

Dancing Planets and Modular Multiplication

Fran Herr

July 3, 2024

1 Introduction

Our main objects of study in this paper—modular multiplication tables and planet dances—appear throughout recreational mathematics. They are called by many names, including “string art”, “light caustics”, “spirographs”, and “curve stitching”, to name a few. To construct a modular multiplication table, we place m points (the *modulus*) evenly spaced around a circle and choose some *multiplier* a . Then we draw a line segment between point p and $ap \bmod m$ for each point p . One of the most well-known appearances of these objects is in a YouTube video by *Mathologer*: “Times Tables, Mandelbrot, and the Heart of Mathematics” [1]. *Mathologer* discusses basic patterns that appear in modular multiplication tables, including those for small multipliers and when the multiplier is half the modulus.

“Planet dances” are objects from antiquity. Strongly associated with heliocentric models of the solar system, they are characteristic of Ptolemy’s work. One can imagine a stretchy tether between two orbiting planets; we are interested in the pattern this line will make over time. Matt Henderson has made a fantastic animation of such a system which demonstrates the relation between the orbits of the Earth and Venus. It can be found on his Twitter or in the *Numberphile* video “The Strange Orbit of Earth’s Second Moon (plus The Planets)” [2]. In “An Envelope for a Spirograph” [3], Simoson gives a delightful introduction to these objects and discusses how the number of cusps in the caustic of a given planet dance can be determined. Many other sources, including [4], [5], and [6] discuss the relation between planet dances and epicycloids/hypocycloids, as well as the famous coffee-cup caustics.

In this paper, we will briefly discuss well-known patterns in these objects, but our focus will be the connection between modular multiplication tables and planet dances. We will also introduce another perspective by considering paths on the torus. This will reveal why certain patterns appear in the caustics of these line arrangements.

2 Modular Multiplication Tables

Choose some natural number m and place m evenly spaced points around a circle, labeling them 0 through $m - 1$. For practical reasons involving computing and visual aesthetics, we will normally work with m somewhere between 20 and 500. Now choose an integer a and draw a directed chord from every point p to $ap \bmod m$. This creates a *modular multiplication table*—which we denote $\text{MMT}(m, a)$. We will often drop the “MMT” and refer to this table as (m, a) . Figure 1 shows some examples of modular multiplication tables with various values of m and a . Despite being simple objects, modular multiplication tables can display a large variety of visual patterns.

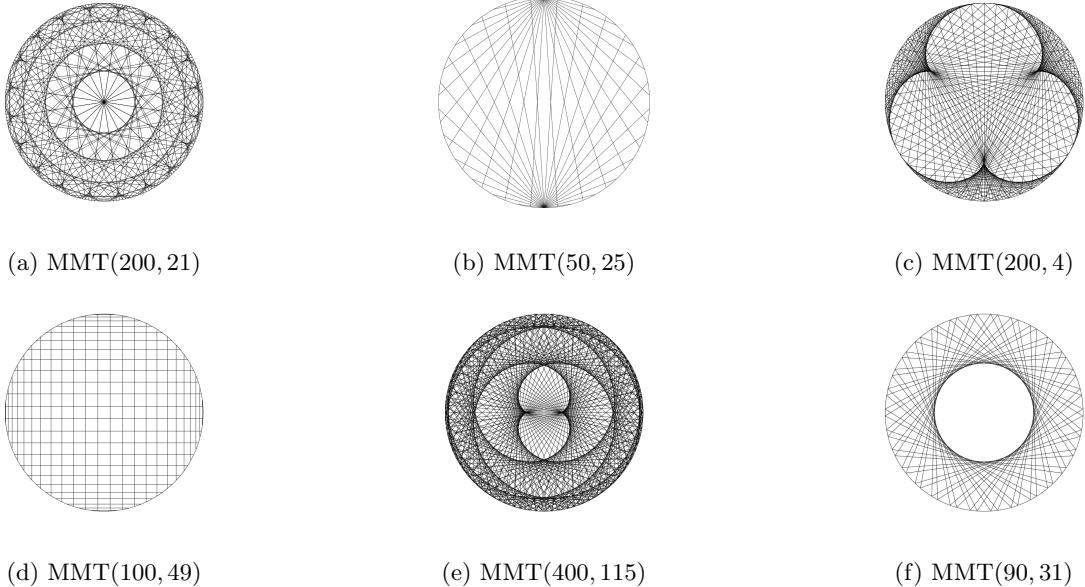


Figure 1: MMTs with various values for m and a .

We will think about the MMT object as a finite set of chords on the circle. These chords maintain a direction even though we draw them without arrows. Although a can be any integer, note that (m, a_1) and (m, a_2) will give the same set of chords if $a_1 \equiv a_2 \pmod{m}$. Hence, we will typically only choose multipliers a with $0 \leq a < m$ to have a canonical representative for each equivalence class.

Question 1. *Given the values for m and a , what pattern will $\text{MMT}(m, a)$ create?*

Above is our guiding question for this paper. Before continuing, I encourage the reader to try drawing some MMTs to make observations and predictions. There are many tools online to draw these pictures; one that I would recommend is made by Mathias Lengler at this link [7]. My own code to draw these objects can be found on github.

2.1 Some basic patterns

One of the first features commonly observed about these objects can be seen by fixing a at a “small” value and increasing m ; as we do this, a well-known curve emerges. For example, Figure 2 shows this process for $a = 2$ and we see the cardioid appear as we increase m . This curve, which all the chords are tangent to, is called the *envelope* of the chords. As we repeat the experiment with $a = 3, 4, 5, \dots$ we might notice a pattern. With a large enough m , the table (m, a) looks like a curve with $a - 1$ “humps” (see Figure 3). This curve is called an *epicycloid*. The epicycloid with $a - 1$ humps is made by rolling a circle with radius $\frac{1}{a+1}$ around a fixed circle with radius $\frac{a-1}{a+1}$ and

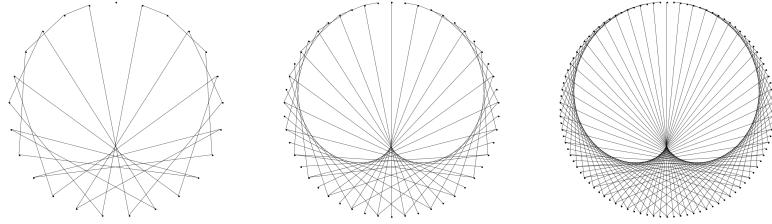


Figure 2: Increasing values for m with $a = 2$. From left to right, $m = 25, 50, 100$.

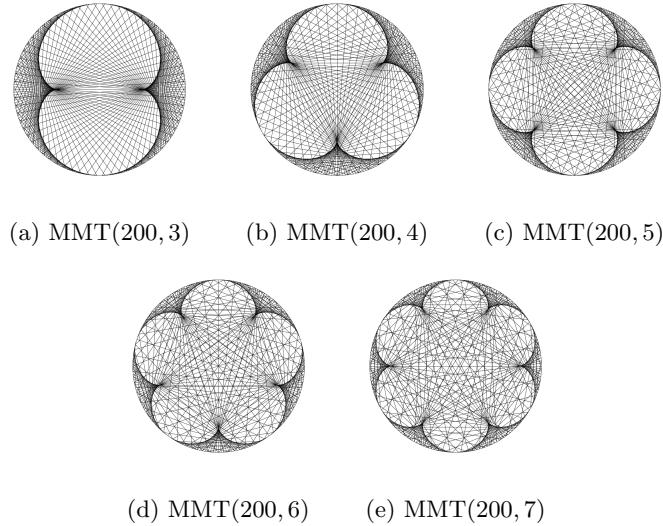


Figure 3: MMTs with $m = 200$ and increasing a values

tracking a point on the boundary of the outer circle.¹ For $a = 2$, we have two circles both with a radius of $\frac{1}{3}$. See Figure 4 for an example of this rolling circle construction with $a = 4$. The epicycloid with $a - 1$ humps is given by the parametric equation

$$x(t) = \frac{a}{a+1} \cos(t) + \frac{1}{a+1} \cos(at)$$

$$y(t) = \frac{a}{a+1} \sin(t) + \frac{1}{a+1} \sin(at).$$

As we experiment with small values of a (between $a = 2$ and $a = 12$ approximately), we might be lead to believe that the envelope of $\text{MMT}(m, a)$, for sufficiently large m , is always the epicycloid given by the equations above. As we shall see, this would be a hasty conclusion.

