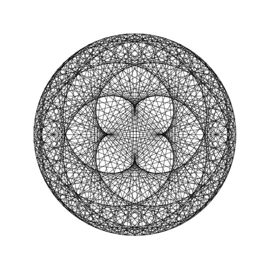
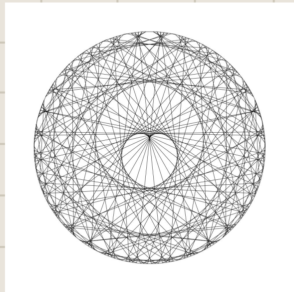
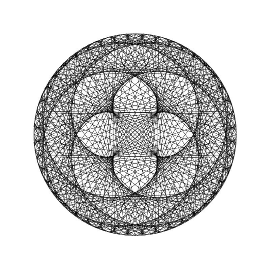
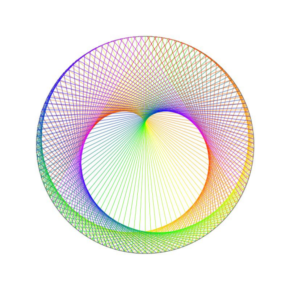
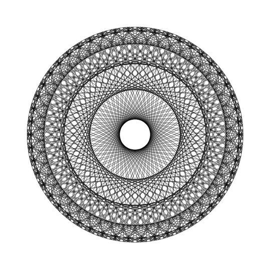
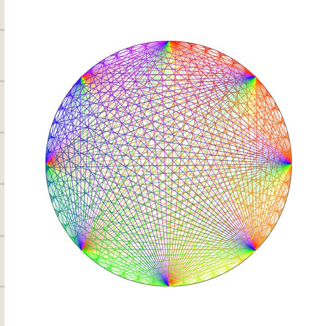
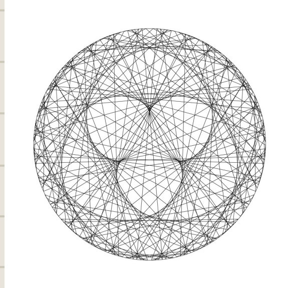
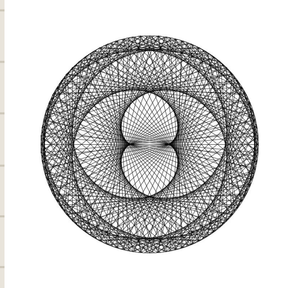





Modular Multiplication and Dancing Planets

Fran Herr

herrf@uchicago.edu

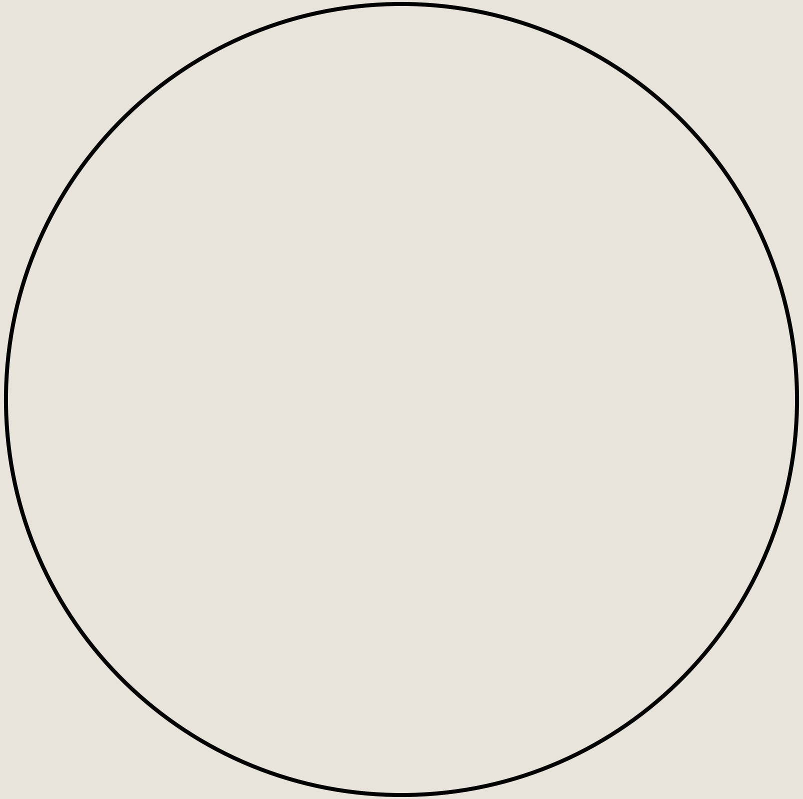
Outline

1. Modular Multiplication Tables
2. Dancing Planets
3. A topological perspective

Construct
MMT(m, a)

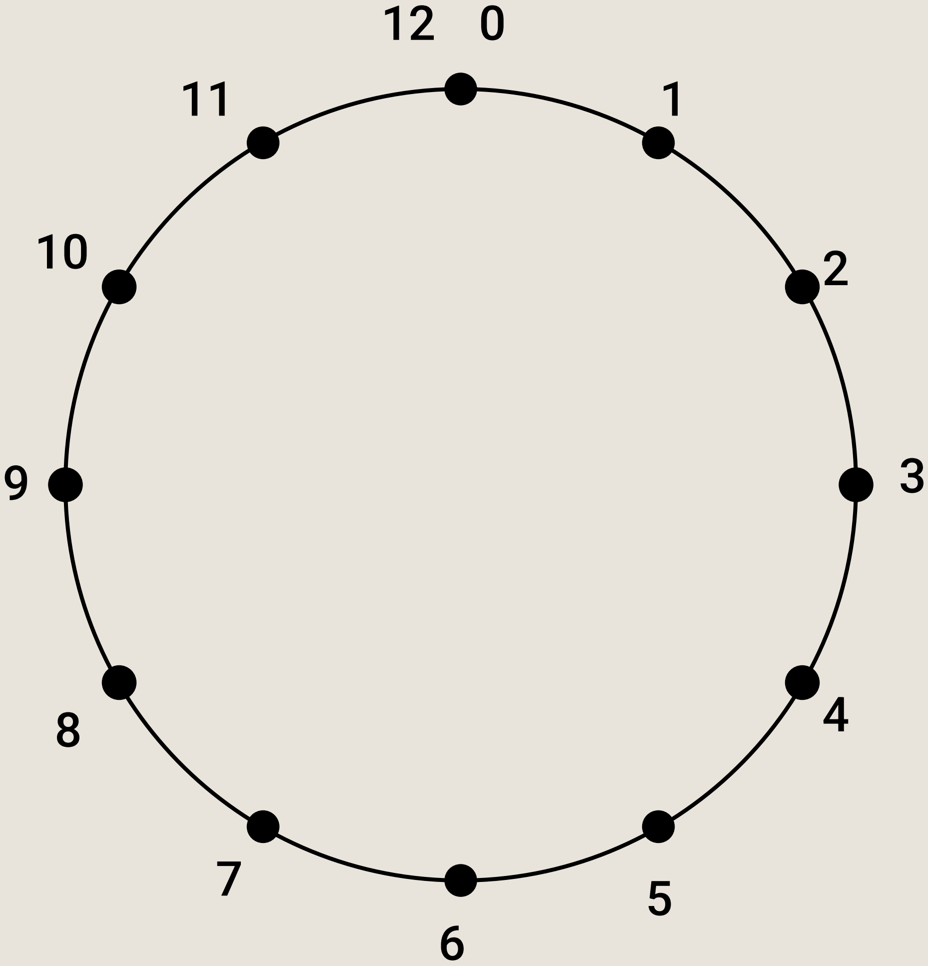
m = modulus
a = multiplier

MMT(12, 2)



Construct MMT(m, a)

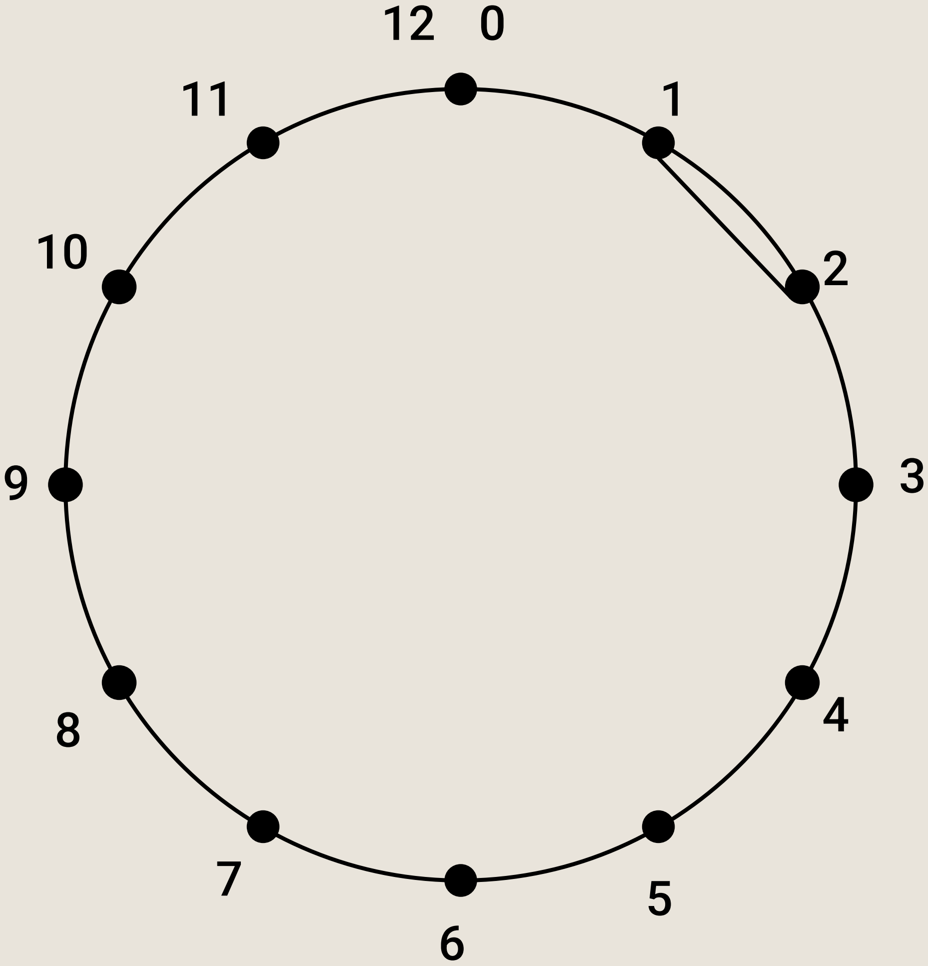
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m, a)

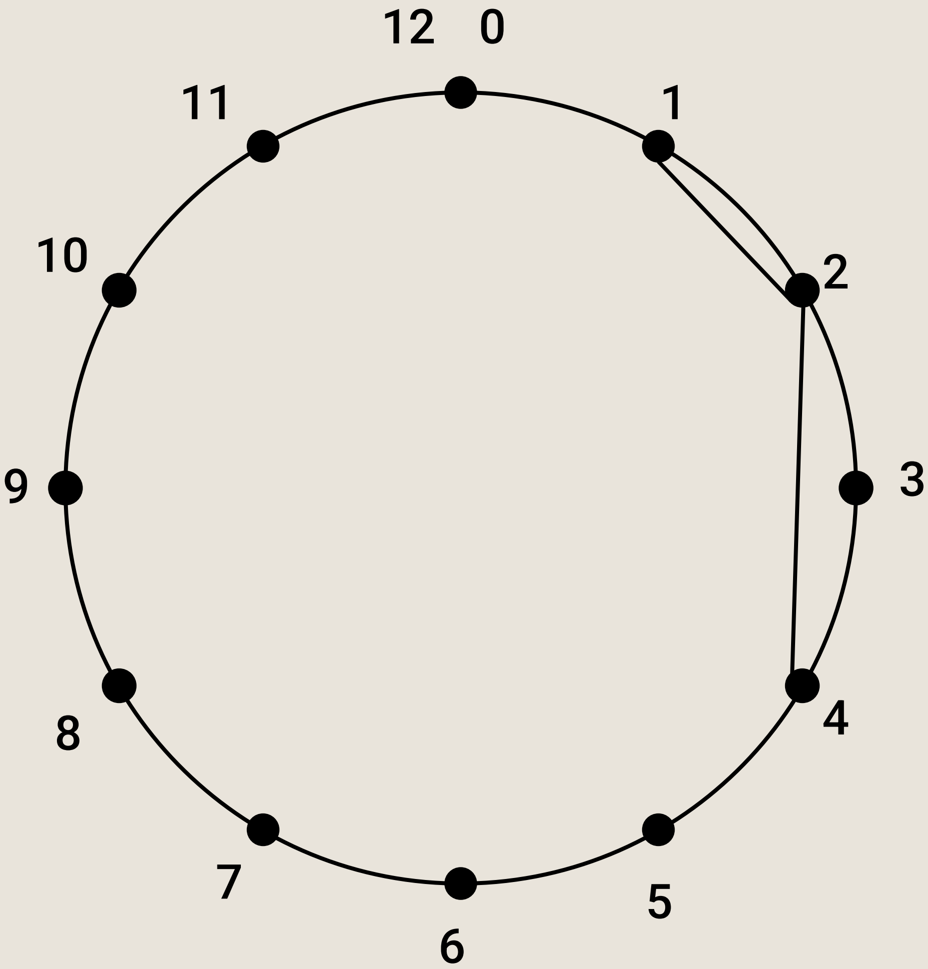
MMT(12, 2)



m = modulus
a = multiplier

Construct
MMT(m, a)

