), and so on. We define the four corner Cantor set to be the limit set $K = \bigcap_{n=0}^{\infty} K_n$.

In this class, we will discuss some interesting properties of the projections of the four corner Cantor set, including connections to the following number theory fact: If m and n are odd integers, then m/n can be written as the ratio of two numbers of the form $\sum_{j=0}^{\ell} \varepsilon_j 4^j$, where $\varepsilon_j \in \{-1, 0, 1\}$. (Incidentally, this number theory fact is proved in a paper called "An awful problem about integers in base four.")

1.2 References

1. J.H. Loxton, A.J. van der Poorten, *An awful problem about integers in base four.* Acta Arith., 49 (1987), pp. 193-203

2. Mattila's *Fourier analysis and Hausdorff dimension*, Chapter 10

3. Bishop–Peres's *Fractals in probability and analysis*, Chapter 9

1.3 Guide for these notes

For the exercises, here is the difficulty scale:

- : easy
- : medium
- : hard

The words "easy," "medium," and "hard" are not well-defined. Don't be afraid of difficult problems! It's by struggling with these exercises that you really learn.

Things labeled "Fun fact" are not needed for the class.

2 Day 1

2.1 Introduction

In this class, we will begin with a question in *fractal geometry* about projections of fractals. That will lead us to a *number theory* question. To solve that question, we will use *Fourier analysis on cyclic groups* (or if you prefer, generating functions and roots of unity). Because of time, I won't be able to prove everything that I state. Instead, the plan of this class is to show how these topics are related.

2.2 Projections

First we introduce some notation from additive combinatorics.

Definition 2.1. Let $A, B \subset \mathbb{R}$ and let $\alpha \in \mathbb{R}$. We define the sum-set $A + B$ and the dilate αA as follows:

$$A + B = \{a + b : a \in A, b \in B\} \tag{2.1}$$

$$\alpha A = \{\alpha a : a \in A\} \tag{2.2}$$

Remark 2.2. Note that in general, $A + A \neq 2A$.

Now we define projection.

Definition 2.3. For $\alpha \in \mathbb{R}$, we define $\operatorname{proj}_\alpha : \mathbb{R}^2 \to \mathbb{R}$ by $\operatorname{proj}_\alpha(x, y) = x + \alpha y$. We refer to α as the *direction* of the projection $\operatorname{proj}_\alpha$.

(For this paragraph, it helps to draw a picture!) Here is a geometric interpretation. Imagine the x-axis is the "ground." Suppose the "sun" is "infinitely far away," so its rays are all parallel to each other. If the slope of the of the rays is $-1/\alpha$, then the point (x, y) casts a shadow on the point $(x + \alpha y, 0)$ on the x-axis. The x-coordinate of this is precisely $\operatorname{proj}_\alpha(x, y)$.

For $S \subset \mathbb{R}^2$,

$$\operatorname{proj}_\alpha S = \{x + \alpha y : (x, y) \in S\} \tag{2.3}$$

Note that if S is a subset of the upper-half plane, its shadow (as desribed above) on the x-axis is $\operatorname{proj}_\alpha S$.

Example 2.4. $S = A \times B$, then its projection is $\operatorname{proj}_\alpha S = A + \alpha B = \{a + \alpha b : a \in A, b \in B\}$.

Remark 2.5. The projections we have described geometrically above are not orthogonal projections, but they are parallel projections.

2.3 The middle-half Cantor set

Let $C_0 = [0,1]$. To form C_1, remove the middle half of C_0. Now C_2 is the union of two intervals of length 1/4. To form C_2, remove the middle half of each interval of C_1. Repeat this way to construct C_n for all $n \in \mathbb{N}_0$. ($\mathbb{N}_0 = \{0, 1, 2, \ldots\}$.) For example

$$C_0 = [0,1] \tag{2.4}$$

$$C_1 = [\tfrac{0}{4}, \tfrac{1}{4}] \cup [\tfrac{3}{4}, \tfrac{4}{4}] \tag{2.5}$$

$$C_2 = [\tfrac{0}{16}, \tfrac{1}{16}] \cup [\tfrac{3}{16}, \tfrac{4}{16}] \cup [\tfrac{12}{16}, \tfrac{13}{16}] \cup [\tfrac{15}{16}, \tfrac{16}{16}] \tag{2.6}$$

Define the *middle-half Cantor set* to be $C = \bigcap_{n=0}^{\infty} C_n$. (In other words, $x \in C$ if and only if $\forall n \in \mathbb{N}_0, x \in C_n$.) Another way to describe C is

$$C = \{x \in [0,1] : x \text{ has a base 4 expansion with only 0s and 3s}\}. \tag{2.7}$$

We will often refer to C as just the "Cantor set" since we are not considering other types of Cantor sets.

Example 2.6. Here are some examples:

1. $\frac{3}{4} = 0.3_4$, so $\frac{3}{4} \in C$.

2. $\frac{1}{4} = (0.03333\ldots)_4$, so $\frac{1}{4} \in C$. (This is despite the fact that $\frac{1}{4} = 0.1_4$.)