When we begin to look at higher multipliers, we find the large variety of patterns showcased in Figure 1. We notice that the numerical relationship between m and a plays a key role in determining

¹Note that the two circles are scaled so that the curve sits inside a circle with radius 1. We could just as well roll a circle with radius 1 around a circle with radius $a - 1$.

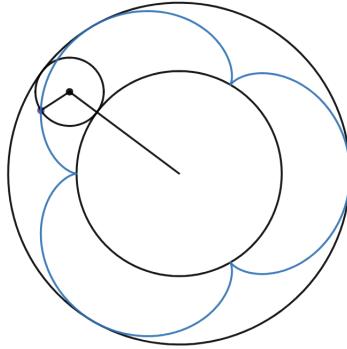


Figure 4: Constructing the epicycloid for $a = 4$. The smaller circle has radius $\frac{1}{5}$ and the larger circle has radius $\frac{3}{5}$.

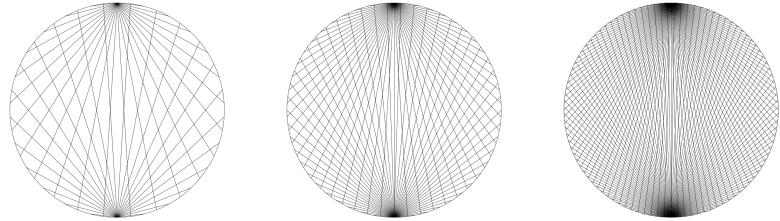


Figure 5: Tables $(50, 25)$, $(100, 50)$, $(200, 100)$

the pattern. For example, if $m = 2a$, then the MMT will look like those in Figure 5; for a given point p , either $ap \equiv 0$ if p is even and $ap \equiv a$ if p is odd. If $m = 2a + 2$ or $m = 2a - 2$, then we also get some interesting patterns shown in Figures 6 and 7.

When I started looking at these modular multiplication tables, immediately I developed a simple goal: can I know what pattern the chords will make just from the number theoretic relationship between m and a ? But as I waded deeper into this world, I found that approaching these objects from only a number theory perspective restricted my field of vision. And when I discovered a particularly interesting family of tables—those described in Section 5—I found myself at the end of my rope. This is where our second mathematical object enters the story. First though, we give a few more details on modular multiplication tables and epicycloids.

2.2 Embedding modular multiplication tables into \mathbb{C}

Although it is often useful to think about modular multiplication tables as discrete objects without any ambient space, it will also be helpful for our purposes to define them more geometrically. Parameterize the unit circle in \mathbb{C} by e^{it} for $t \in [0, 2\pi]$. Then $\text{MMT}(m, a)$ is the set of chords with initial point $e^{2\pi i t_k}$ and terminal point $e^{2\pi i a t_k}$ with $t_k = \frac{k}{m}$ for all $k \in \{0, \dots, m-1\}$.

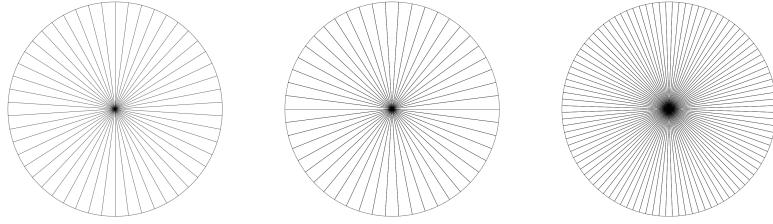


Figure 6: Tables (50, 26), (100, 51), (200, 101)

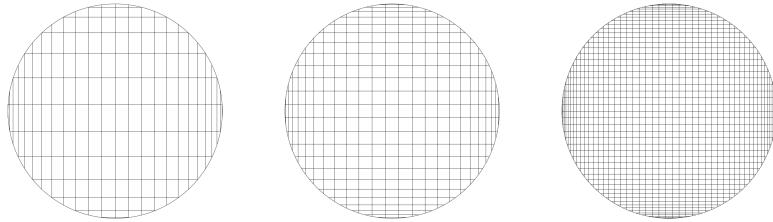


Figure 7: Tables (50, 24), (100, 49), (200, 99)

2.3 Epicycloids and hypocycloids

Recall from Section 2.1 than an *epicycloid* is a curve constructed by rolling one circle around another fixed circle and tracking a point on the boundary of the outer circle. A *hypocycloid* is similar to an epicycloid but the rolling circle is on the inside of the fixed circle. We can realize both these curves with the following parametric equations.

$$\begin{aligned} x(t) &= \alpha \cos t + \beta \cos \left(\frac{\alpha}{\beta} t \right) \\ y(t) &= \alpha \sin t + \beta \sin \left(\frac{\alpha}{\beta} t \right) \end{aligned} \tag{1}$$

In the case of an epicycloid, both α and β should be positive real numbers. When $0 < \beta \leq \alpha$, the equation (1) describes a circle of radius β rolling around a circle of radius $\alpha - \beta$. If $0 < \alpha < \beta$, this physical interpretation does not make sense because we cannot have a circle with radius $\alpha - \beta$. However, switching α and β by setting $\alpha' = \beta$ and $\beta' = \alpha$ will give the same curve. This follows by a change of variables $s = \frac{\beta}{\alpha}t$.

To draw a hypocycloid, we maintain $\alpha > 0$ but set $\beta < 0$. Then these equations (1) describe the hypocycloid with fixed circle radius $\alpha - \beta$ and rolling circle radius $|\beta|$.

In this way, we can realize epicycloids and hypocycloids using the same set of parametric equations. For our purposes, we will only be concerned with cases where α and β are integers, because we are interested in periodic curves. We will revisit these equations in the next section.

3 Dancing Planets

We now turn our attention to another mathematical object, inspired by the epicyclic model of the solar system and often associated with the work of Ptolemy. In this planetary model, a “moon” orbits a “planet” in a circular fashion as that “planet” moves in a circle around a “sun”². The name *epicycle* refers to the “circle within a circle” motion. There seems to be no standard name for such a system among other sources, so the name “*planet dance*” is of the author’s creation.

Definition 3.1. We denote a *planet dance* by $\mathcal{P}(\alpha, \beta)$ where $\alpha, \beta \in \mathbb{Z}$ are integers. These integers define a set of directed chords of the circle with initial point at $e^{2\pi i \alpha t}$ and terminal point at $e^{2\pi i \beta t}$ for all $t \in [0, 1]$.

Even though we define a planet dance as a set of chords, we will tend to think of it as dynamical system developing over time.³ We imagine two “planets”—planet A and planet B—moving around the same circular orbit at different speeds. Planet A will make α circles in one minute and planet B will make β circles in one minute. We are interested in an infinitely stretchy tether between the two planets, and the pattern it makes over time.

Since α and β are both integers, when $t = 0$ or $t = 1$ the chord becomes a single point at $e^0 = 1$. Note that one or both of α and β can be 0. The planet dance $\mathcal{P}(0, 0)$ will form a single point at $e^0 = 1$. Some planet dances will produce the same set of chords. We would then like to normalize and choose a representative from each equivalence class so that the set of chords is unique to the pair (α, β) .

- If $\alpha = 0$, but $\beta \neq 0$, then $\mathcal{P}(0, \beta)$ will be the same set of chords as $\mathcal{P}(0, 1)$. And likewise, $\mathcal{P}(\alpha, 0)$ will be the same set of chords as $\mathcal{P}(1, 0)$ when $\alpha \neq 0$. Thus, to normalize, if $\mathcal{P}(\alpha, \beta) \neq \mathcal{P}(0, 0)$ and if $\alpha = 0$ (resp. $\beta = 0$), we require that $\beta = 1$ (resp. $\alpha = 1$).
- Let α and β be nonzero and suppose that $d = \gcd(\alpha, \beta) > 1$. Then the planet dance $\mathcal{P}(\alpha, \beta)$ will contain the same set of chords as $\mathcal{P}\left(\frac{\alpha}{d}, \frac{\beta}{d}\right)$ and will repeat d times. Thus, we will typically assume that $\gcd(\alpha, \beta) = 1$.