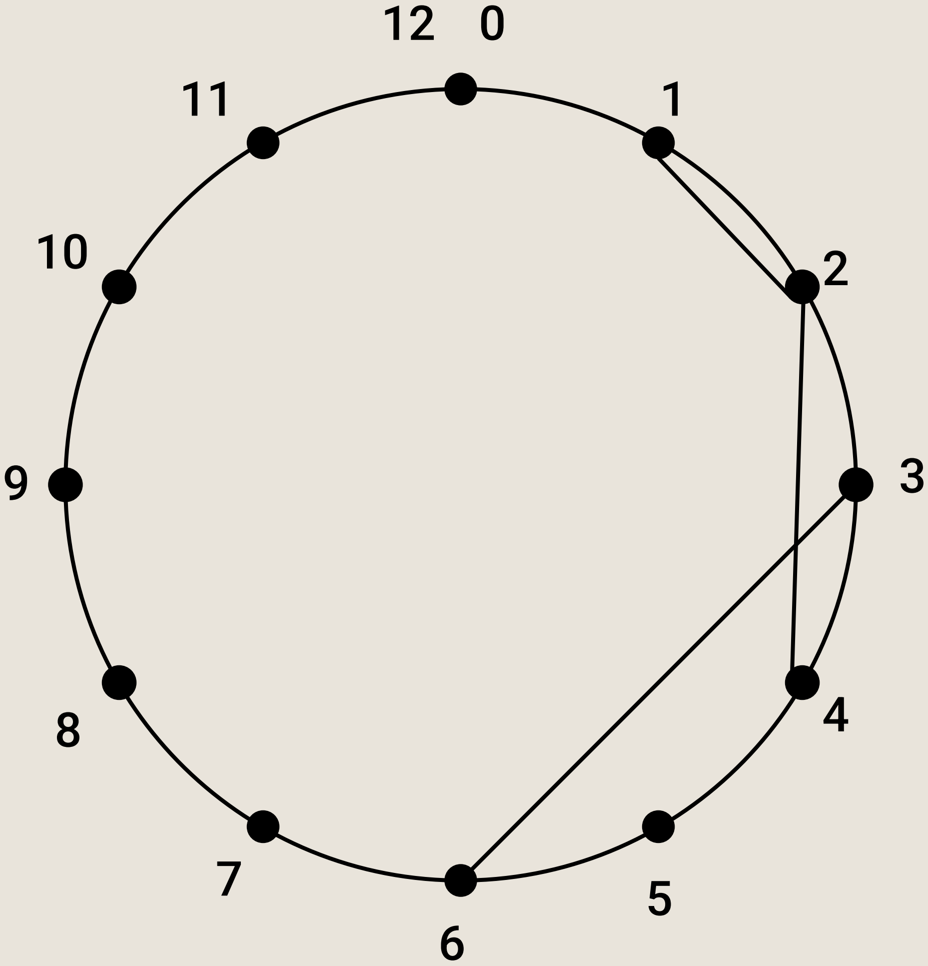
MMT(12, 2)



m = modulus
a = multiplier

Construct
MMT(m, a)

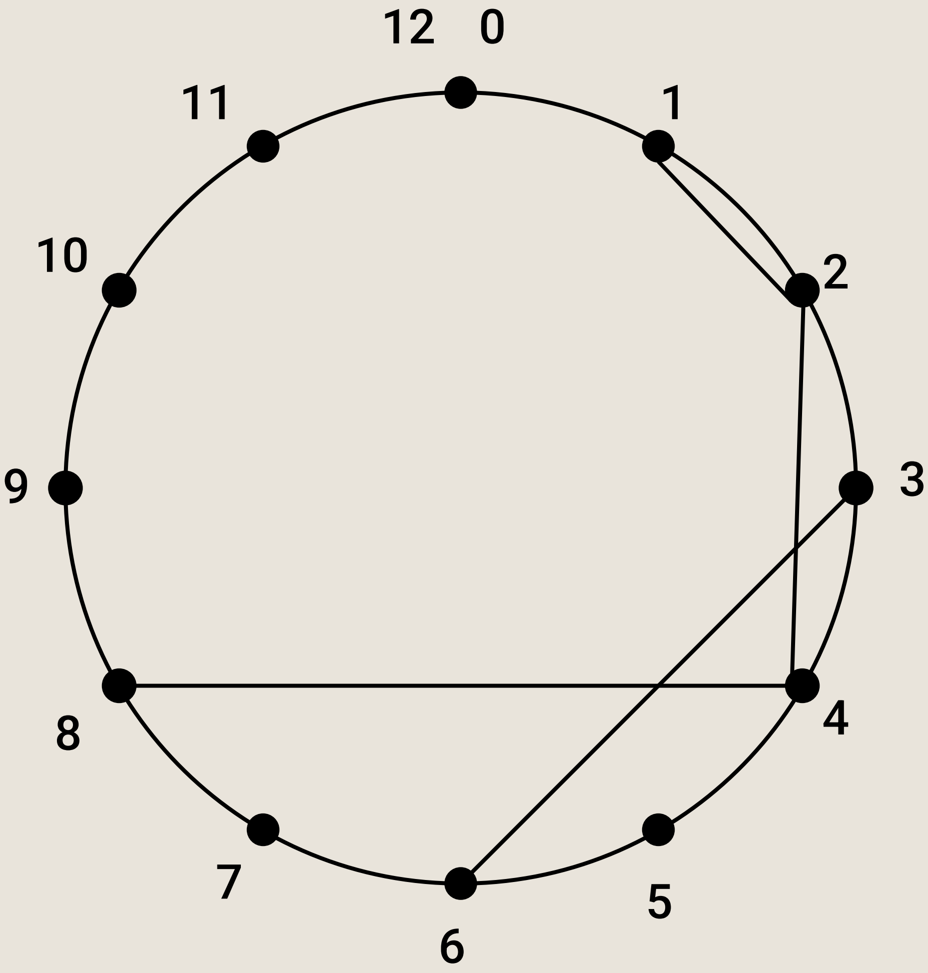
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m, a)

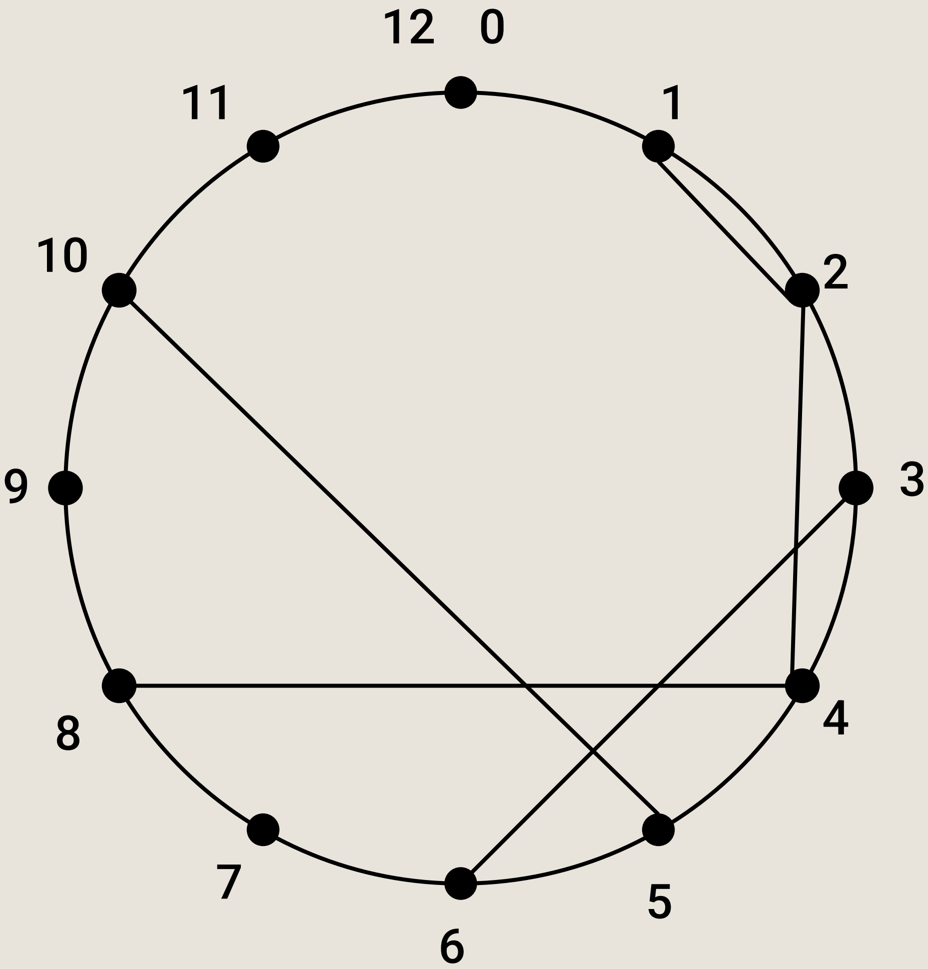
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m,a)

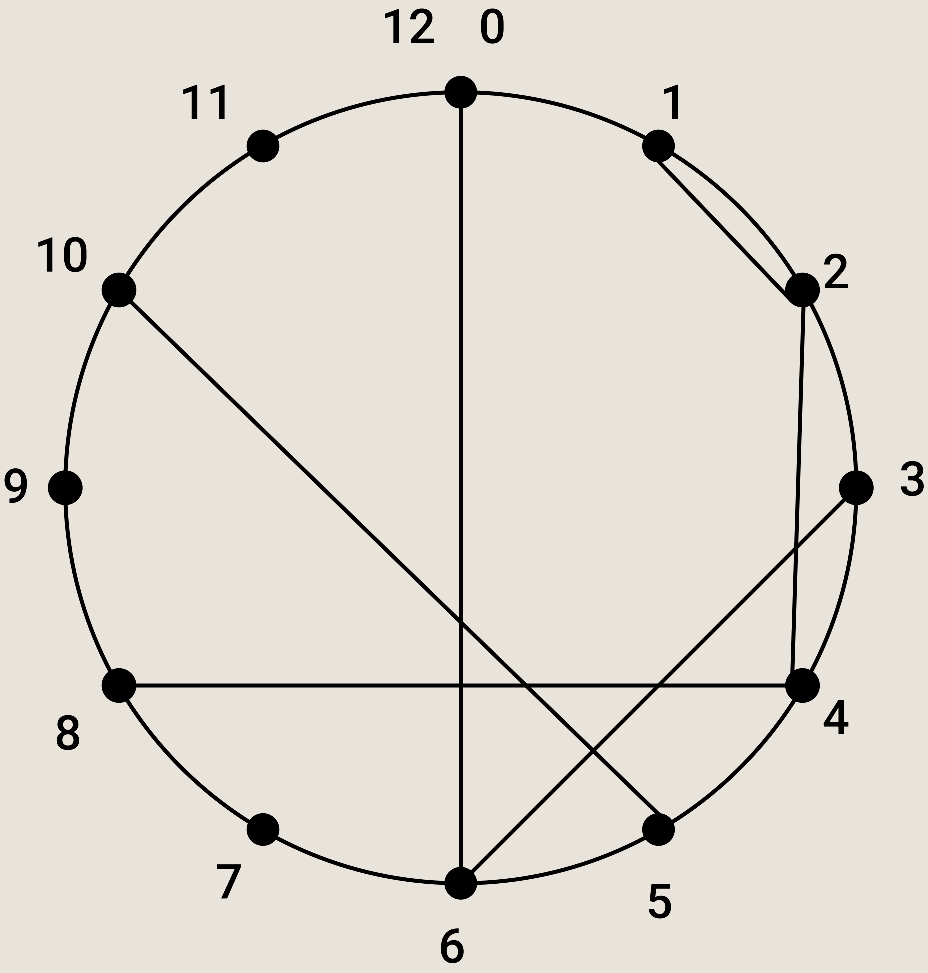
MMT(12, 2)



m = modulus
a = multiplier

Construct
MMT(m, a)