3. $\frac{1}{5} = (0.030303\ldots)_4$, so $\frac{1}{5} \in C$.

4. The only ways of writing $\frac{1}{2}$ in base 4 are $(0.13333\ldots)_4$ and 0.2_4, so $\frac{1}{2} \notin C$.

An interesting property of the middle-half Cantor set is that it has "zero length."

Definition 2.7. A set $S \subset \mathbb{R}$ has *measure zero* if

$$\forall \varepsilon > 0, \exists \text{ intervals } (I_i)_{i=1}^{\infty} \text{ s.t. } S \subset \bigcup_i I_i \text{ and } \sum_{i=1}^{\infty} (\text{length of } I_i) < \varepsilon. \tag{2.8}$$

(It does not matter if we take open or closed intervals.)

Theorem 2.8. *C has measure zero.*

Proof. C_n can be covered by 2^n intervals, each of length 4^{-n}. The total length is $(2/4)^n$. Since $C \subset C_n$ for all n, this completes the proof. □

Furthermore, the Cantor set C has the same cardinality as $\mathbb{R}$. (See Exercise 3.1.) Thus, C is "large" in the sense of cardinality but "small" in the sense of measure.

2.4 The four corner Cantor set

We also consider a 2-dimensional version of C by taking the direct product. Note that $C \times C = \bigcap_{n=0}^{\infty} C_n \times C_n$. We can also describe $C \times C$ as follows. First $C_0 \times C_0$ is the unit square. Divide the unit square into 16 squares of equal size. Then $C_1 \times C_1$ is the union of the four corner squares. Repeat the same procedure on each of the four squares of $C_1 \times C_1$ to get $C_2 \times C_2$ (a union of 16 squares), and so on.

Now we look at projections $\operatorname{proj}_\alpha(C \times C)$, or equivalently, sum-sets $C + \alpha C$. Let us first consider $\alpha = 1$. Note that $\operatorname{proj}_1(C_0 \times C_0) = [0, 2]$. However, in the limit, we lose "most" of the points in $[0, 2]$.

Theorem 2.9. $\operatorname{proj}_1(C \times C) = C + C$ *has measure zero.*

Proof. Note that two of the four squares of $C_1 \times C_1$ overlap each other exactly when projected in direction 1. Thus, for every n, $C_n + C_n$ can be covered by 3^n intervals, each of length $2 \cdot 4^{-n}$. The total length is $2 \cdot (3/4)^n$. □

To be precise, we give the following definition.

Definition 2.10. Two squares $S, T \subset C_n \times C_n$ *overlap exactly* when projected in direction α if $\operatorname{proj}_\alpha S = \operatorname{proj}_\alpha T$. (The two squares S and T must each be one of the 4^n squares in $C_n \times C_n$ of slide length 4^{-n}.)

The reason for the exponential decay factor of $(3/4)^n$ in the proof above is that two squares in $C_1 \times C_1$ overlapped exactly when projected in direction 1. In general, since $C_n \times C_n$ is the union of 4^n squares each of side length 4^{-n}, any exact overlap will lead to exponential decay. This idea is made more precise in Exercise 3.3.

If we change the projection direction from 1 to 2, then we avoid overlap.

Theorem 2.11. $\operatorname{proj}_2(C \times C) = C + 2C = [0, 3]$

Proof. Clearly, $\operatorname{proj}_2(C_0 \times C_0) = [0, 3]$. By drawing a picture, we can also see that $\operatorname{proj}_2(C_1 \times C_1) = \operatorname{proj}_2(C_0 \times C_0)$. Informally, this says that even though we are removing squares to get from $C_0 \times C_0$ to $C_1 \times C_1$, the remaining squares are still "enough to cover everything" in the shadow. Furthermore, $C_2 \times C_2$ is created from $C_1 \times C_1$ the same way that $C_1 \times C_1$ was created from $C_0 \times C_0$, so $\operatorname{proj}_2(C_2 \times C_2) = \operatorname{proj}_2(C_1 \times C_1)$. By induction $\operatorname{proj}_2(C_n \times C_n) = [0, 3]$ for all n, and taking the limit gives $\operatorname{proj}_2(C \times C) = [0, 3]$. □

Thus, $\operatorname{proj}_1(C \times C)$ and $\operatorname{proj}_2(C \times C)$ are very different. One of the questions we will study in this class is the following, which turns out to be closely related to a number theory question.

Question 2.12. *Let* $\alpha \in \mathbb{R}$. *What can we say about* $\operatorname{proj}_\alpha(C \times C) = C + \alpha C$*?*

Fun fact 2.13. Define

$$S = \{\alpha \in \mathbb{R} : C + \alpha C \text{ does not have measure zero}\} \tag{2.9}$$

The following is true:

$$S \text{ has measure zero.} \tag{2.10}$$

In fact, we can say more:

$$S = \{2^k \tfrac{p}{q} : k, p, q \text{ are all odd integers}\}. \tag{2.11}$$

Furthermore, (2.10) implies the existence of Kakeya sets (a.k.a. Besicovitch sets), which are sets in the plane with area zero and that contain a line in every direction. (Sometimes it is defined without the area zero condition, and sometimes it is defined with "line segment" in place of "line." There is no definition that is universally agreed upon.) We do not have time to talk about this more unfortunately.