Definition 3.2. When the planet dance $\mathcal{P}(\alpha, \beta)$ is $\mathcal{P}(0, 0)$, $\mathcal{P}(0, 1)$, $\mathcal{P}(1, 0)$, or $\gcd(\alpha, \beta) = 1$, we say that $\mathcal{P}(\alpha, \beta)$ is in *reduced form*.

- If α and β are both positive (or both negative) then planet A and planet B will move in the same direction around the circle. If α and β have opposite signs then A and B will move in opposite directions around the circle. However, in either case, $\mathcal{P}(\alpha, \beta)$ and $\mathcal{P}(-\alpha, -\beta)$ will produce the same set of chords. This follows by a change of variables $t \mapsto 1 - t$ (or imagine the dynamical system “playing in reverse”).

Definition 3.3. If α and β have the same sign, then $\mathcal{P}(\alpha, \beta)$ is a *positive planet dance*. If α and β have opposite signs, then $\mathcal{P}(\alpha, \beta)$ is a *negative planet dance*. We will typically assume that $\alpha \geq 0$, so that the sign of the planet dance is determined by the sign of β .

For a positive planet dance $\mathcal{P}(\alpha, \beta)$, the chords envelope a recognizable epicycloid. Figure 8 shows both $\mathcal{P}(3, 2)$ and the corresponding epicycloid: this is described by the equations (1) with $\alpha = 3$ and $\beta = 2$.

²In Ptolemy’s time, all celestial bodies were thought to orbit the earth. Hence the quotes around “moon”, “planet”, and “sun”. Luckily, this “change of variables” does not change our geometric picture.

³Hence, the name ‘dance’.

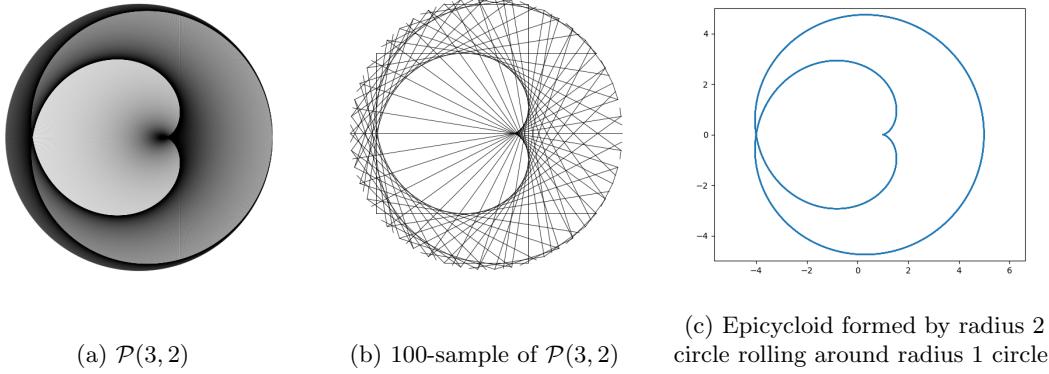


Figure 8: A planet dance and its 100-sample

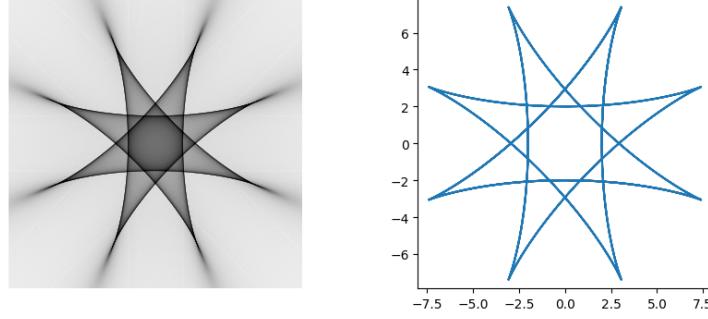


Figure 9: $\mathcal{P}(5, -3)$ and the corresponding hypocycloid

Upon first inspection, negative planet dances do not share this correspondence. However the pattern is still there, but a bit hidden. To see the correspondence with an hypocycloid, we need to extend the chords beyond the circle. The curve will be given by a circle with radius $|\beta|$ rolling inside a circle with radius $\alpha - \beta$.⁴ Figure 9 shows $\mathcal{P}(5, -3)$ and its corresponding hypocycloid.

In both the positive and the negative case, the curve (epicycloid or hypocycloid) will be given by the parametric equations given in Section 2.3. This is proved by Bouthillier in “Representations of Epitrochoids and Hypotrochoids” [8] in Theorems 25 and 27.

$$x(t) = \alpha \cos t + \beta \cos \left(\frac{\alpha}{\beta} t \right)$$

$$y(t) = \alpha \sin t + \beta \sin \left(\frac{\alpha}{\beta} t \right)$$

Now imagine taking a picture of the planet dance m times at regular intervals over the duration

⁴We are assuming that $\alpha \geq 0$ as discussed in Definition 3.3

of the time interval $[0, 1]$. We will overlay all these pictures to create one composite image. This generates a picture that looks rather like a modular multiplication table: it produces a finite set of chords on the circle. (See Figure 8 for an example.) But does this visual correlation between samples of planet dances and MMTs point to a more robust mathematical correspondence?

Definition 3.4 (m -regular sampling of a planet dance). Let $\mathcal{P}(\alpha, \beta)$ be a planet dance and m be a positive integer. Then an m -regular sampling of $\mathcal{P}(\alpha, \beta)$ is the finite set of chords for $t = 0, \frac{1}{m}, \frac{2}{m}, \dots, \frac{m-1}{m}$. We denote this set $\mathcal{S}(\alpha, \beta, m)$.

Question 2. For every $\text{MMT}(m, a)$ are there α and β such that $\text{MMT}(m, a) = \mathcal{S}(\alpha, \beta, m)$? And, for each $\mathcal{S}(\alpha, \beta, m)$, can we find some $\text{MMT}(m, a)$ that produces the same set of chords?

The first of these questions has an immediate affirmative answer. The modular multiplication table $\text{MMT}(m, a)$ will be exactly the same set of chords as $\mathcal{S}(1, a, m)$. When the initial end of the chord has traveled distance p , then the terminal end will have traveled a distance of ap . Thus, each chord in $\mathcal{S}(1, a, m)$ can be constructed by multiplying the initial point p by a , and this gives the correspondence to $\text{MMT}(m, a)$. We will call planet dances of the form $\mathcal{P}(1, \beta)$ *unit speed dances*.

Lemma 3.5 (Fundamental Correspondence). *The modular multiplication table $\text{MMT}(m, a)$ is an m -regular sampling of the unit speed planet dance $\mathcal{P}(1, a)$.*

Proof. The m -regular sampling consists of all chords at $t = 0, \frac{1}{m}, \dots, \frac{m-1}{m}$. Hence, these will be all chords with initial point $e^{2\pi i \frac{k}{m}}$ and terminal point $e^{2\pi i \frac{ak}{m}}$ for $0 \leq k \leq m$, k an integer. These are exactly the chords in the modular multiplication table $\text{MMT}(m, a)$ embedded in \mathbb{C} . \square

The answer to our second question is not so simple. If we have a planet dance $\mathcal{P}(\alpha, \beta)$ with $\alpha > 1$ and we follow the same method as for unit speed planet dances, the multiplier of the modular multiplication table should be $\frac{\beta}{\alpha}$; if we assume that $\mathcal{P}(\alpha, \beta)$ is in reduced form, then this is not an integer. But in our definition of modular multiplication tables, we do not allow non-integral multipliers. Of course, we could change our definition of modular multiplication tables, but we will see that there is a way forward without this restructuring.

Remark 3.6. Other sources have taken the route of defining modular multiplication tables using non-integer multipliers. See [7] for an example.