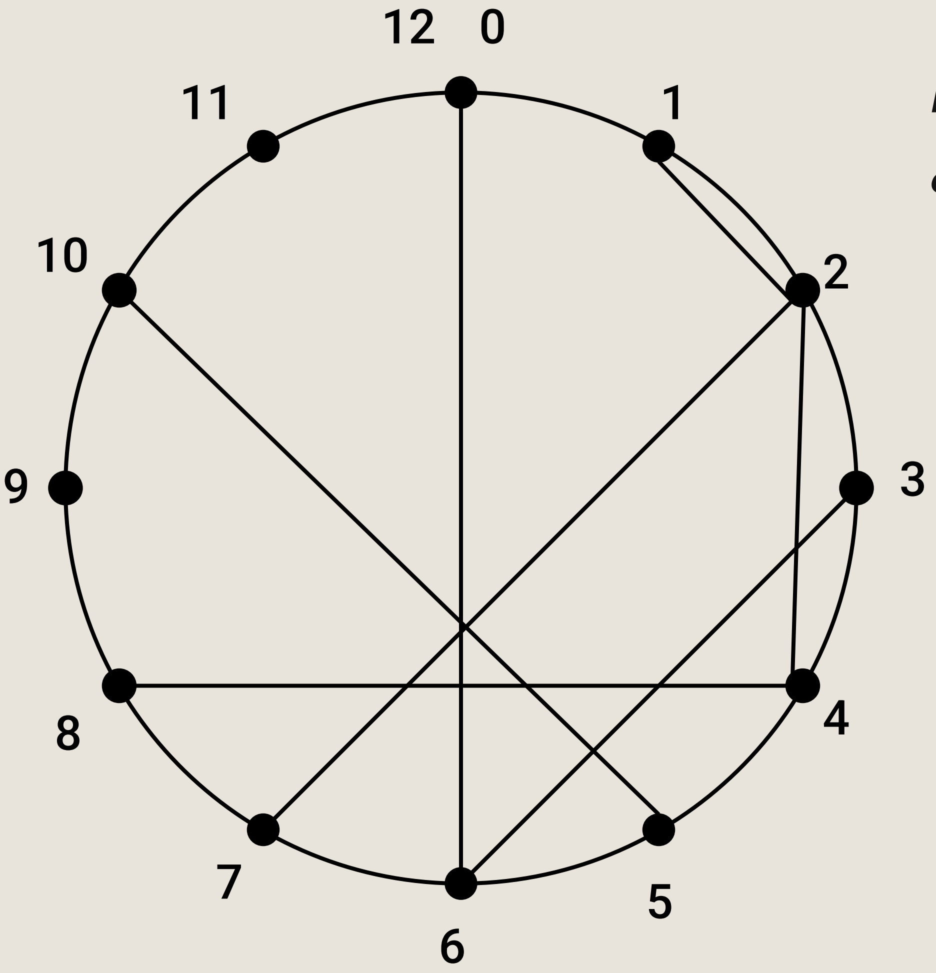
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m,a)

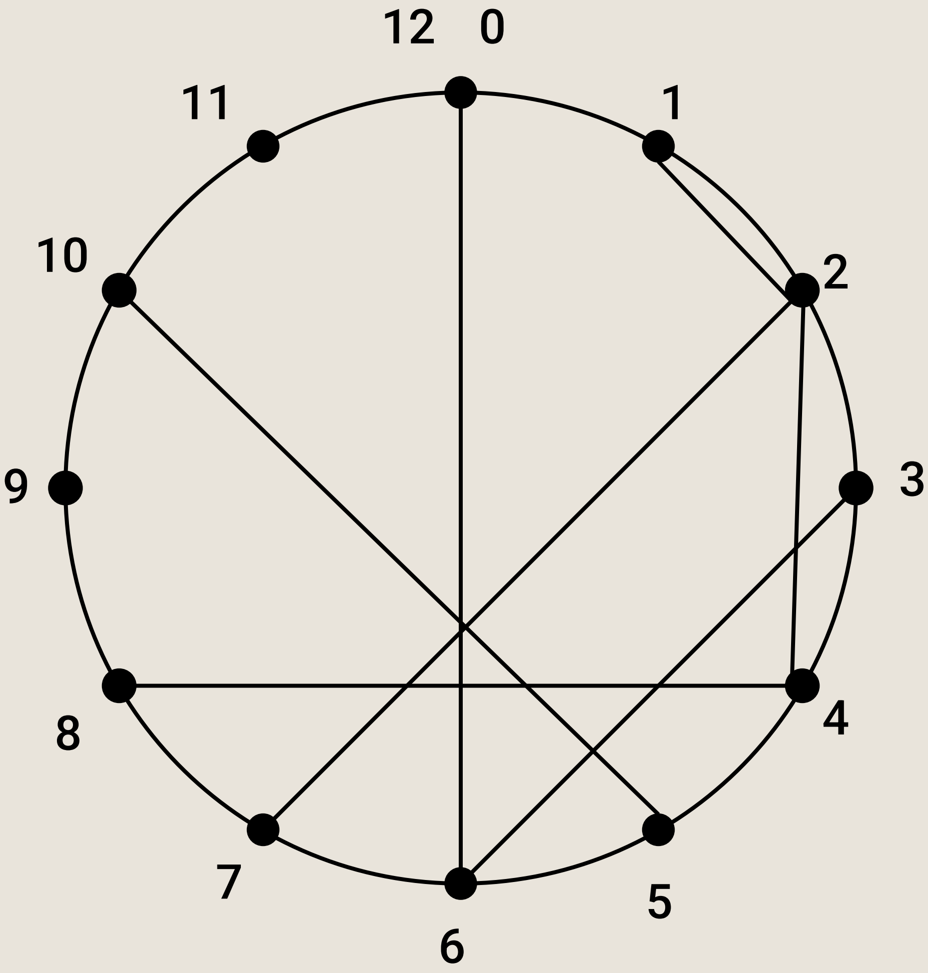
MMT(12, 2)



m = modulus
a = multiplier

Construct
MMT(m,a)

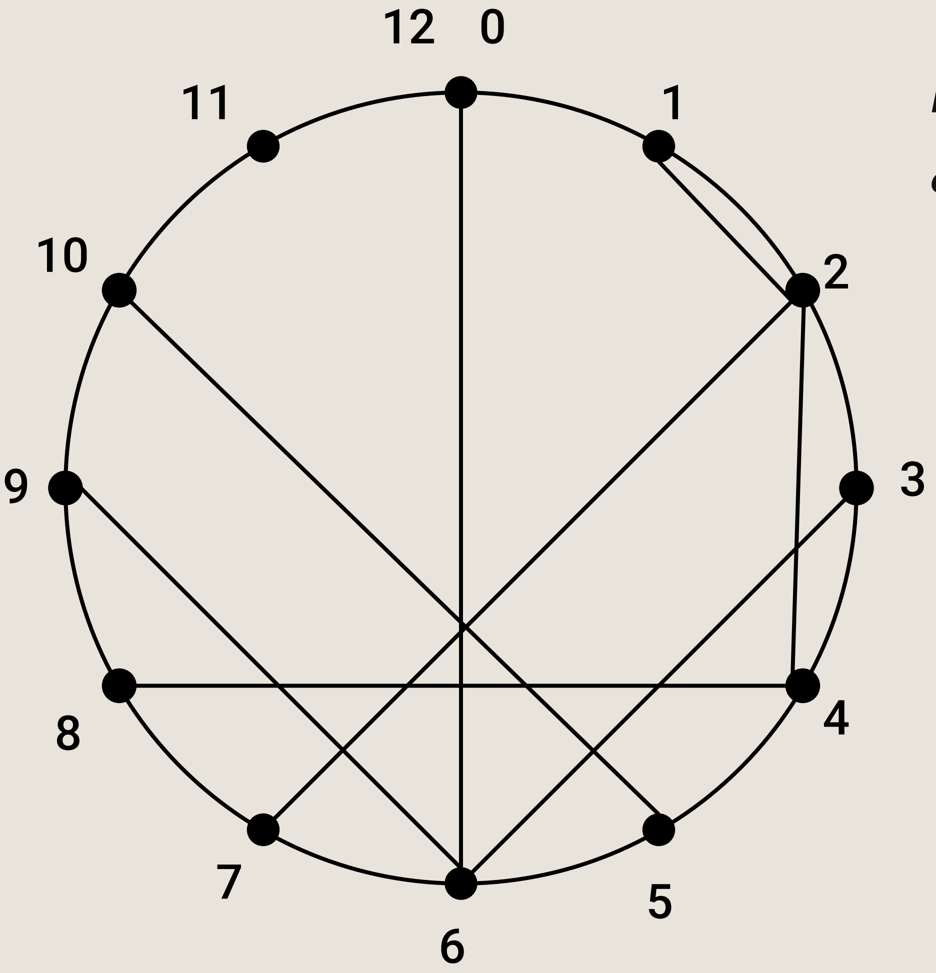
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m, a)

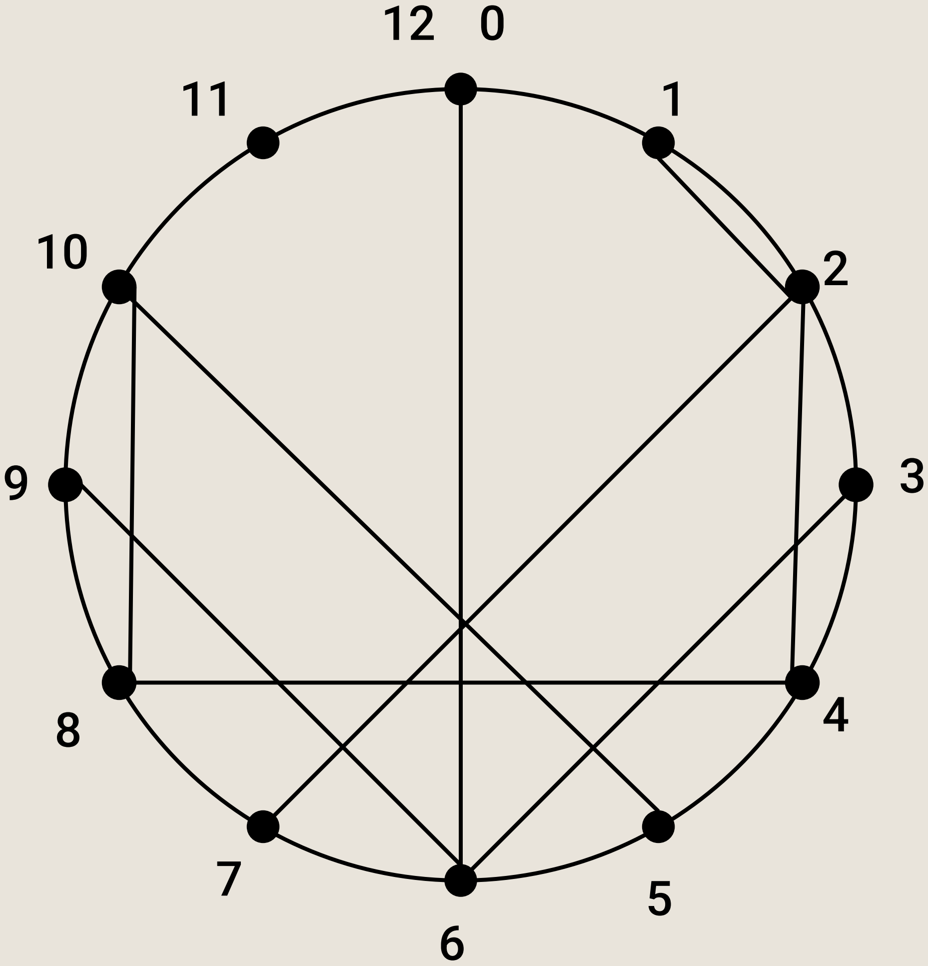
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m,a)