(See Mattila's *Fourier analysis and Hausdorff dimension*, Chapter 10 or Bishop–Peres's *Fractals in probability and analysis*, Chapter 9 for more information, including proofs.)

2.5 A discretization of the middle-half Cantor set

Now we introduce a discretization of the middle-half Cantor set C. For $n \in \mathbb{N}_0$, we define

$$\begin{aligned} D_n &= \{0,1\} + \{0,4\} + \{0,4^2\} + \cdots + \{0,4^{n-1}\} \qquad (2.12)\\ &= \{x \in \mathbb{R} : x = (x_1 x_2 \cdots x_n)_4 \text{ for some } x_1, \ldots, x_n \in \{0,1\}\}. \qquad (2.13)\end{aligned}$$

For example,

$$\begin{aligned} D_0 &= \{0\} \qquad (2.14)\\ D_1 &= \{0,1\} \qquad (2.15)\\ D_2 &= \{0,1,4,5\} \qquad (2.16)\\ D_3 &= \{0,1,4,5,16,17,20,21\} \qquad (2.17)\end{aligned}$$

We can relate D_n to C_n as follows. Recall that C_n is a union of 2^n intervals, each of length 4^{-n}. Similar to (2.7), we have

$$\begin{aligned} &\{x \in [0,1] : x = (0.x_1 x_2 \cdots x_n)_4 \text{ for some } x_1, \ldots, x_n \in \{0,3\}\}\\ &\quad = \{\text{left endpoints of intervals in } C_n\}. \end{aligned} \tag{2.18}$$

Thus, if we rescale by $\frac{1}{3}$, the allowed digits are now 0 and 1:

$$\begin{aligned} &\{x \in [0,1] : x = (0.x_1 x_2 \cdots x_n)_4 \text{ for some } x_1, \ldots, x_n \in \{0,1\}\}\\ &\quad = \{\text{left endpoints of intervals in } \tfrac{1}{3} C_n\} \end{aligned} \tag{2.19}$$

We can then rescale by 4^n to shift all the digits:

$$\begin{aligned} D_n &= \{x \in \mathbb{R} : x = (x_1 x_2 \cdots x_n)_4 \text{ for some } x_1, \ldots, x_n \in \{0,1\}\} \\ &= \{\text{left endpoints of intervals in } \tfrac{4^n}{3} C_n\} \end{aligned} \tag{2.20}$$

3 Day 1 exercises

Highly recommended: Exercise 3.3, Exercise 3.4

Exercise 3.1. (🦎) Show that C has the same cardinality as $\mathbb{R}$. (Hint: Use (2.7).)

Exercise 3.2. (🦎) Use (2.7) to give another proof of Theorem 2.11. (Hint: It's easier to show that $\frac{1}{3}C + \frac{1}{3}C = [0,1]$)

Exercise 3.3. (🦎🐉) Let $\alpha \in \mathbb{R}$. Suppose that there exists a $n \in \mathbb{N}$ such that two squares in $C_n \times C_n$ overlap exactly when projected in direction α. Then $\mathrm{proj}_\alpha(C \times C)$ has measure zero.

(Hint: Consider $\mathrm{proj}_\alpha(C_{kn} \times C_{kn})$ as $k \to \infty$.)

Exercise 3.4. (🦎🐉) Recall that $D_2 + 3D_2 = \{a + 3b : a, b \in D_2\}$. There are 16 pairs $(a,b) \in D_2 \times D_2$. How many numbers are in the sum-set $D_2 + 3D_2$? What does this imply about $\mathrm{proj}_3(C_2 \times C_2)$? What does this imply about $\mathrm{proj}_3(C \times C)$?

Exercise 3.5. (🦎) Define the middle-third Cantor set $\widetilde{C} = \bigcap_{n=0}^{\infty} \widetilde{C}_n$ like the middle-half Cantor set in Section 2.3, except that we remove the middle *third* instead of the middle half in each step. For example,

$$\widetilde{C}_0 = [0,1] \tag{3.1}$$

$$\widetilde{C}_1 = [\tfrac{0}{3}, \tfrac{1}{3}] \cup [\tfrac{2}{3}, \tfrac{3}{3}] \tag{3.2}$$

$$\widetilde{C}_2 = [\tfrac{0}{9}, \tfrac{1}{9}] \cup [\tfrac{2}{9}, \tfrac{3}{9}] \cup [\tfrac{6}{9}, \tfrac{7}{9}] \cup [\tfrac{8}{9}, \tfrac{9}{9}] \tag{3.3}$$

Alternatively,

$$\widetilde{C} = \{x \in [0,1] : x \text{ has a base 3 expansion with only 0s and 2s}\}. \tag{3.4}$$

1. Show that $\widetilde{C}$ has measure zero.

2. Show that $\widetilde{C} + \widetilde{C} = [0,2]$.

3. Show that $\widetilde{C}$ has the same cardinality as $\mathbb{R}$.

Exercise 3.6. (🦎🐉) For the middle-third Cantor set $\widetilde{C}$ (see Exercise 3.5), find a non-degenerate interval $I \subset \mathbb{R}$ such that $C + \alpha C$ has measure zero for all $\alpha \in I$. (Note: Because of (2.10), this is impossible for the middle-half Cantor set.)