Why do we have hope that we can use the current definition of modular multiplication tables to represent samplings of non-unit speed planet dances? Because of empirical evidence. Figure 10 shows $\mathcal{P}(3, 2)$ and $\text{MMT}(100, 34)$ side-by-side. Upon visual inspection, it seems that they depict the same epicycloid curve. And, in fact, any MMT of the form $\text{MMT}(3a - 2, a)$ will envelope this same curve as well⁵. Is there a deeper reason that these two patterns look the same?

⁵This example is one member in an infinite family which initiated this research project. I discuss this story and the family of tables in Section 5.

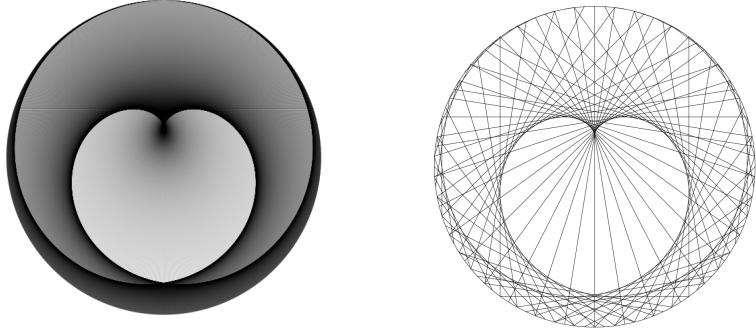


Figure 10: $\mathcal{P}(3, 2)$ (left) and MMT(100, 34) (right)

4 Introducing Topology

We now introduce a topological perspective in order to expand this correspondence to include non unit speed planet dances.

4.1 Planet dances as paths on a torus

A directed chord on the circle is uniquely determined by the position of the two endpoints—planet A and planet B. Hence, the space of all such possible chords is $\mathbb{S}^1 \times \mathbb{S}^1 = \mathbb{T}^2$... a torus! We will use the square torus as our model of this space.

A point on the torus will give a single chord on the circle, and a path on the torus will give a continuous family of chords. For a planet dance $\mathcal{P}(\alpha, \beta)$, we know planet A and planet B are moving at constant speeds α and β respectively. So all chords in $\mathcal{P}(\alpha, \beta)$ form a linear closed path on the flat torus. These loops are commonly used to represent torus knots. Figure 11 shows two examples of these linear paths on the torus.

For a directed chord with initial point e^{it} and terminal point e^{is} , we will define the following homeomorphism:

$$\Phi : \mathbb{S}^1 \times \mathbb{S}^1 \rightarrow \mathbb{R}^2 / \mathbb{Z}^2, \quad \Phi(e^{it}, e^{is}) = \left(\frac{t}{2\pi}, \frac{s}{2\pi} \right)$$

The first \mathbb{S}^1 -term, and thus the x -coordinate, will represent the position of planet A. And likewise, the second \mathbb{S}^1 -term and the y -coordinate will represent the position of planet B. Thus, the line in $\mathbb{R}^2 / \mathbb{Z}^2$ which corresponds to $\mathcal{P}(\alpha, \beta)$ is given by

$$x = \alpha t, \quad y = \beta t, \quad \text{or, if } \alpha \neq 0, \quad y = \frac{\beta}{\alpha} x.$$

We will identify the planet dance $\mathcal{P}(\alpha, \beta)$ with this loop in the torus, and depending on the context, we will say $\mathcal{P}(\alpha, \beta)$ to mean the line with parametric equation $x = \alpha t$ and $y = \beta t$ in $\mathbb{R}^2 / \mathbb{Z}^2$.

Remark 4.1 (On direction). Swapping the values of α and β in a planet dance will not make a difference in the visual pattern produced, but it does change the direction of each chord as we have formally defined them. And it will change the slope of the corresponding line in $\mathbb{R}^2 / \mathbb{Z}^2$. As we

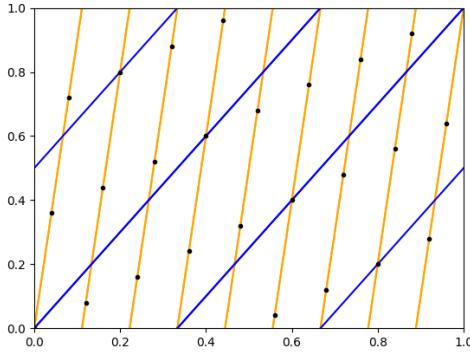


Figure 11: An example of linear loops on the torus. The blue lines depict $y = \frac{3}{2}x$ which corresponds with $\mathcal{P}(2, 3)$ and the orange lines depicts $y = 9x$ which corresponds to $\mathcal{P}(1, 9)$. The black dots indicate that $\mathcal{P}(1, 9)$ is sampled at a rate of 25, corresponding with $\text{MMT}(25, 9)$.

move forward, it will be important for us to maintain the proper direction of the chords as this inherently matters for modular multiplication tables. In an MMT, we would like to always think of the initial point of the chord as being multiplied by a to get the terminal point of the chord. That is, we would like $\text{MMT}(m, a)$ to correspond with $\mathcal{S}(1, a, m)$ and not $\mathcal{S}(a, 1, m)$.

If a planet dance is a linear loop on the torus, then a regular sampling of the planet dance is a set of equally spaced points along the loop. As our sampling becomes more frequent, the set of points more closely approximates the loop and the discrete sampling picture will be a better representation of the continuous planet dance.

4.2 Aliasing in sine waves

Aliasing is a pervasive topic in the area of signal processing. Common examples of aliasing are Moiré patterns and the “wagon wheel” effect in cinema. The idea is best demonstrated with sine waves. Suppose that a computer is storing discrete-time samples of a musical note, represented as a sine wave. If the sampling rate is too low, then when the computer plays back the note from its discrete samples, the listener will hear it as a lower note with a lower frequency. This happens because there is more “natural” wave that fits the samples. The two waves—the original sine wave and the lower frequency alias—will intersect exactly at the sample points. This is shown in Figure 12. In signal processing, aliasing is often seen as an unfortunate reality, and research into “anti-aliasing filters” is common. However, this phenomenon is the reason why we see such a large variety of patterns among modular multiplication tables. And this is the phenomenon on which we will focus for the rest of the paper.

4.3 An aliasing phenomenon with planet dances

Just as one sine wave can “alias” as another when we take a discrete sampling, one planet dance can alias as another. The key to this aliasing is the points of intersection. When two linear loops on the torus intersect, they will do so at regular intervals. This follows because both lines have

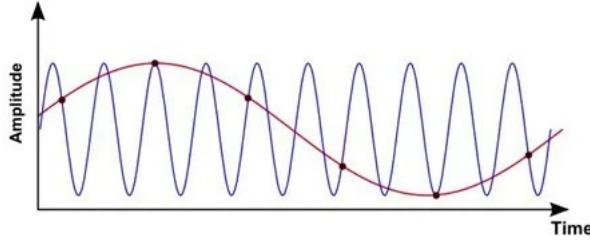


Figure 12: When a higher frequency sine wave is under-sampled, it can appear as a lower frequency sine wave where the sampling points are exactly the points of intersection.

constant rational slopes. These intersection points correspond to a set of shared chords between the two corresponding planet dances.

More specifically, suppose that the linear loops corresponding to planet dances \mathcal{P}_1 and \mathcal{P}_2 intersect m times in $\mathbb{R}^2/\mathbb{Z}^2$. Then the m -regular sampling of \mathcal{P}_1 and the m -regular sampling of \mathcal{P}_2 will be the same set of chords and will look identical. Since we know how to achieve m -regular samplings of unit speed planet dances with MMTs, this will give us a way to sample any planet dance with an MMT by finding a unit speed “alias”.

Conveniently, studying how many times two linear loops on the torus intersect has already been done for the purpose of torus knot intersections.

Lemma 4.2 (Planet dance intersection). *Let lines ℓ_1 and ℓ_2 in $\mathbb{R}^2/\mathbb{Z}^2$ be given by*

$$\ell_1(t) = (\alpha t, \beta t) \quad \text{and} \quad \ell_2(t) = (\gamma t, \delta t)$$

such that $\gcd(\alpha, \beta) = \gcd(\gamma, \delta) = 1$. Then ℓ_1 and ℓ_2 will intersect $|\alpha\delta - \beta\gamma|$ times and will do so at regular intervals.