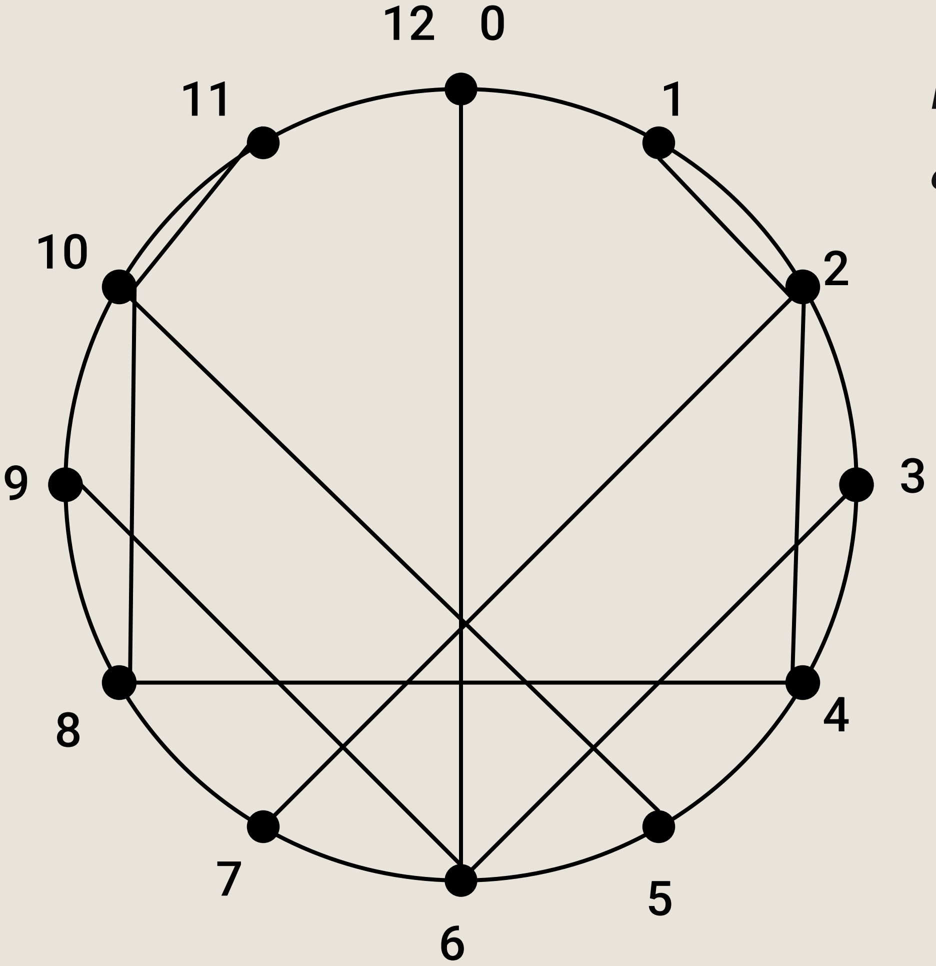
MMT(12, 2)



m = modulus
a = multiplier

Construct MMT(m, a)

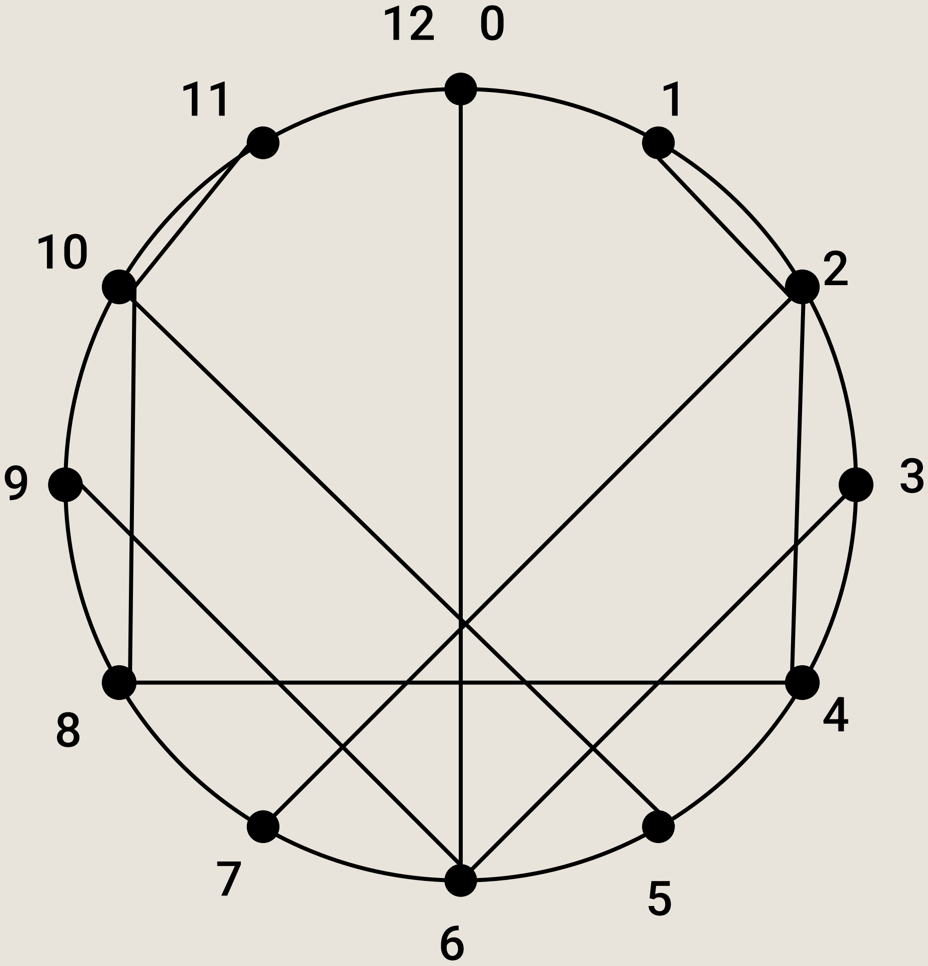
MMT(12, 2)



m = modulus
a = multiplier

Construct
MMT(m, a)

MMT(12, 2)



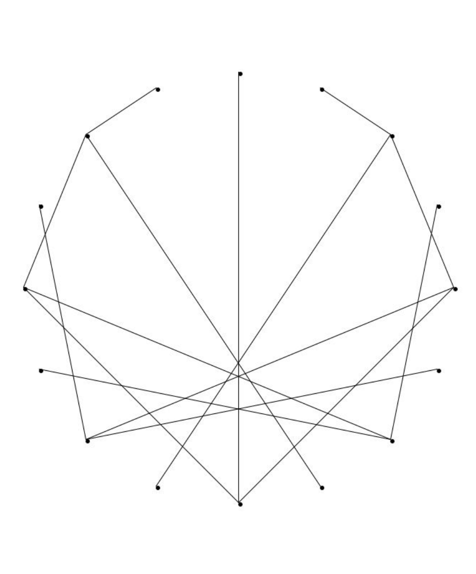
m = modulus
a = multiplier

Big Question: Given m and a, what does MMT(m, a) look like?

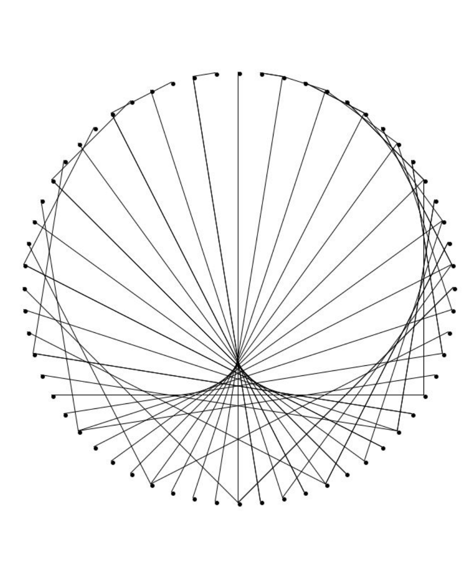
https://times-tables.lengler.dev/

First, fix a at a “sr … nd increase m.

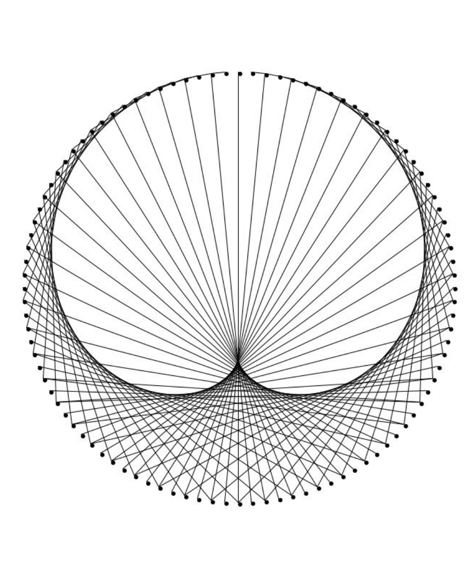
MMT(16,2)

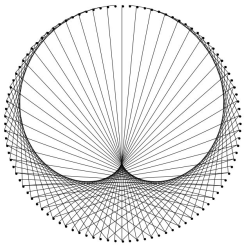


MMT(50,2)

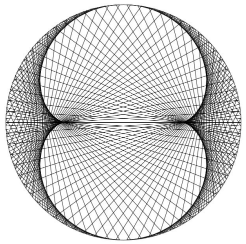


MMT(100,2)

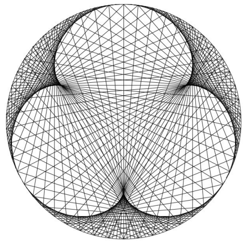




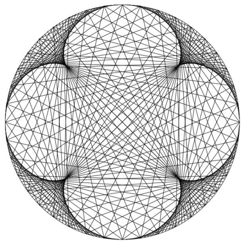
a = 2



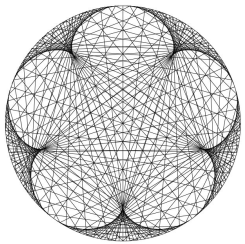
a = 3



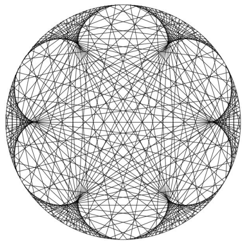
a = 4



a = 5



a = 6



a = 7

Guess: For large enough m, MMT(m, a) looks like a curve with a-1 "petals".