Exercise 3.7. (🌶🌶) Define the middle-3/5 Cantor set by $\widetilde{C} = \bigcap_{n=0}^{\infty} \widetilde{C}_n$ like the middle-half Cantor set in Section 2.3, except that we remove the middle 3/5 instead of the middle half in each step. For example,

$$\widetilde{C}_0 = [0,1] \tag{3.5}$$

$$\widetilde{C}_1 = [\tfrac{0}{5}, \tfrac{1}{5}] \cup [\tfrac{4}{5}, \tfrac{5}{5}] \tag{3.6}$$

$$\widetilde{C}_2 = [\tfrac{0}{25}, \tfrac{1}{25}] \cup [\tfrac{4}{25}, \tfrac{5}{25}] \cup [\tfrac{20}{25}, \tfrac{21}{25}] \cup [\tfrac{24}{25}, \tfrac{25}{25}] \tag{3.7}$$

Show that for any $\alpha \in \mathbb{R}$, $\widetilde{C} + \alpha\widetilde{C}$ has measure zero.

4 Day 2

4.1 Collisions and a number theory question

Definition 4.1. We say "$A + B$ has a collision" if there exist $a, a' \in A$ and $b, b' \in B$ such that $a + b = a' + b'$ and $(a, b) \neq (a', b')$. (Note that it is not the set $A + B$ itself that has a collision. It is the process of adding the two sets A and B that has a collision.) We make similar definitions for "$A + B + C$ has a collision," "$A + 2B$ has a collision," etc.

For finite sets A and B, note that $A + B$ has a collision if and only if $|A + B| < |A||B|$.

Example 4.2. $\{0, 1\} + \{0, 1, 2\}$ has a collision, while $\{0, 1\} + \{0, 2\}$ does not have a collision. (Note that in both cases, the sum is $\{0, 1, 2, 3\}$.)

We now relate collisions to the size of the projections $\mathrm{proj}_\alpha(C \times C)$.

Theorem 4.3. *Let $\alpha \in \mathbb{R}$. Two squares in $C_n \times C_n$ overlap exactly when projected in direction α if and only if $D_n + \alpha D_n$ has a collision.*

Proof. By the definition of D_n (see (2.20)), we have

$$\{\text{bottom-left corner of the squares in } C_n \times C_n\} = \tfrac{3}{4^n} D_n \times \tfrac{3}{4^n} D_n. \tag{4.1}$$

Take two different squares from $C_n \times C_n$. Let their bottom-left corners be $(\frac{3}{4^n}a, \frac{3}{4^n}b)$ and $(\frac{3}{4^n}c, \frac{3}{4^n}d)$, where $a, b, c, d \in D_n$. The projection proj_α sends these two points to $\frac{3}{4^n}(a + \alpha b)$ and $\frac{3}{4^n}(c + \alpha d)$. Thus, these two squares overlap exactly if and only if $a + \alpha b = c + \alpha d$. That is precisely the condition that $D_n + \alpha D_n$ has a collision. □

The goal of the remainder of the class is to prove the following theorem.

Theorem 4.4. *If α is an odd integer, then there exists a $n \in \mathbb{N}$ such that $D_n + \alpha D_n$ has a collision.*

4.2 An example: $\alpha = 7$

4.2.1 Direct computation

Note that $D_{n+1} = D_n + 4^n D_1$, which implies

$$D_{n+1} + 7D_{n+1} = D_n + 7D_n + 4^n(D_1 + 7D_1) \tag{4.2}$$

This gives us a way to recursively compute $D_n + 7D_n$. Our base case is

$$D_1 + 7D_1 = \{0, 1\} + \{0, 7\} = \{0, 1, 7, 8\}. \tag{4.3}$$

Then

$$D_2 + 7D_2 = D_1 + 7D_1 + 4(D_1 + 7D_1) = \{0, 1, 7, 8\} + \{0, 4, 28, 32\} \tag{4.4}$$

We can systematically calculate the 16 sums in (4.4) by making a table. See Figure 4.1. The header column contains the elements of $4(D_1 + 7D_1)$. The header row contains the elements of $D_1 + 7D_1$ grouped by congruence class modulo 4.

	$0, 8$	1	7
$4 \cdot 0 = 0$	$0, 8$	1	7
$4 \cdot 1 = 4$	$4, 12$	5	11
$4 \cdot 7 = 28$	$28, 36$	29	35
$4 \cdot 8 = 32$	$32, 40$	33	39

Figure 4.1: This table calculates the sum-set $(D_1 + 7D_1) + 4(D_1 + 7D_1)$.

Since all the elements of $4(D_1 + 7D_1)$ are congruent to 0 modulo 4, two numbers in different columns (i.e., separated a vertical line) of Figure 4.1 are not congruent modulo 4 and hence cannot be equal to each other.

Note that all 16 numbers in (4.1) are different. This means we have not found a collision yet.