This is a standard result in knot theory. By restating Lemma 4.2, we can relate non unit speed planet dances to modular multiplication tables.

Corollary 4.3. *Suppose that $\mathcal{P}(\alpha, \beta)$ and $\mathcal{P}(\gamma, \delta)$ are two planet dances in reduced form and let $m = |\alpha\delta - \beta\gamma|$. Then $\mathcal{S}(\alpha, \beta, m) = \mathcal{S}(\gamma, \delta, m)$.*

Proposition 4.4. *Given a planet dance $\mathcal{P}_1 = \mathcal{P}(\alpha, \beta)$ and a unit speed planet dance $\mathcal{P}_2 = \mathcal{P}(1, a)$, let $m = |\alpha a - \beta|$. Then the modular multiplication table MMT(m, a) will be an m -regular sampling of \mathcal{P}_1 .*

A sampling of a planet dance $\mathcal{S}(\alpha, \beta, m)$ can be realized as a modular multiplication table exactly when

$$m = |\alpha a - \beta|$$

for some positive integer a . We break this into two cases: $\alpha a - \beta = m$ or $\alpha a - \beta = -m$. Then we see that either

$$\beta \equiv m \pmod{\alpha} \quad \text{or} \quad m + \beta \equiv 0 \pmod{\alpha}.$$

If you choose a general planet dance $\mathcal{P}(\alpha, \beta)$, and a desired approximate sampling rate, then I can give you a modular multiplication table (m, a) with m “close” to your sampling rate so that

$\text{MMT}(m, a)$ is an m -sampling of $\mathcal{P}(\alpha, \beta)$. This “closeness” depends on α —we choose the nearest m such that $m \equiv \beta \pmod{\alpha}$ or $m + \beta \equiv 0 \pmod{\alpha}$.

So this answers our question stated in Section 2 for all planet dances. Given any planet dance $\mathcal{P}(\alpha, \beta)$, we can find a corresponding family of MMTs which are all samplings of $\mathcal{P}(\alpha, \beta)$. This also elucidates why certain MMTs exhibit patterns which are very different from the unit-speed planet dance given by the Fundamental Correspondence Lemma. When an MMT (m, a) is viewed as an m -sampling of $\mathcal{P}(1, a)$, if m is an “under-sampling” then $\text{MMT}(m, a)$ will alias as a sampling of another planet dance.

But this correspondence is only the tip of the iceberg. In the next section, we see how MMTs can present as planet dances which are outside of our definition. This will mirror the way that samplings of unit speed planet dances can represent modular multiplication tables which have fractional multipliers.

5 Overlaying Patterns

Now we return to the patterns in modular multiplication tables that we noticed in Section 2. Assuming that m is even, we observed that tables of the form $\text{MMT}(m, \frac{m}{2})$ or $\text{MMT}(m, \frac{m}{2} + 1)$ or $\text{MMT}(m, \frac{m}{2} - 1)$ each have a distinct form which holds for all such m (recall Figures 5, 6, and 7).⁶ A natural generalization is to replace ‘2’ with any natural number b . That is, supposing that m is divisible by b , we study three classes of tables:

$$(m, \frac{m}{b}), \quad (m, \frac{m}{b} + 1), \quad \text{and} \quad (m, \frac{m}{b} - 1).$$

Each of these classes of tables demonstrate interesting patterns that are generalizations of those when $b = 2$. Examples of these classes of tables are shown in Figure 13.

Remark 5.1. To avoid the assumption that m is divisible by b , it might make for a simpler description to start by choosing a multiplier a . Then we could describe these tables as (ba, a) , $(ba - b, a)$, and $(ba + b, a)$. However, in order to keep the narrative of discovery coherent, we will keep the perspective above for now.

As I was considering these classes of tables, I wondered if we could define a similar kind of MMT without the assumption that m was divisible by b . I decided to look at MMTs where $b \nmid m$ and $a = \lceil \frac{m}{b} \rceil$ or $a = \lfloor \frac{m}{b} \rfloor$, since I still wanted a to be an integer. I was amazed to find a very regular pattern in tables of this form. Figure 14 shows tables of the form $\text{MMT}(m, \lceil \frac{m}{b} \rceil)$. The rows are indexed by the value for b and the columns are indexed by the remainder of $m \pmod{b}$. I encourage the reader to take a minute and find patterns within this “table of tables”.

I discovered these patterns before considering MMTs from the perspective of planet dances. But now, with this other perspective, the mysteries are unraveled. Let $m \equiv r \pmod{b}$. Then we can write $a = \lceil \frac{m}{b} \rceil$ as

$$a = \frac{m + (b - r)}{b}.$$

If we do some algebraic rearranging, then we have the relationship

$$\begin{aligned} ba &= m + b - r \\ ba - (b - r) &= m \end{aligned}$$

⁶We didn’t prove that it holds for all m , but this is straightforward to see.

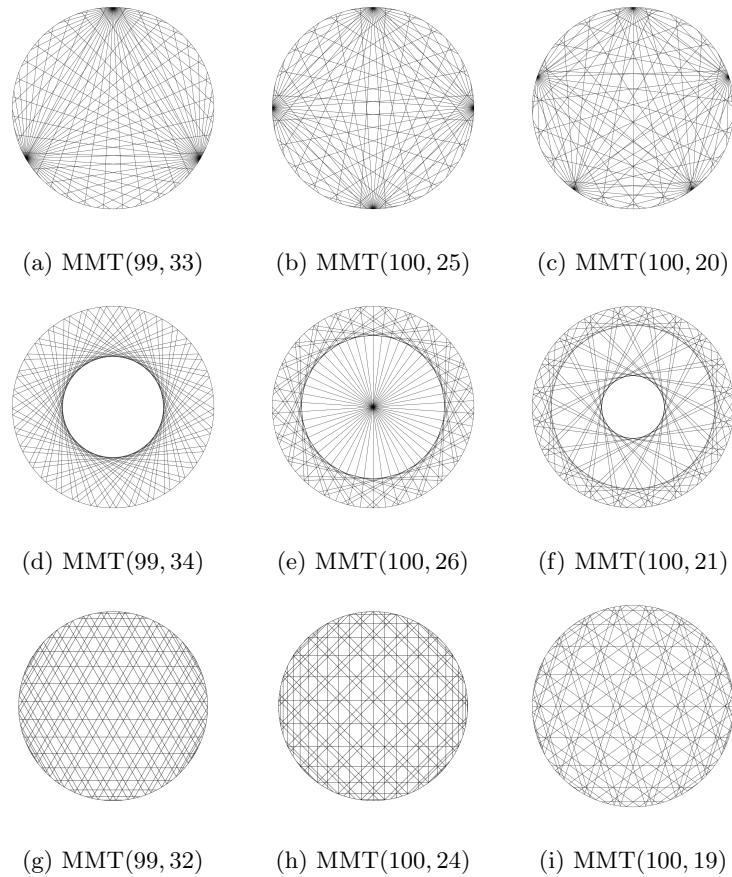


Figure 13: The top row shows examples of tables of the form $(m, \frac{m}{b})$ with $b = 3, 4$, and 5 from left to right. The second row shows examples of tables of the form $(m, \frac{m}{b} + 1)$ with the same b values. The last row shows tables of the form $(m, \frac{m}{b} - 1)$ again with the same values for b .