Epicycloid:

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

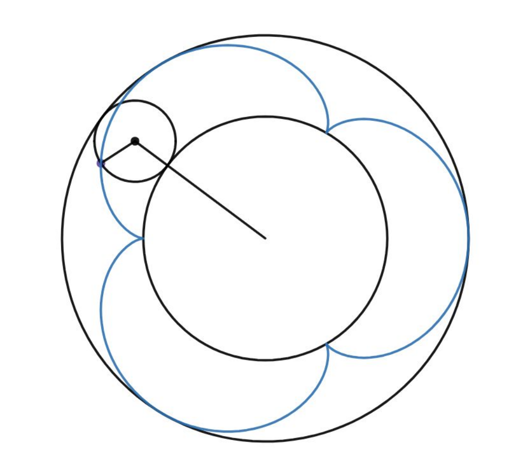
$$y(t) = \alpha \sin t + \beta \sin\left(\frac{\alpha}{\beta} t\right)$$

https://www.desmos.com/calculator/dbbfkfgp1w

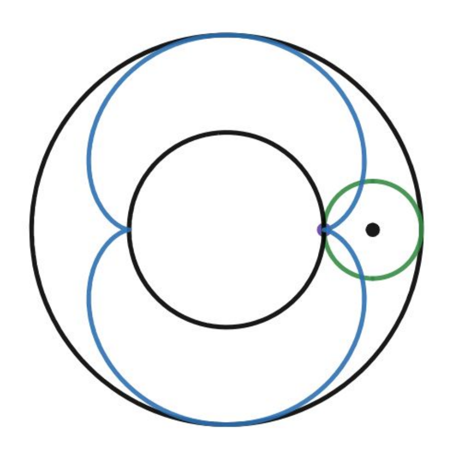
https://www.desmos.com/calculator/mjjv8abvbo

Epicycloid:

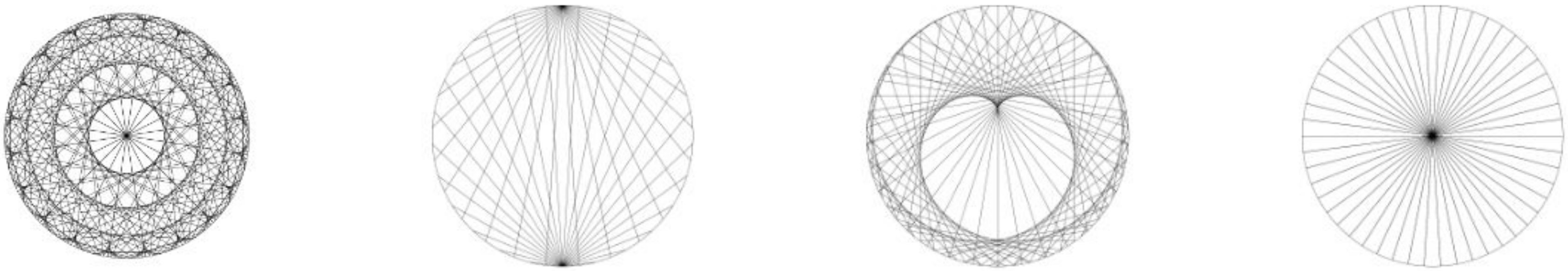
$$x(t) = \alpha \cos t + \beta \cos\left(\frac{\alpha}{\beta} t\right)$$
$$y(t) = \alpha \sin t + \beta \sin\left(\frac{\alpha}{\beta} t\right)$$



To get the curve with a-1 petals, set α = a and β = 1

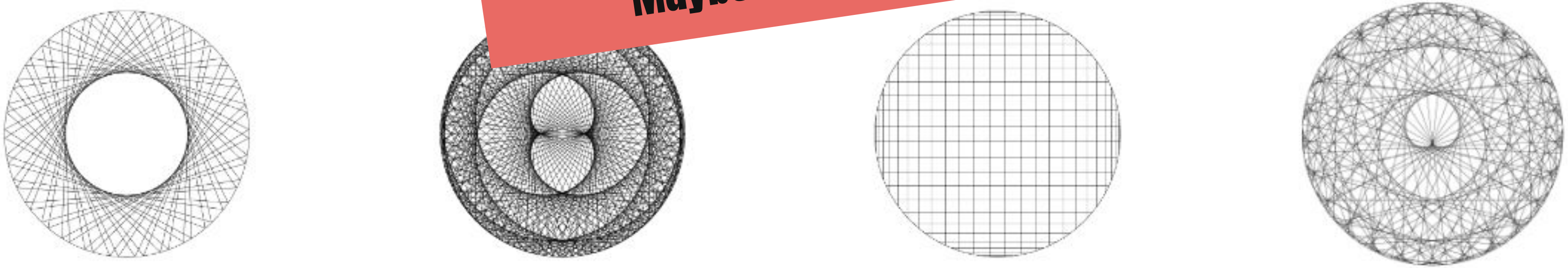


Guess: For large enough *a*, MMT(*m*, *a*) looks like the epicycloid with α = a and β = 1.



(a) MMT(200, 21) (b) MMT(50, 25) (100, 34) (d) MMT(100, 51)

Maybe not....



(e) MMT(90, 31) (f) MMT(400, 115) (g) MMT(100, 49) (h) MMT(206, 21)

Families of Tables

m = 2a

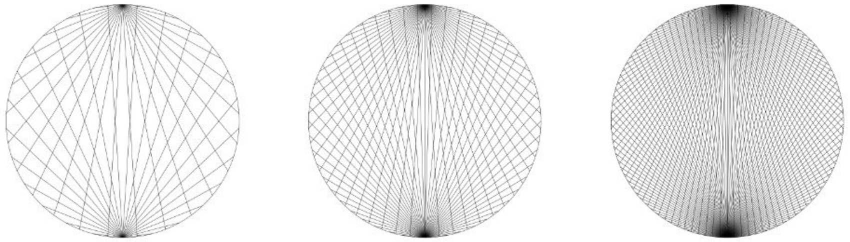


Figure 5: Tables (50, 25), (100, 50), (200, 100)

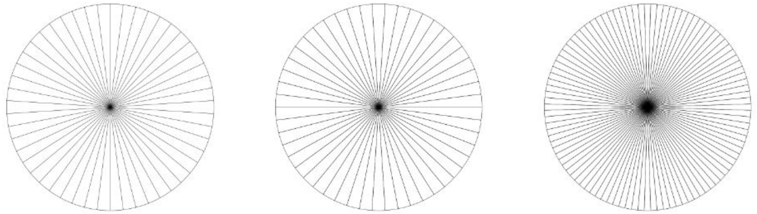


Figure 6: Tables (50, 26), (100, 51), (200, 101)

m = 2a - 2

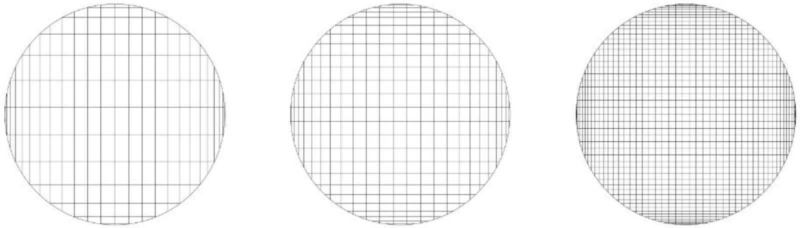


Figure 7: Tables (50, 24), (100, 49), (200, 99)

m = 2a + 2

meta

Families of Tables

m = 2a

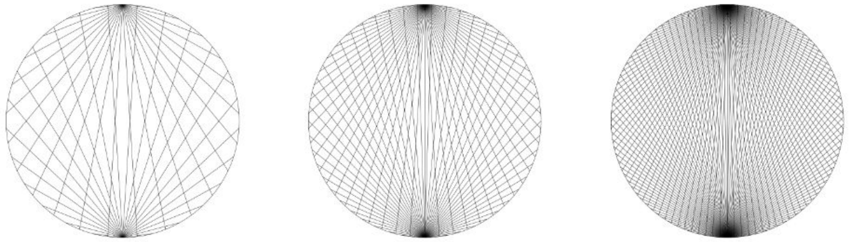


Figure 5: Tables (50, 25), (100, 50), (200, 100)

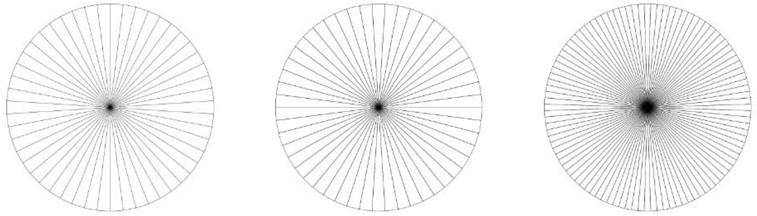


Figure 6: Tables (50, 26), (100, 51), (200, 101)

m = 2a - 2b

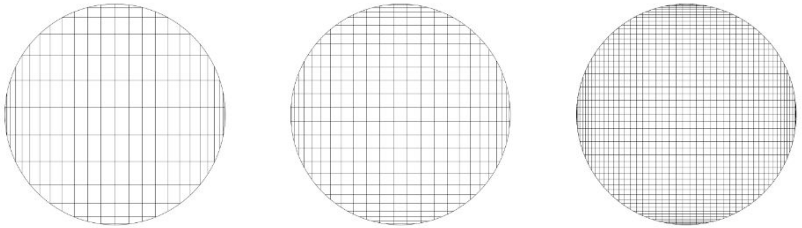
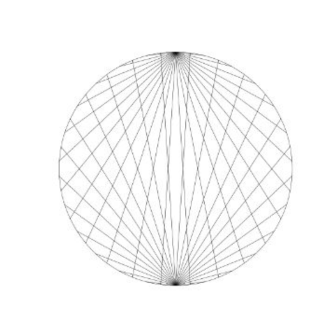


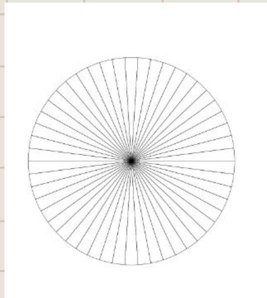
Figure 7: Tables (50, 24), (100, 49), (200, 99)

m = 2a + 2b

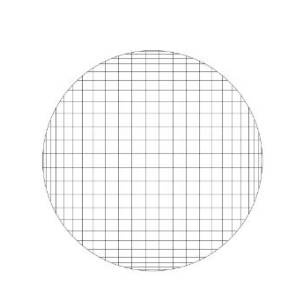
m = b*a

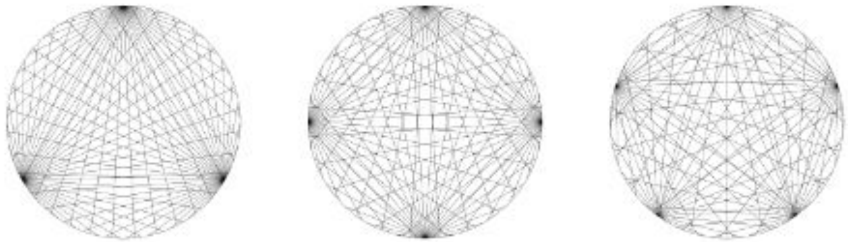


m = b*a - b

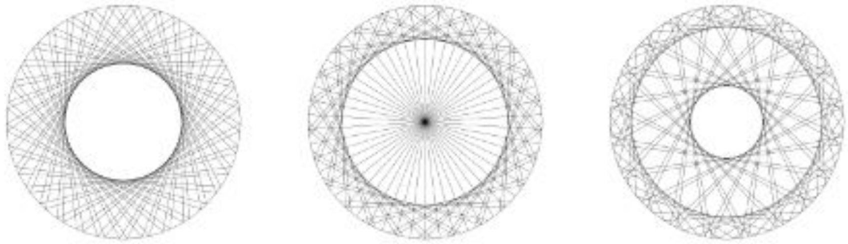


m = b*a + b

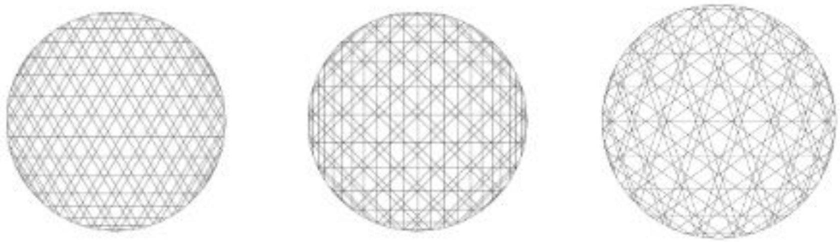




(a) MMT(99, 33) (b) MMT(100, 25) (c) MMT(100, 20)

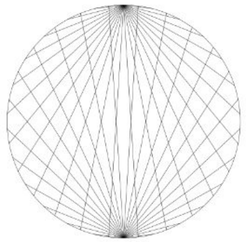


(d) MMT(99, 34) (e) MMT(100, 26) (f) MMT(100, 21)

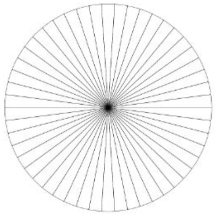


(g) MMT(99, 32) (h) MMT(100, 24) (i) MMT(100, 19)