Now we use the relation $D_3 + 7D_3 = D_2 + 7D_2 + 4^2(D_1 + 7D_1)$. See Figure 4.2. The header column contains the elements of $4^2(D_1 + 7D_1)$. The header row contains the elements of $D_2 + 7D_2$ grouped by congruence class modulo 16.

Similar to above, here, two numbers in different columns are not congruent modulo 16 and hence cannot be equal to each other.

We notice that in the $\{12, 28\}$ column, the number 28 shows up twice. This means that there are two ways obtain 28, which, by retracing the calculations, are

$$28 = 0 + 7 \cdot 4 = (1 + 4 + 4^2) + 7 \cdot 1, \tag{4.5}$$

This gives a collision for $D_2 + 7D_2$. (Similarly, there are two ways to get 140.)

	$0, 32$	$4, 36$	$8, 40$	$12, 28$	$1, 33$	5	29	$7, 39$	11	35
$4^2 \cdot 0 = 0$				$12, 28$						
$4^2 \cdot 1 = 16$				$28, 42$						
$4^2 \cdot 7 = 112$				$124, 140$						
$4^2 \cdot 8 = 128$				$140, 156$						

Figure 4.2: This table calculates the sum-set $(D_2 + 7D_2) + 4^2(D_1 + 7D_1)$.

4.2.2 Simplification of the calculations

Let us analyze the calculations above to see if there is a way to reduce the amount of calculation as well as to avoid adding and multiplying big numbers.

1. To get the column for $\{0, 8\}$ in Figure 4.1 (corresponding to 0 mod 4), we computed $\{0, 8\} + 4(D_1 + 7D_1)$. But we could have factored out a 4 from everything before calculating the sum set:

$$\{0, 8\} + 4(D_1 + 7D_1) = 4(\{0, 2\} + D_1 + 7D_1) \tag{4.6}$$

   Now the sum-set has smaller numbers:

$$\{0, 2\} + D_1 + 7D_1 = \{0, 2\} + \{0, 1, 7, 8\} = \{0, 1, 2, 3, 7, 8, 9, 10\} \tag{4.7}$$

   From this, we see there are no collisions in (4.6).

2. Similarly, to get the column for $\{0, 32\}$ in Figure 4.2 (corresponding to 0 mod 16), we have

$$\{0, 32\} + 4^2(D_1 + 7D_1) = 16(\{0, 2\} + D_1 + 7D_1). \tag{4.8}$$

   Once again, the sum-set (4.7) appears. Thus, without having to do any more calculations, we know there are no collisions in (4.8).

3. Now consider the column $\{4, 36\}$ in Figure 4.2 (corresponding to 4 mod 16).

$$\begin{aligned} \{4, 36\} + 4^2(D_1 + 7D_1) &= 4 + \{0, 32\} + 4^2(D_1 + 7D_1) && (4.9) \\ &= 4 + 16(\{0, 2\} + D_1 + 7D_1) && (4.10) \end{aligned}$$

   It's the same computation again! There are no collisions here either. (When $x \in \mathbb{R}$ and $A \subset \mathbb{R}$, $x + A$ is defined to be $\{x\} + A$.)

4. Now let's consider the column $\{12, 28\}$ in Figure 4.2 (corresponding to 12 mod 16).

$$\{12, 28\} + 4^2(D_1 + 7D_1) = 12 + \{0, 16\} + 4^2(D_1 + 7D_1) \tag{4.11}$$

$$= 12 + 16(\{0, 1\} + D_1 + 7D_1) \tag{4.12}$$

   Finally, we have something different. Since

$$\{0, 1\} + D_1 + 7D_1 = \{0, 1\} + \{0, 1, 7, 8\} = \{0, 1, 2, 7, 8, 9\}, \tag{4.13}$$

   this sum set only has 6 numbers, so there are collisions. Thus (4.11) has collisions too.

4.3 The "type" of a congruence class

Recall $D_{n+1} + 7D_{n+1} = D_n + 7D_n + 4^n(D_1 + 7D_1)$. If we use the RHS to look for collisions in $D_{n+1} + 7D_{n+1}$, we can partition $D_n + 7D_n$ into equivalence classes modulo 4^n.

Suppose $\{s_1, \dots, s_m\} \subset D_n + 7D_n$ is one such equivalence class with $s_1 < \cdots < s_m$. In particular, $s_1 \equiv \cdots \equiv s_m \pmod{4^n}$. Then there are integers $0 = t_1 < \cdots < t_m$ such that $s_i = s_1 + 4^n t_i$. Then

$$\{s_1, \dots, s_m\} + 4^n(D_1 + 7D_1) = s_1 + 4^n(\{t_1, \dots, t_m\} + D_1 + 7D_1) \tag{4.14}$$

Thus, we say the set $\{s_1, \dots, s_m\} \subset D_n + 7D_n$ is of *type* $\{t_1, \dots, t_m\}$. Here is the general definition.