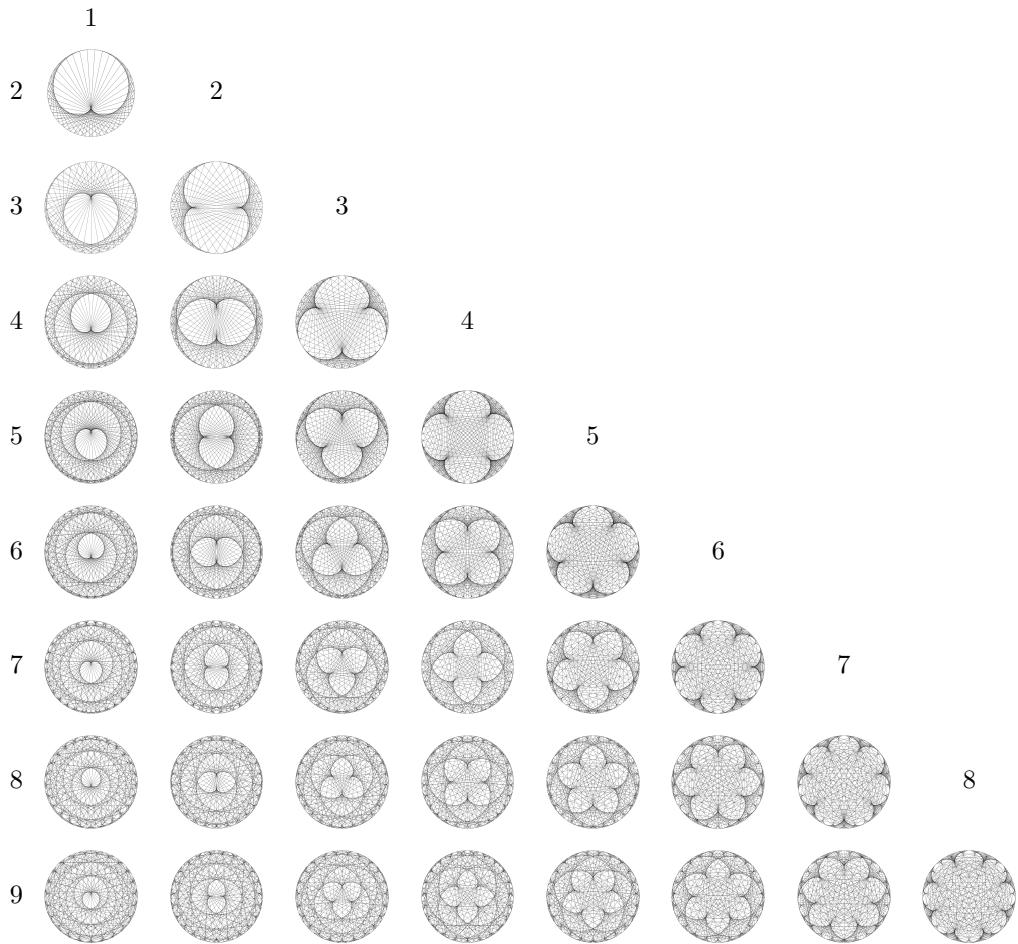


Figure 14: A “table of tables”! Each table is of the form $(m, \lceil \frac{m}{b} \rceil)$ for some positive integers with $b < m$. The rows are indexed by the value for b and the columns are indexed by r where $m \equiv r \pmod{b}$. We have taken m to be relatively large so as to see the pattern clearly. Most values for m are approximately 100.

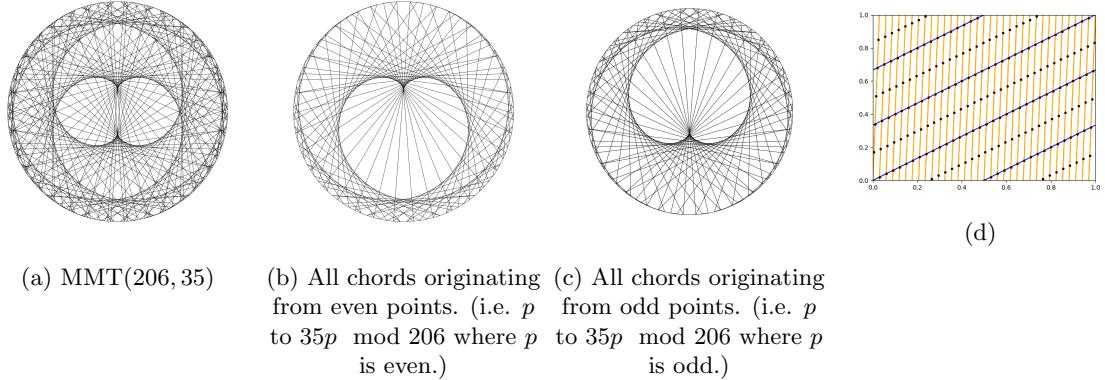


Figure 15: MMT(206, 35) “reduces” to two copies of MMT(103, 35), one rotated halfway around the circle. Figure 15d depicts the corresponding linear torus loops. The orange lines represent $\mathcal{P}(1, 35)$, with the black dots showing a sampling at rate 206. The blue lines represent $\mathcal{P}(3, 2)$.

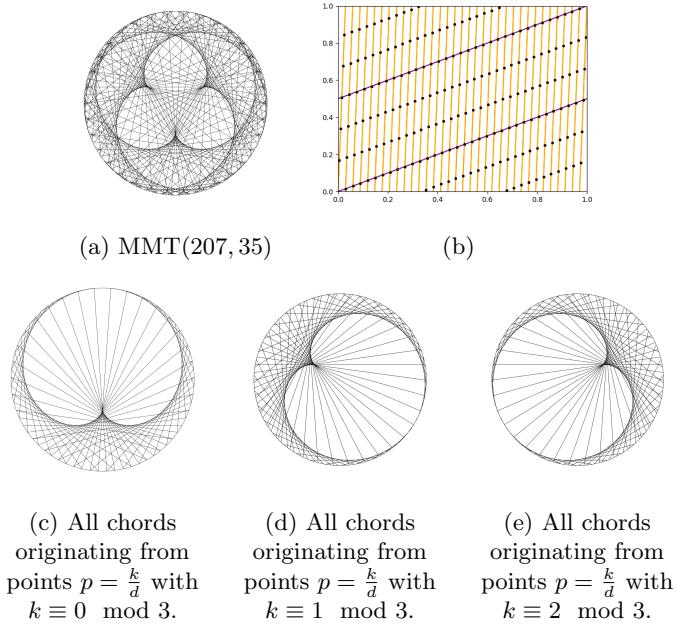


Figure 16: MMT(207, 35) “reduces” to three copies of MMT(69, 35) one rotated a third around the circle and one rotated two thirds. Figure 16b depicts the corresponding linear torus loops. The orange lines represent $\mathcal{P}(1, 35)$, with the black dots showing a sampling at rate 207. The blue lines represent $\mathcal{P}(2, 1)$.

With our knowledge about the intersection number of linear loops on the torus, we recognize that the above equation says that $\mathcal{P}(b, b-r)$ and $\mathcal{P}(1, a)$ will intersect m times. However, there is one missing link: this is only true if both planet dances are in reduced form. That is, if $\gcd(b, b-r) = 1$. In this case, $\text{MMT}(m, a)$ will be an m -sampling of $\mathcal{P}(b, b-r)$ by Theorem 4.4. We have already seen one example of this case: when $b = 3$ and $r = 1$. If we set $a = 34$, then $m = 3 \cdot 34 - 2 = 100$. Following the discussion in Section 4.3, $\text{MMT}(100, 34)$ is a 100-sampling of $\mathcal{P}(3, 2)$.

Corollary 5.2. *Let m and b be positive integers with $b < m$ such that $b \nmid m$. Let $m \equiv r \pmod{b}$ for $0 < r < b$. If $\gcd(r, b) = 1$, then $\text{MMT}(m, \lceil \frac{m}{b} \rceil)$ will be an m -regular sampling of $\mathcal{P}(b, b-r)$.*

However, it may be the case that $\gcd(b, b-r) = d > 1$. Upon examination of the “table of tables”, one might notice that many of the images look like “overlays” of others. For example, when $r = 2$ and $b = 6$, the design looks like two copies of the pattern when $r = 1$ and $b = 3$, but one copy is rotated halfway around the circle. I observed this when I first found this family of tables and I decided to test my idea experimentally. Figure 15 shows a member of the $r = 2, b = 6$ family ($\text{MMT}(206, 35)$) along with two subsets of this MMT. The first shows only the chords originating from even points (Figure 15b) and the second shows only the chords originating from odd points (Figure 15c). Another example of this overlay phenomenon is shown in Figure 16a.