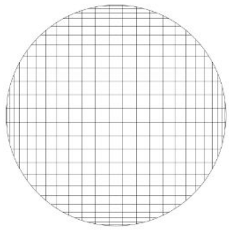
$$\left(m, \frac{m}{b}\right)$$

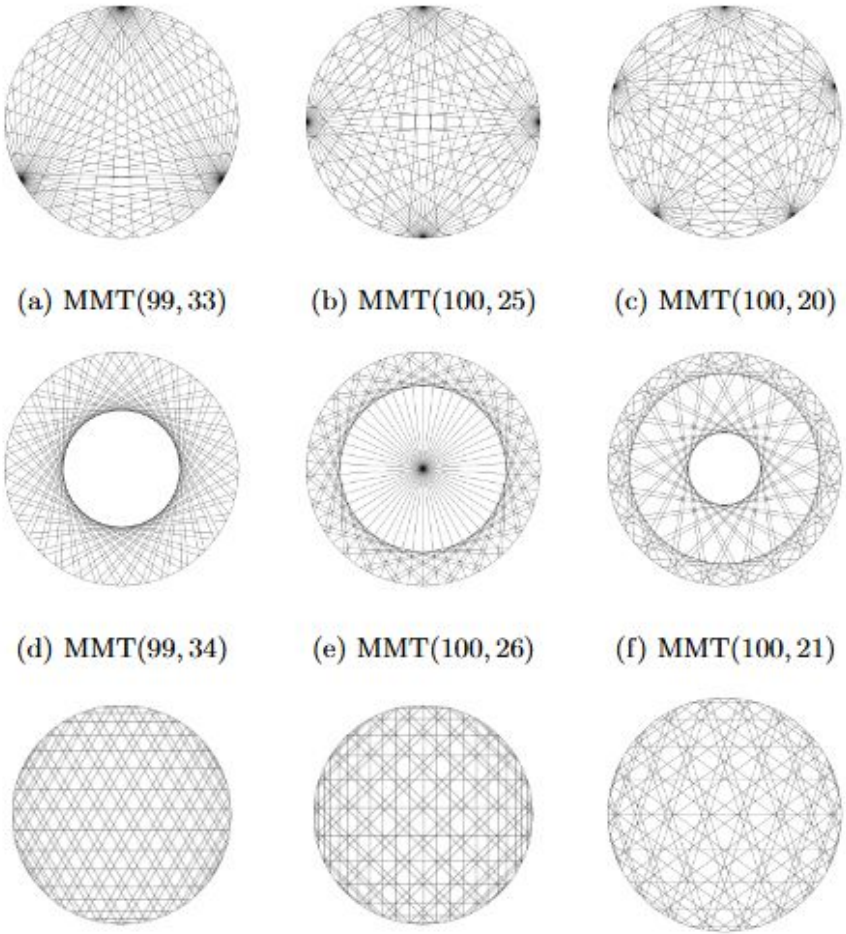


$$\left(m, \frac{m}{b} + 1\right)$$



$$\left(m, \frac{m}{b} - 1\right)$$





(a) MMT(99, 33) (b) MMT(100, 25) (c) MMT(100, 20)

(d) MMT(99, 34) (e) MMT(100, 26) (f) MMT(100, 21)

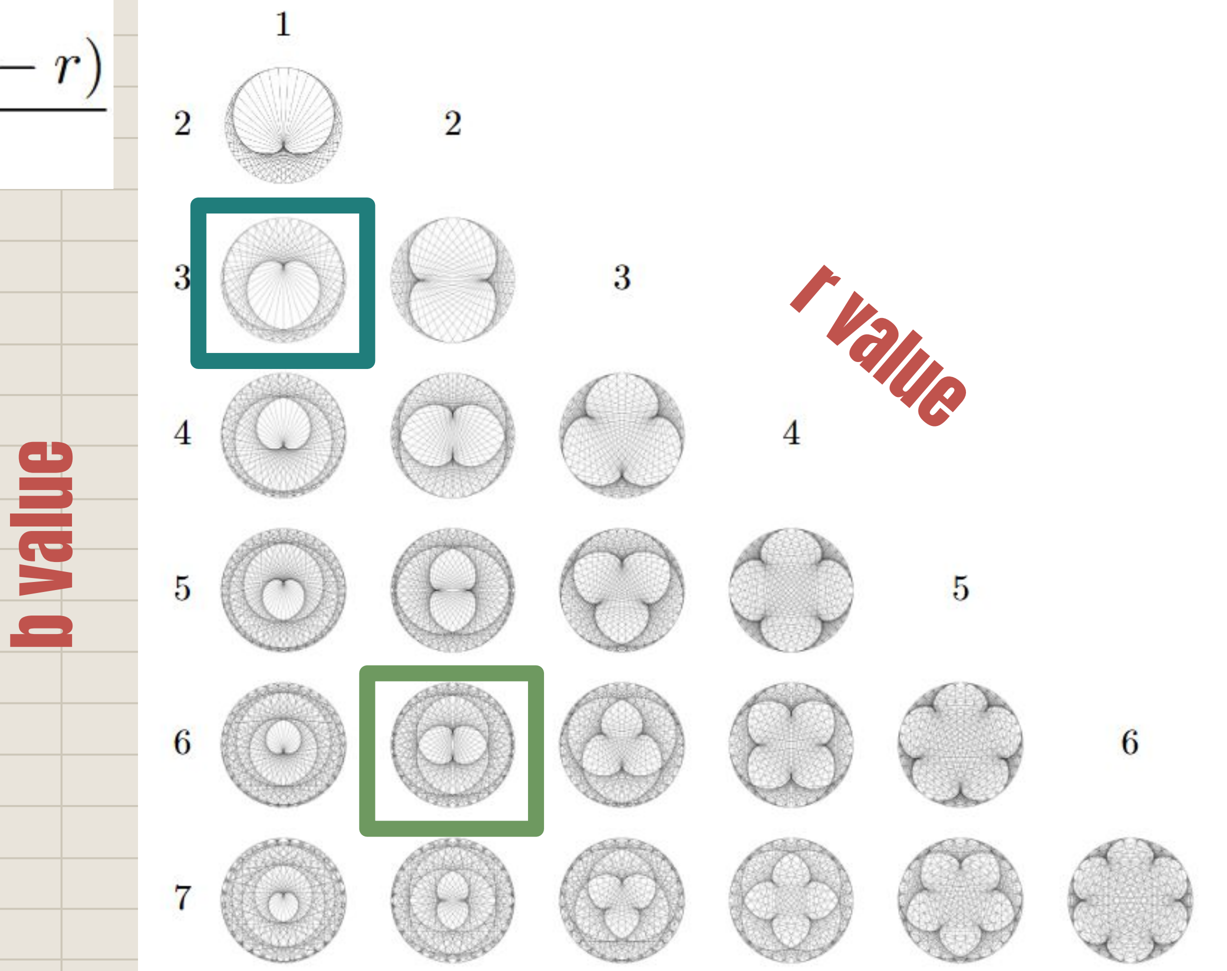
(g) MMT(99, 32) (h) MMT(100, 24) (i) MMT(100, 19)

Question: What if *m* is not divisible by *b*? But we want to keep the multiplier an integer.

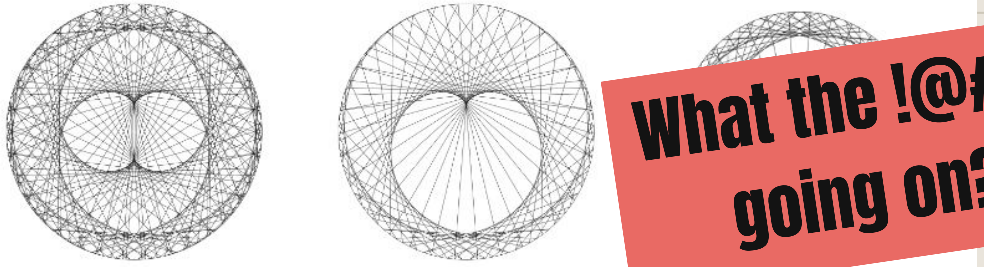
$$a = \left\lceil \frac{m}{b} \right\rceil \text{ or } a = \left\lfloor \frac{m}{b} \right\rfloor$$

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

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



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

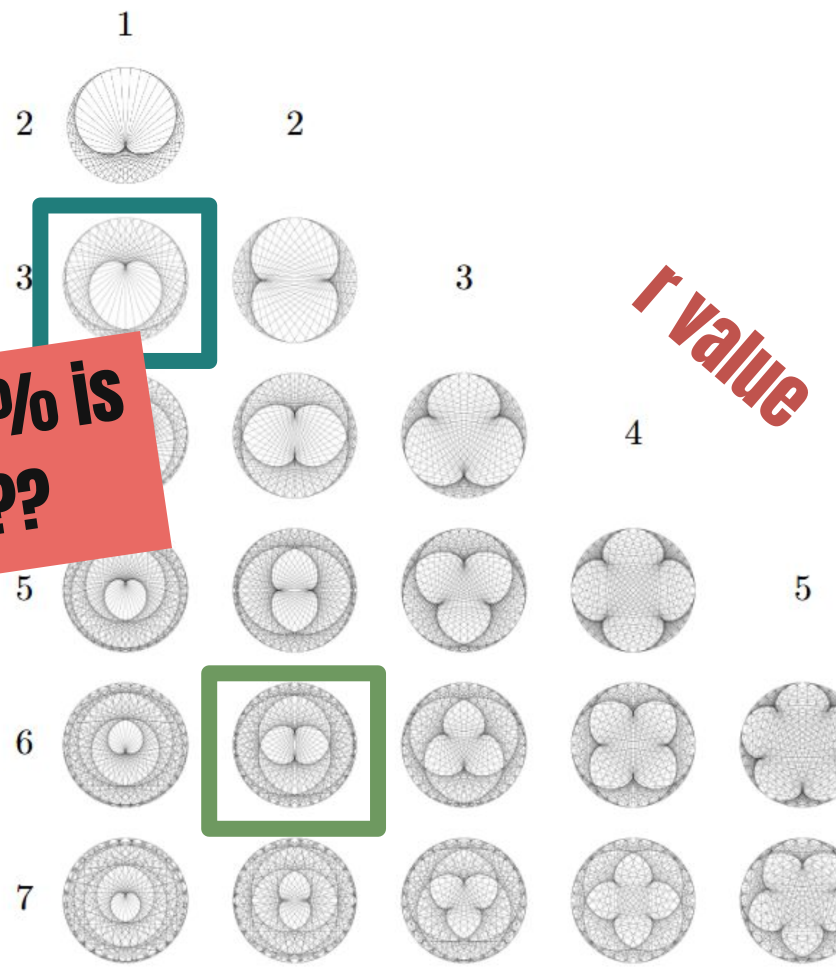


(a) MMT(206, 35)

(b) All chords originating from even points. (i.e. p to $35p \mod 206$ where p is even.)