Definition 4.5. Fix α. Fix $n \in \mathbb{N}$ and $k \in \mathbb{Z}/4^n\mathbb{Z}$. Let

$$S_{n,k} = \{x \in D_n + \alpha D_n : x \equiv k \pmod{4^n}\} \tag{4.15}$$

and let $\min S_{n_k}$ be the smallest element of $S_{n,k}$. Let

$$T = \frac{S_{n,k} - (\min S_{n,k})}{4^n} \subset \mathbb{Z} \tag{4.16}$$

Then we say the set $S_{n,k} \subset D_n + \alpha D_n$ is of *type* T.

Example 4.6. Take a look again at the examples in Section 4.2.2.

1. The set $\{0, 8\} \subset D_1 + 7D_1$ is of type $\{0, 2\}$.

2. The set $\{1\} \subset D_1 + 7D_1$ is of type $\{0\}$.

3. The set $\{7\} \subset D_1 + 7D_1$ is of type $\{0\}$.

4. The sets $\{0, 32\}, \{4, 36\}, \{8, 40\}, \{1, 33\}, \{7, 39\} \subset D_2 + 7D_2$ are all of type $\{0, 2\}$.

5. The set $\{12, 28\} \subset D_2 + 7D_2$ is of type $\{0, 1\}$.

6. The set $\{5\}, \{29\}, \{11\}, \{35\} \subset D_2 + 7D_2$ are all of type $\{0\}$.

Lemma 4.7. *Fix α. Then there are finitely many types that can appear as n and k range over all possible values.*

Proof. The maximum element of D_n is $1 + 4 + 4^2 + \cdots + 4^{n-1} = \frac{4^n-1}{3}$. Thus, the maximum element of $D_n + \alpha D_n$ is

$$(1+\alpha)\frac{4^n - 1}{3} \tag{4.17}$$

Thus, for every type arising from $D_n + \alpha D_n$, the maximum element is

$$\leq (1+\alpha)\frac{4^n-1}{3} \cdot \frac{1}{4^n} < \frac{1+\alpha}{3}. \tag{4.18}$$

This means that every type is a subset of $\mathbb{Z} \cap [0, \frac{1+\alpha}{3})$. □

Example 4.8. From Figure 4.1, we see that the set $\{0, 8\} \subset D_1 + 7D_1$ (which is of type $\{0, 2\}$) "generates" the sets $\{0, 32\}, \{4, 36\}, \{8, 40\}, \{12, 28\} \subset D_2 + 7D_2$. The first three are of type $\{0, 2\}$ and the last is of type $\{0, 1\}$.

Another way to see this is to observe that the congruence classes modulo 4 of $\{0, 2\} + D_1 + 7D_1$ are $\{0, 8\}, \{1, 9\}, \{2, 10\}, \{3, 7\}$. The first three are of type $\{0, 2\}$ and the last is of type $\{0, 1\}$. (We already calculated this sum-set in (4.7).)

The following lemma says that you can use types to "generates" more types. It may be helpful to consider $n = 1$ and look at Example 4.8.

Lemma 4.9. *Fix α. Fix m and n. Let T be a type that arises in $D_m + \alpha D_m$. Then the congruence classes mod 4^n of $T + D_n + \alpha D_n$ give rise to types that also appear as types of congruence classes mod 4^{m+n} of $D_{m+n} + \alpha D_{m+n}$.*

More precisely, let $k \in \{0, \ldots, 4^m - 1\}$ and let $S_{m,k}$ be as in (4.15). Suppose $S_{m,k}$ has type T, so that $S_{m,k} = (\min S_{m,k}) + 4^m T$. Then for any $\ell \in \{0, \ldots, 4^n - 1\}$,

$$S_{m+n,\, k+4^m\ell} = (\min S_{m,k}) + 4^m\{x \in T + D_n + \alpha D_n : x \equiv \ell \pmod{4^n}\}. \tag{4.19}$$

Proof. The statement of the lemma looks very complicated, but the result follows from unpacking all the definitions and using the recurrence relation

$$D_{m+n} + \alpha D_{m+n} = D_m + \alpha D_m + 4^m(D_n + \alpha D_n), \tag{4.20}$$

which follows from $D_{m+n} = D_m + 4^m D_n$. □

4.4 "Fourier analysis on cyclic groups"

4.4.1 The generating function for D_n

For a finite set $S \subset \mathbb{N}_0$, define $\phi_S(x) = \sum_{s \in S} x^s$. Generating functions are a useful way of studying sum-sets. For example, the fact that $D_2 = \{0,1,4,5\} = \{0,1\} + \{0,4\}$ and that there are no collisions can be expressed by:

$$\phi_{D_2}(x) = 1 + x + x^4 + x^5 = (1+x)(1+x^4) \tag{4.21}$$

In general,

$$\text{if } S+T \text{ has no collisions, then } \phi_{S+T}(x) = \phi_S(x)\phi_T(x). \tag{4.22}$$

Similarly, by noting that there are no collisions in (2.12), we have

$$\phi_{D_n}(x) = (1+x)(1+x^4)\cdots(1+x^{4^{n-1}}) = \prod_{j=0}^{n-1}(1+x^{4^j}) \tag{4.23}$$

It is also clear from the definition of generating function that

$$\phi_{\alpha D_n}(x) = \phi_{D_n}(x^\alpha) = \prod_{j=0}^{n-1}(1+x^{\alpha 4^j}) \tag{4.24}$$

4.4.2 Roots of unity

For $n \in \mathbb{N}$, we say a complex number z is a nth *root of unity* if $z^n = 1$. For example, there are four 4th roots of unity: $1, i, -1, -i$. See https://en.wikipedia.org/wiki/Root_of_unity for more on roots of unity.