Every example that I tested gave the same result. When $\gcd(b, b-r) = d$, the table $\text{MMT}(m, \lceil \frac{m}{b} \rceil)$ consisted of d copies of $\text{MMT}(\frac{m}{d}, \lceil \frac{m}{b} \rceil)$, rotated symmetrically around the circle. I managed to devise a number theoretic proof of this fact but it wasn’t very illuminating. With our topological perspective, we can see what is going on more clearly. When we draw the corresponding linear torus loops for the examples in Figures 15 and 16, we see that the sampling points trace out copies of $\mathcal{P}(b, b-r)$ which are shifted. Although we do not get these linear loops from the planet dance construction, they do appear by sampling.

The following theorem addresses a general case of these “overlay” tables, which we will then apply to our specific example.

Theorem 5.3. *Let $\mathcal{P}(\alpha, \beta)$ be a planet dance in reduced form with $\alpha \neq 0$ and let $a \in \mathbb{Z}$ be any integer. For $m = |\alpha a - \beta|$ we have $\mathcal{S}(\alpha, \beta, m) = \mathcal{S}(1, a, m)$ by Proposition 4.4. Then, for any positive integer d , $\mathcal{S}(1, a, dm)$ consists of d sets $\mathcal{S}(\alpha, \beta, m)$, each one rotated by $\frac{k}{(\alpha-\beta)d}$ around the circle for $k = 0, 1, \dots, d-1$.*

Proof. We will think of all points and lines as lying in $\mathbb{R}^2/\mathbb{Z}^2$ but we will use coordinates for \mathbb{R}^2 to simplify notation. Recall that $\mathcal{P}(\alpha, \beta)$ is given by a line in $\mathbb{R}^2/\mathbb{Z}^2$ with the parametric equations

$$x = \alpha t, \quad y = \beta t, \quad \text{or} \quad y = \frac{\beta}{\alpha}x \quad \text{since } \alpha \neq 0.$$

Let $P = \{p_0, p_1, \dots, p_{m-1}\} \subset T^2$ be the set of sample points of $\mathcal{S}(1, a, m)$, ordered so that $p_j = (\frac{j}{m}, a \frac{j}{m})$. Let $Q = \{q_0, q_1, \dots, q_{dm-1}\} \subset T^2$ be the set of sample points of $\mathcal{S}(1, a, dm)$, ordered in the same way. For each $0 \leq k \leq d-1$, we define $Q_k := \{q_j \in Q \mid j \equiv k \pmod{d}\}$. Notice that $Q_0 = P$, so all points in Q_0 lie on the line $x = \alpha t, y = \beta t$ since $\mathcal{S}(1, a, m) = \mathcal{S}(\alpha, \beta, m)$.

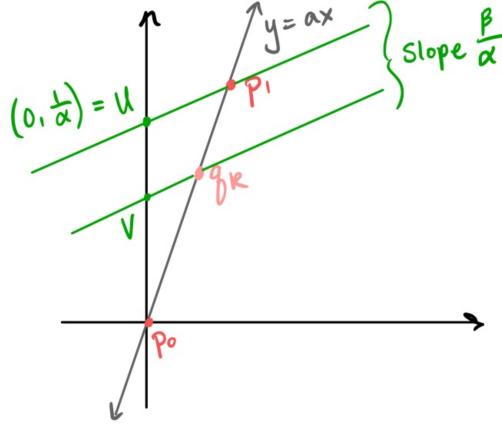


Figure 17: The point q_k lies between p_0 and p_1 on the line $y = ax$. We can use the Triangle Proportionality Theorem to find the point V .

We claim that all points in Q_k lie on the line given by

$$x = \alpha t, \quad y = \beta t + \frac{k}{d\alpha}. \quad (2)$$

First, all points $p_j \in P$ are colinear and lie on the line $y = ax$ because they are sampling points of $\mathcal{P}(1, a)$. Since the sampling is regular, $\|p_j - p_{j+1}\|$ is the same for all j . Let $L = \|p_0 - p_1\|$. Given $p_j \in P$, we have $q_{jd+k} \in Q_k$, because of the regular sampling, we know that

$$q_{jd+k} = p_j + \frac{k}{L\sqrt{1+a^2}} \begin{pmatrix} 1 \\ a \end{pmatrix}.$$

In particular, the part that we add to p_j is invariant of j . Since $P = Q_0$ is a set of colinear points lying on the line $y = \frac{\beta}{\alpha}x$ and translating a line leaves the slope invariant, we conclude that Q_k lies on a line of the form

$$y = \frac{\beta}{\alpha}x + C_k$$

where C_k is a constant. We then use the Triangle Proportionality theorem to find the y -intercept of the line. See Figure 17. To do this, we extend a line with slope $\frac{\beta}{\alpha}$ from the point q_k and determine where it intersects the y -axis. Note that q_k sits between the points p_0 and p_1 on the line $y = ax$. Extending a line of slope $\frac{\beta}{\alpha}$ from p_1 , we know it will intersect the y -axis at the point $(0, \frac{1}{\alpha})$. Let U and V be the points labeled in Figure 17. Then, by the Triangle Proportionality Theorem, we have

$$\frac{\|U - V\|}{\|V\|} = \frac{\|p_1 - q_k\|}{\|q_k\|}.$$

Using the fact that $\frac{\|p_1 - q_k\|}{\|q_k\|} = \frac{d-k}{k}$ by construction and that $\|U - V\| = \|U\| - \|V\|$ since U , V , and 0 are all colinear, we find that

$$\frac{k}{d}\|U\| = \|V\|.$$

Thus, we have $V = \frac{k}{d\alpha}$. And this shows that all points in Q_k lie on the line given by (2).

The last step is to show why the line given by (2) is a copy of $\mathcal{P}(\alpha, \beta)$ rotated by $\frac{k}{d(\alpha-\beta)}$. We notice that every planet dance $\mathcal{P}(\alpha, \beta)$ starts at $t = 0$ with both planets in the same position, and this can be seen as an intersection with $\mathcal{P}(1, 1)$. But since (2) has a non-zero y -intercept, the corresponding planets will start at different positions at $t = 0$. So we find a point of intersection between the line (2) with $\mathcal{P}(1, 1)$ and this will give the rotation amount.

$$\begin{aligned}\alpha t &= \beta t + \frac{k}{d\alpha} \\ (\alpha - \beta)t &= \frac{k}{d\alpha} \\ t &= \frac{k}{d\alpha(\alpha - \beta)}\end{aligned}$$

And then we find $x = y = \frac{k}{d(\alpha-\beta)}$ at this value for t . \square

Now we apply this general theory of overlays to extend Corollary 5.2 to cases where $\gcd(r, b) > 1$. We give an explicit description for tables of the form $\text{MMT}(m, \lceil \frac{m}{b} \rceil)$ and $\text{MMT}(m, \lfloor \frac{m}{b} \rfloor)$.

Proposition 5.4. *Let m and b be positive integers with $b < m$ such that $b \nmid m$. Let $m \equiv r \pmod{b}$ for $0 < r < b$ and let $d = \gcd(r, b)$. Then:*

- the table $\text{MMT}(m, \lceil \frac{m}{b} \rceil)$ is composed of d sets $\mathcal{S}(\frac{b}{d}, \frac{b-r}{d}, \frac{m}{d})$, each one rotated by $\frac{k}{r}$ around the circle for $0 \leq k \leq d-1$;
- the table $\text{MMT}(m, \lfloor \frac{m}{b} \rfloor)$ is composed of d sets $\mathcal{S}(\frac{b}{d}, \frac{-r}{d}, \frac{m}{d})$, each one rotated by $\frac{k}{r}$ around the circle for $0 \leq k \leq d-1$.

6 Some more patterns to explore

Now that we have built a framework to understand why certain patterns appear in modular multiplication tables, we can return to the variety of patterns shown in Figure 1. In this Section, I have included images of these different families of tables along with the correlating sampled torus loop. I encourage the reader to think about why the different patterns appear based on our discussion in the previous sections.