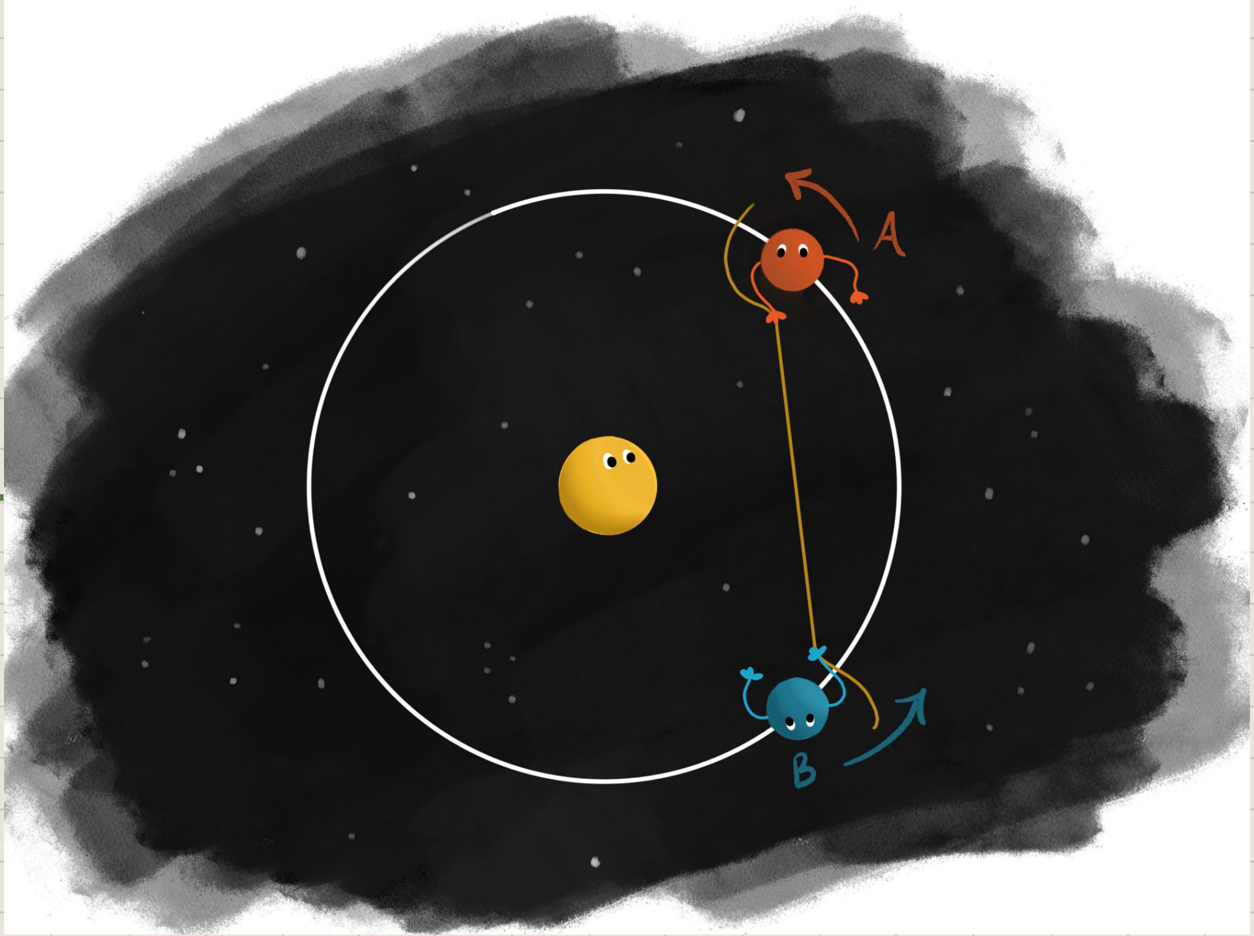
(c) All chords originating from odd points. (i.e. p to $35p \mod 206$ where p is odd.)

What the !@#% is going on???



Dancing Planets

https://x.com/matthen2/status/1437716084686299138



Planet Dances

Planet dance:

$$\mathcal{P}(\alpha,\beta) =: \left\{\text{chords on } S^1; \text{connecting } e^{2\pi i t\alpha} \text{ to } e^{2\pi i t\beta}\right\}$$

Planet Dances

Planet dance:

$$\mathcal{P}(\alpha, \beta) =: \left\{\text{chords on } S^1; \text{connecting } e^{2\pi i t\alpha} \text{ to } e^{2\pi i t\beta}\right\}$$

m-Sampling of a Planet Dance:

$$\mathcal{S}(\alpha, \beta, m) =: \left\{\text{chords in } \mathcal{P}(\alpha, \beta) \text{ for } t = 0, \tfrac{1}{m}, \tfrac{2}{m}, \ldots, \tfrac{m-1}{m}\right\}$$

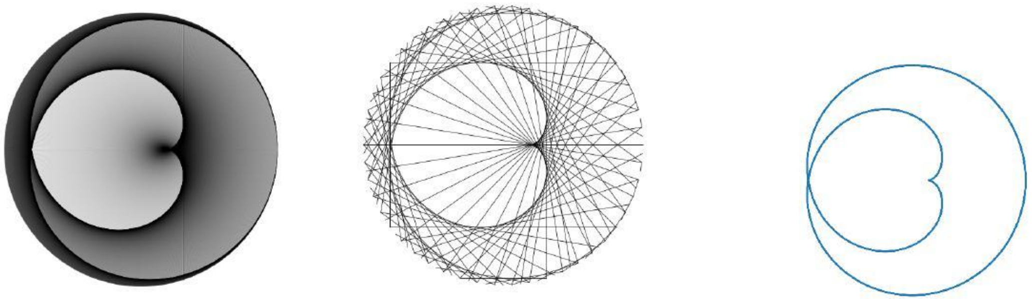
Planet Dances

Planet dance:

$$\mathcal{P}(\alpha,\beta) =: \left\{\text{chords on } S^1 ; \text{connecting } e^{2\pi i t\alpha} \text{ to } e^{2\pi i t\beta}\right\}$$

m-Sampling of a Planet Dance:

$$\mathcal{S}(\alpha,\beta,m) =: \left\{\text{chords in } \mathcal{P}(\alpha,\beta) \text{ for } t = 0, \tfrac{1}{m}, \tfrac{2}{m}, \ldots, \tfrac{m-1}{m}\right\}$$



(a) $\mathcal{P}(3,2)$

(b) 100-sample of $\mathcal{P}(3,2)$

(c) Epicycloid formed by radius 2 circle rolling around radius 1 circle.

Figure 1: A planet dance and its 100-sample

A correspondence?

Question

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

A correspondence?

Question

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

Lemma (Fundamental Correspondence)

The modular multiplication table $\mathrm{MMT}(m, a)$ *is an m-sampling of the integral planet dance* $\mathcal{P}(1, a)$.

$$\mathrm{MMT}(m, a) \quad \Rightarrow \quad \mathcal{S}(1, a, m)$$

$\longleftarrow$?

Hope for the other direction

MMT$(100, 34)$ "should" look like $\mathcal{S}(1, 34, 100)$, but instead, it looks like $\mathcal{P}(3, 2)$.

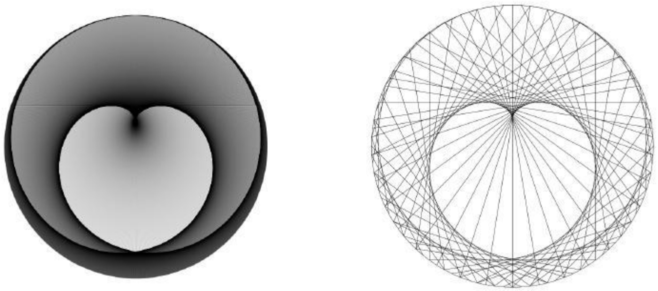
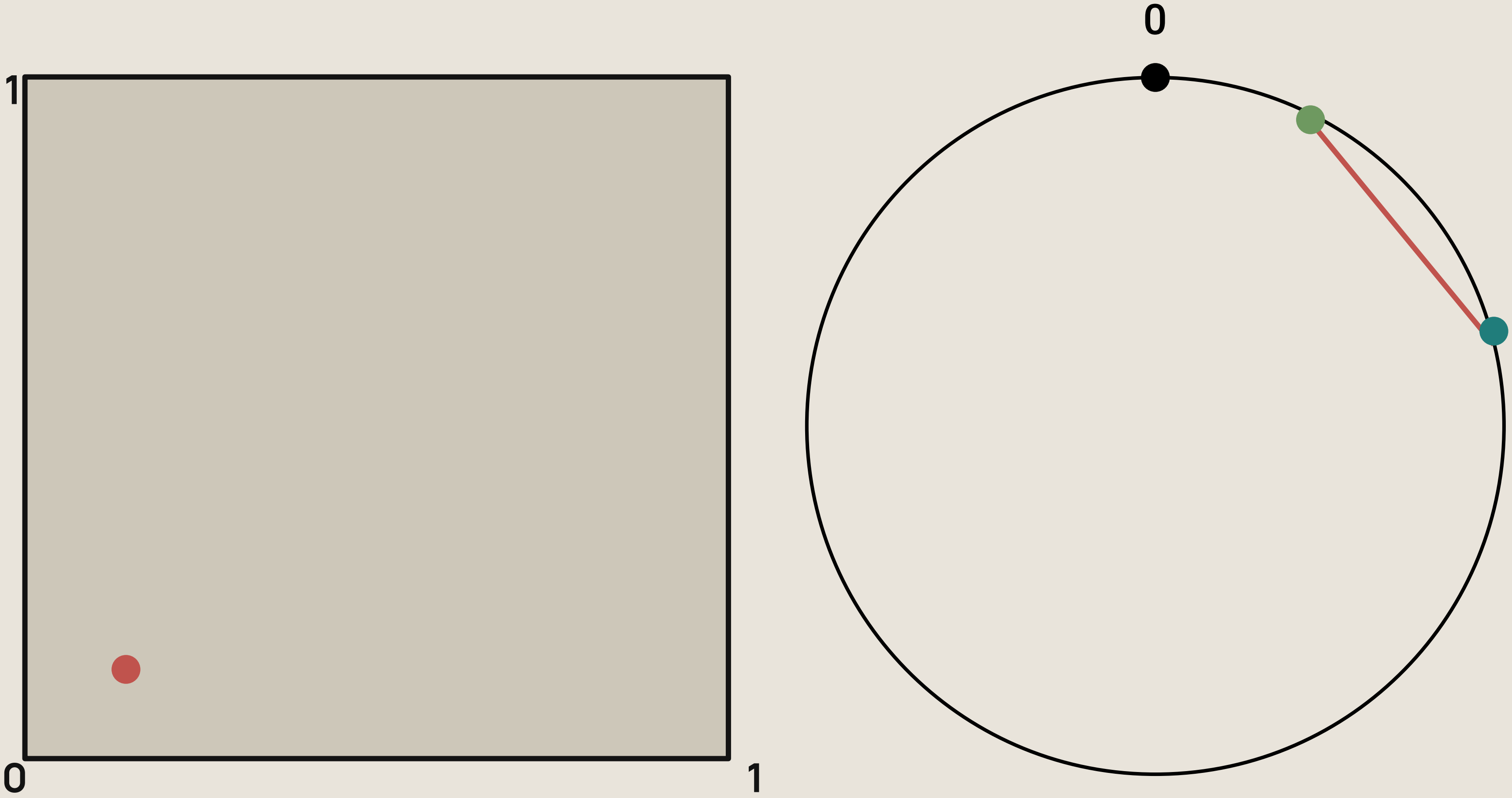
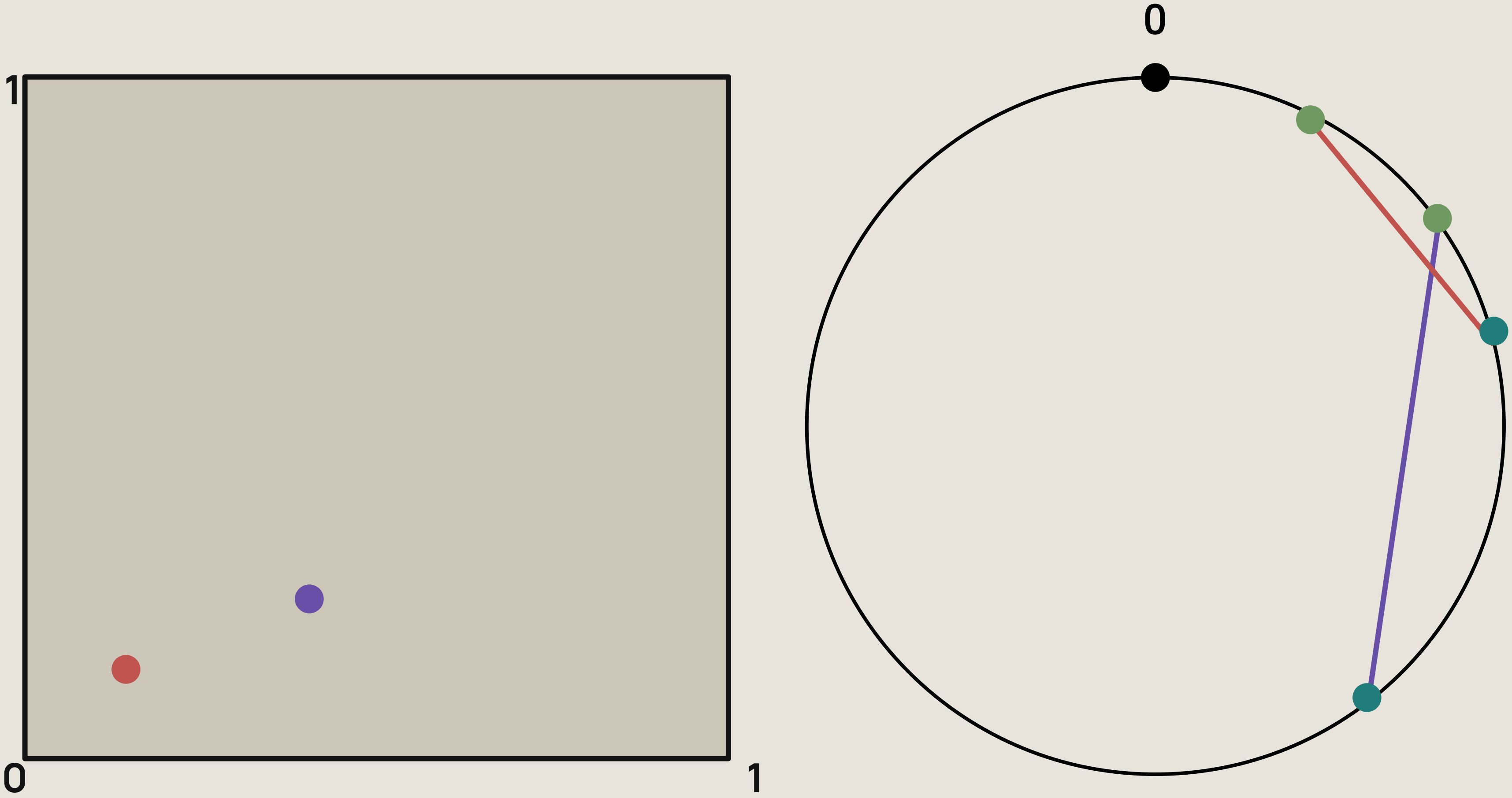
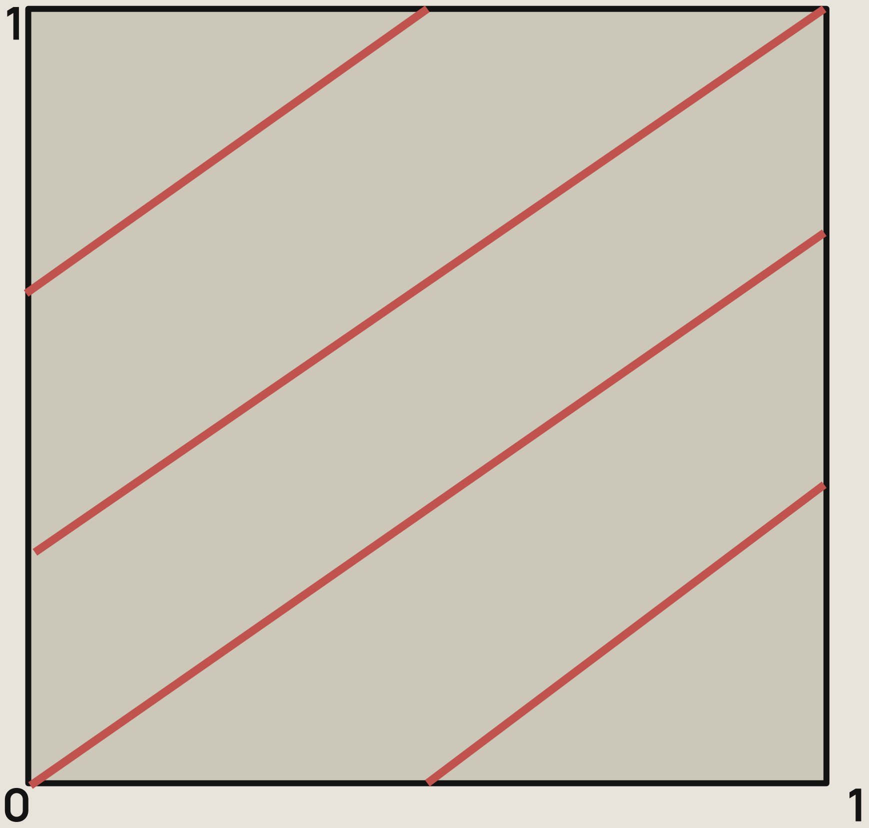