It turns out that when $S \subset \mathbb{N}_0$ has some special properties, then we can say something about the roots of its generating function $\phi_S(x)$.

Lemma 4.10. *Let $S \subset \mathbb{N}_0$ be a finite set. Suppose S has the same number of elements in each congruence class modulo 4, i.e.,*

$$|S_0| = |S_1| = |S_2| = |S_3|, \text{ where } S_k = \{x \in S : x \equiv k \pmod 4\} \tag{4.25}$$

Then

$$\phi_S(i) = \phi_S(-1) = \phi_S(-i) = 0 \tag{4.26}$$

where $i = \sqrt{-1}$.

Proof. Note that

$$\phi_S(x) = \phi_{S_0}(x) + \phi_{S_1}(x) + \phi_{S_2}(x) + \phi_{S_3}(x) \tag{4.27}$$

Also, if $m \equiv n \pmod 4$, then $i^m = i^n$. Thus,

$$\phi_{S_k}(i) = \sum_{s \in S_k} i^s = \sum_{s \in S_k} i^k = |S_k| i^k \tag{4.28}$$

which implies

$$\phi_S(i) = |S_0|i^0 + |S_1|i^1 + |S_2|i^2 + |S_3|i^3 = |S_0|(i^0 + i^1 + i^2 + i^3) = 0 \tag{4.29}$$

The proofs that $\phi_S(-1) = 0$ and $\phi_S(-i) = 0$ are similar. □

Here is a generalization of Lemma 4.10.

Lemma 4.11. *Let $S \subset \mathbb{N}_0$ be a finite set and let $n \in \mathbb{N}$. Suppose S has the same number of elements in each congruence class modulo n. Then*

$$\phi_S(\omega^k) = 0 \text{ for all } k \in \{1, 2, \dots, n-1\}, \tag{4.30}$$

where

$$\omega = e^{2\pi i/n} = \cos\tfrac{2\pi}{n} + i \sin\tfrac{2\pi}{n}. \tag{4.31}$$

Proof. The argument is similar to the proof of Lemma 4.10 but in place of $i^0+i^1+i^2+i^3 = 0$, it uses the following fact : Let $\omega \in \mathbb{C}$ be defined as in (4.31). Then

$$\text{If } k \in \mathbb{Z} \text{ is not a multiple of } n, \text{ then } \sum_{j=0}^{n-1} \omega^{kj} = 1 + \omega^k + \omega^{2k} + \cdots + \omega^{(n-1)k} = 0. \tag{4.32}$$

You are asked to prove (4.32) in Exercise 5.3 □

4.4.3 Fourier analysis?

One of the fundamental theorems in Fourier analysis on $\mathbb{Z}/n\mathbb{Z}$ is that every function f : $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$. has a Fourier series, i.e., $f(x) = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} a_k e^{2\pi i k x/n}$ for some $a_k \in \mathbb{C}$. The topics presented above can be introduced using Fourier analysis, but we do not take that approach in this class.

4.5 The proof of Theorem 4.4

Fix an odd number $\alpha \in \mathbb{Z}$. Because there are only finitely many types (by Lemma 4.7), there is a type $T \subset \mathbb{N}_0$ of maximal cardinality. (It may not be unique.)

Lemma 4.12. *Fix an odd number $\alpha \in \mathbb{Z}$. Let $T \subset \mathbb{N}_0$ be a type of maximal cardinality and let $n \in \mathbb{N}$. Suppose that $T + D_n + \alpha D_n$ has no collisions. Then:*

$$\phi_T(\omega^k) = 0 \text{ for all odd } k \in \{1, 2, \ldots, 4^n - 1\} \tag{4.33}$$

where

$$\omega = e^{2\pi i/4^n}. \tag{4.34}$$

Proof. From the hypotheses of the lemma, we have:

1. $T + D_n + \alpha D_n$ has no collisions, so $|T + D_n + \alpha D_n| = |T||D_n||\alpha D_n| = |T|4^n$.

2. $T + D_n + \alpha D_n$ cannot have a congruence class modulo 4^n with more than $|T|$ elements. This is because the congruence classes modulo 4^n of $T + D_n + \alpha D_n$ also give rise to types (see Lemma 4.9), and no type can have cardinality greater than T.

These two observations imply that each congruence class modulo 4^n of $T + D_n + \alpha D_n$ has exactly $|T|$ elements. Thus, by Lemma 4.11,

$$\phi_{T+D_n+\alpha D_n}(\omega^k) = 0 \text{ for all } k \in \{1, 2, \ldots, 4^n - 1\}, \tag{4.35}$$

where $\omega = e^{2\pi i/4^n}$.