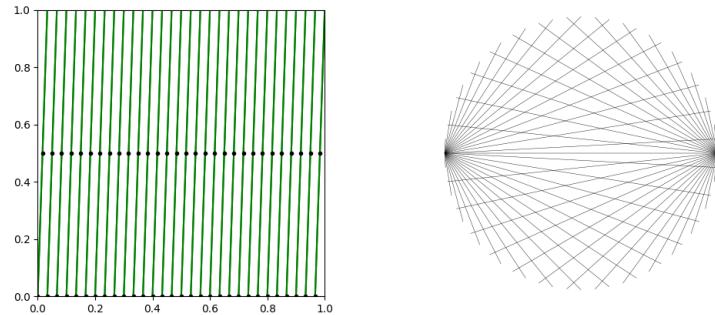


Figure 18: A table of the form $\text{MMT}(2a, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $2a$.

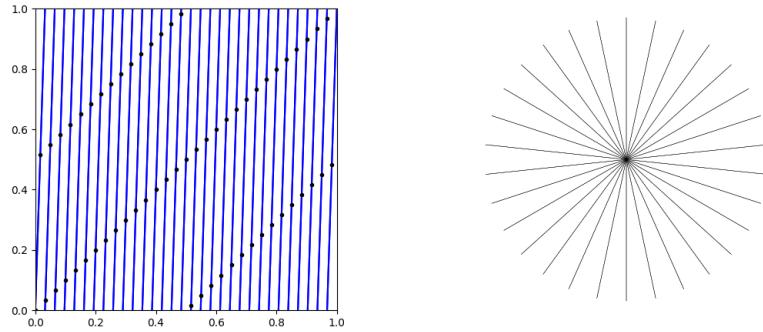


Figure 19: A table of the form $\text{MMT}(2a - 2, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $2a - 2$.

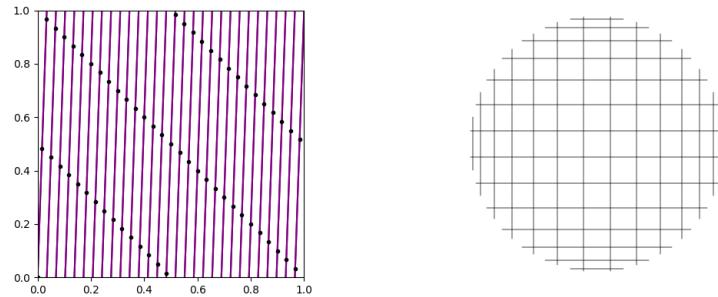


Figure 20: A table of the form $\text{MMT}(2a + 2, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $2a + 2$.

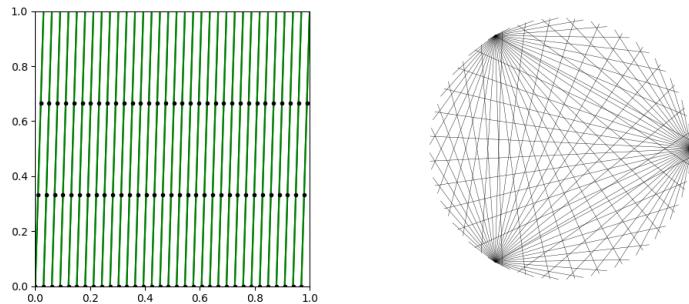


Figure 21: A table of the form $\text{MMT}(3a, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $3a$.

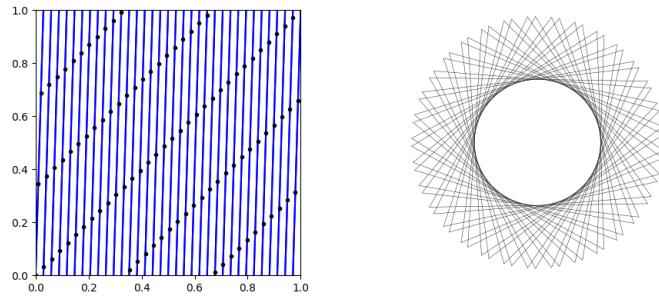


Figure 22: A table of the form $\text{MMT}(3a - 3, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $3a - 3$.

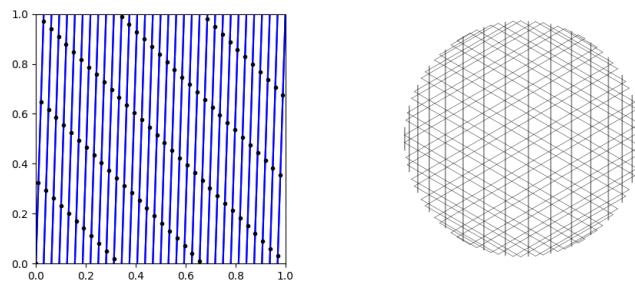


Figure 23: A table of the form $\text{MMT}(3a + 3, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $3a + 3$.

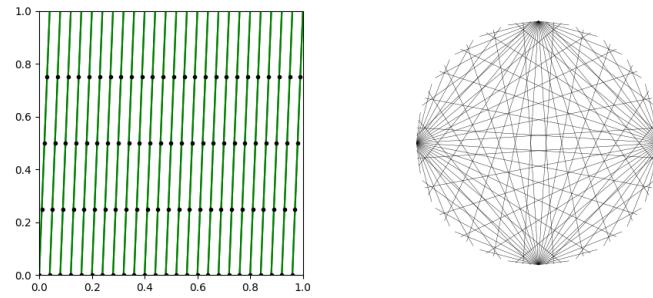


Figure 24: A table of the form $\text{MMT}(4a, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $4a$.

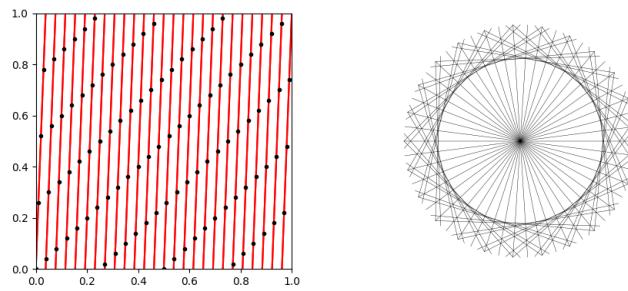


Figure 25: A table of the form $\text{MMT}(4a - 4, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $4a - 4$.

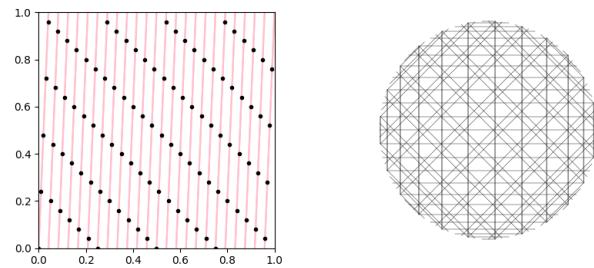


Figure 26: A table of the form $\text{MMT}(4a + 4, a)$ along with $\mathcal{P}(1, a)$ sampled at rate $4a + 4$.

References

- [1] B. Polster, “Times tables, mandelbrot, and the heart of mathematics,” *Mathologer, YouTube*, Nov 2015.
- [2] B. Haran and M. Henderson, “The strange orbit of earth’s second moon (plus the planets),” *Numberphile, YouTube*, Sep 2021.
- [3] A. J. Simoson, “An envelope for a spirograph,” *College Mathematics Journal*, vol. 28, pp. 134–139, 1997.
- [4] M. Hopkins, “The envelope of a line moving between two concentric circles,” *The Mathematics Teacher*, vol. 43, no. 6, pp. 264–268, 1950.
- [5] J. A. Boyle, “Using rolling circles to generate caustic envelopes resulting from reflected light,” *The American Mathematical Monthly*, vol. 122, no. 5, pp. pp. 452–466, 2015.
- [6] A. I. Robold and P. Yff, “From curve stitching to epicycloids,” *School Science and Mathematics*, vol. 96, no. 7, pp. 350–354, 1996.
- [7] M. Lengler, *TimesTableWebGL*.
- [8] M. Bouthillier, “Representations of epitrochoids and hypotrochoids,” April 2018.