Since $T + D_n + \alpha D_n$ has no collisions, we have

$$\phi_{T+D_n+\alpha D_n}(x) = \phi_T(x)\phi_{D_n}(x)\phi_{\alpha D_n}(x) \tag{4.36}$$

By (4.23) and (4.24)

$$\phi_{D_n}(x)\phi_{\alpha D_n}(x) = \prod_{j=0}^{n-1}(1 + x^{4^j})(1 + x^{\alpha 4^j}) \tag{4.37}$$

By using the factorization above, we see that

$$\phi_{D_n}(\omega^k)\phi_{\alpha D_n}(\omega^k) \neq 0 \text{ for all odd } k \in \{1, 2, \ldots, 4^n - 1\}. \tag{4.38}$$

(This is where we use the fact that α is odd.) Combining (4.35), (4.36), and (4.38) finishes the proof of this lemma. □

Now we have everything we need to prove Theorem 4.4. Let α be an odd number and suppose for contradiction that $D_n + \alpha D_n$ has no collisions for all n. Let $T \subset \mathbb{N}_0$ be a type of maximal cardinality. Then by Lemma 4.9, $T + D_n + \alpha D_n$ has no collisions for all n. By Lemma 4.12,

$$\phi_T(e^{2\pi ik/4^n}) = 0 \text{ for all } n \in \mathbb{N} \text{ and all odd } k \in \{1, 2, \dots, 4^n - 1\} \tag{4.39}$$

Note that the numbers $e^{2\pi ik/4^n}$ are distinct for different values for n and k. Thus, we have shown that T has infinitely many roots, which is a contradiction. This completes the proof of Theorem 4.4.

4.6 A more precise theorem

The following is a characterization of the rational numbers α for which collisions occur.

Theorem 4.13. *Let $\alpha \in \mathbb{Q} \setminus \{0\}$. Suppose $\alpha = 2^k \frac{p}{q}$, where $k \in \mathbb{Z}$ and p and q are odd integers.*

1. *If k is even, then there exists a $n \in \mathbb{N}$ such that $D_n + \alpha D_n$ has a collision.*
2. *If k is odd, then for all $n \in \mathbb{N}$, $D_n + \alpha D_n$ does not have a collision.*

The proof of Theorem 4.4 that we gave can be adapted to prove part 1 of Theorem 4.13. You are asked to verify this in Exercise 5.7.

You are asked to prove part 2 of Theorem 4.13 in Exercise 5.8. This part only uses some modular arithmetic.

5 Day 2 exercises

Exercise 5.1. (🦎) This problem gives a more concise way of stating the condition that a collision occurs. Let $D = \bigcup_{n=0}^{\infty} D_n$, i.e., D is the set of nonnegative integers whose base 4 expansion has only 0s and 1s. (There are no constraints on the number of digits.) Then define

$$\frac{D - D}{D - D} = \left\{ \frac{a - b}{c - d} : a, b, c, d \in D \right\}. \tag{5.1}$$

Show that $\alpha \in \frac{D-D}{D-D}$ if and only if there exists a $n \in \mathbb{N}$ such that $D_n + \alpha D_n$ has a collision.

Exercise 5.2. (🦎) Use the same ideas as in Section 4.2 to find the following collision for $D_3 + 9D_3$:

$$4^2 + 9(1 + 4) = 1 + 4 + 4^3 + 9(0) \tag{5.2}$$

Exercise 5.3. (🦎) Prove (4.32). Hint: The sum is a geometric series.

Exercise 5.4. (🦎) Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$, where the sum is finite. Show

$$\frac{f(1) + f(i) + f(-1) + f(-i)}{4} = a_0 + a_4 + a_8 + \cdots \tag{5.3}$$

Is there a similar way to obtain $a_1 + a_5 + a_9 + \cdots$?

Exercise 5.5. (🦎) Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$, where the sum is finite. Suppose $f(i) = f(-i) = 0$. Show that $a_0 + a_4 + a_8 + \cdots = a_2 + a_6 + a_{10} + \cdots$. There are at least two different ways of doing this

1. $f(i) = f(-i) = 0$ implies $x - i$ and $x + i$ are both factors of x.
2. Just prove it directly from the expressions for $f(i)$ and $f(-i)$.

Exercise 5.6. (🦎🦎) Let $n \in \mathbb{N}$, and let $\omega = e^{2\pi i/(2n)}$ be a primitive $2n$-th root of unity. Let $f = \sum_{j=0}^{\infty} a_j x^j$. For $k \in \mathbb{Z}/2n\mathbb{Z}$, let

$$b_k = \sum_{j \equiv k \pmod{2n}} a_j = a_k + a_{2n+k} + a_{4n+k} + \cdots \tag{5.4}$$

Suppose $f(\omega^k) = 0$ for all odd k.

1. Show that $b_0 = b_n$.
2. Show that $b_k = b_{n+k}$ for all k.

(Note that this implies the previous exercise by setting $n = 2$.)

Exercise 5.7. (🦎🦎) Prove part 1 of Theorem 4.13. (Hint: Make some changes to the proof of Theorem 4.4.)

Exercise 5.8. (🦎🦎) Prove part 2 of Theorem 4.13. (Hint: Use modular arithmetic.)