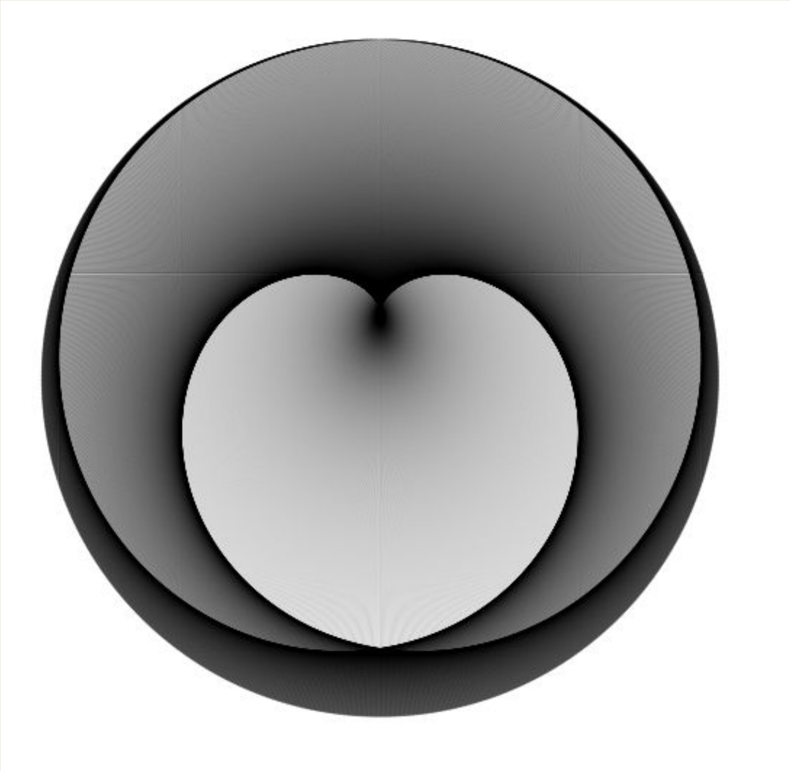
Figure 2: $\mathcal{P}(3, 2)$ (left) and MMT$(100, 34)$ (right)

A Topological Perspective

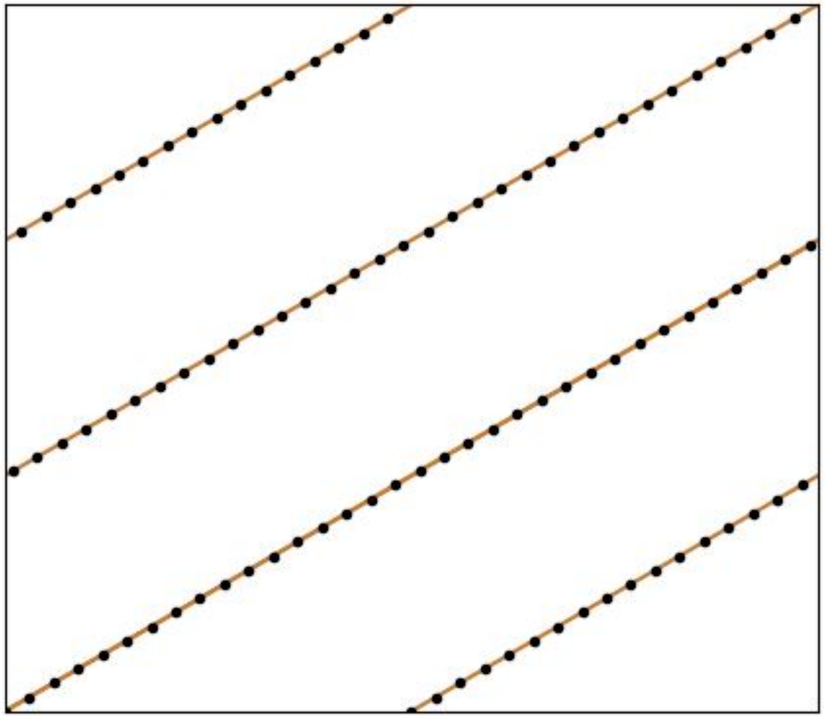

1
0
1
0

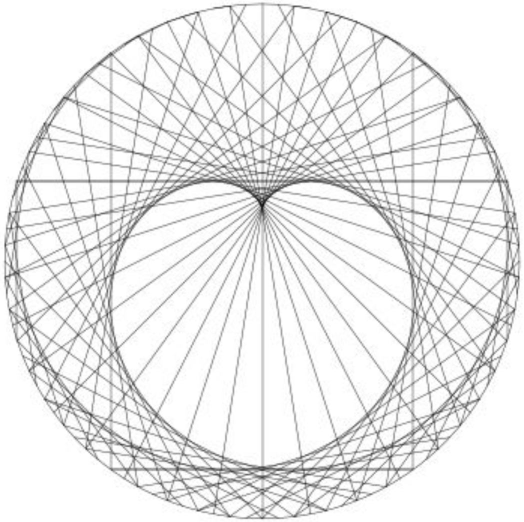

1
0
1
0





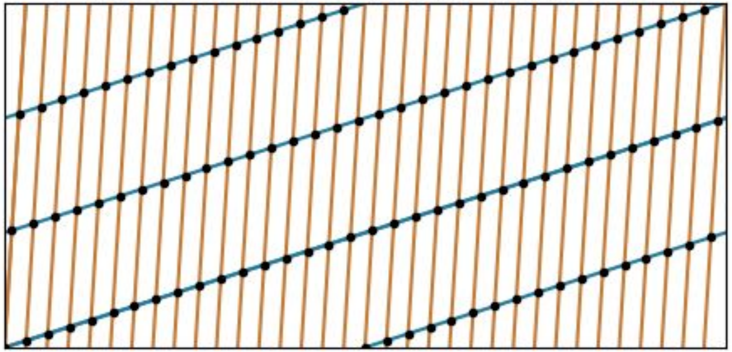
P(3,2)



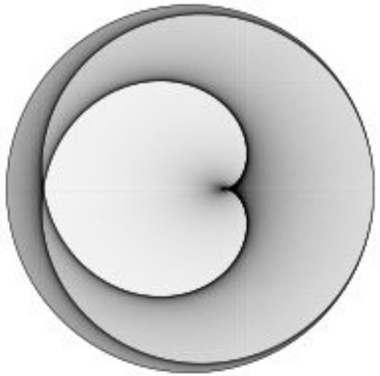


S(3,2,100)

Linear Loops on Torus (3, 2) and (1, 34)

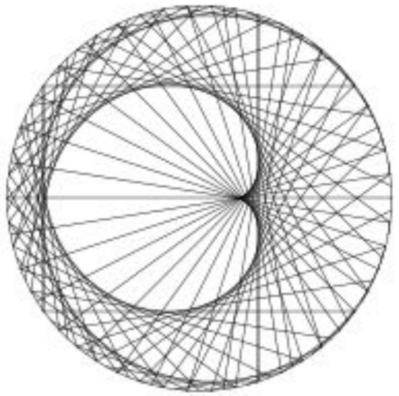


Planet Dance α = 3 β = 2



Epicycloid

MMT(100, 34)



Intersection

$\mathcal{P}(\alpha, \beta) \quad \leftrightarrow$ a line in $\mathbb{R}^2/\mathbb{Z}^2$ given by

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

Intersection

$\mathcal{P}(\alpha, \beta) \quad \leftrightarrow$ a line in $\mathbb{R}^2/\mathbb{Z}^2$ given by

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

Lemma (Planet dance intersection)

Let lines ℓ_1 and ℓ_2 in $\mathbb{R}^2/\mathbb{Z}^2$ be given by

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

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.*

Intersection

Lemma (Planet dance intersection)

Let lines ℓ_1 and ℓ_2 in $\mathbb{R}^2/\mathbb{Z}^2$ be given by

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

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.*

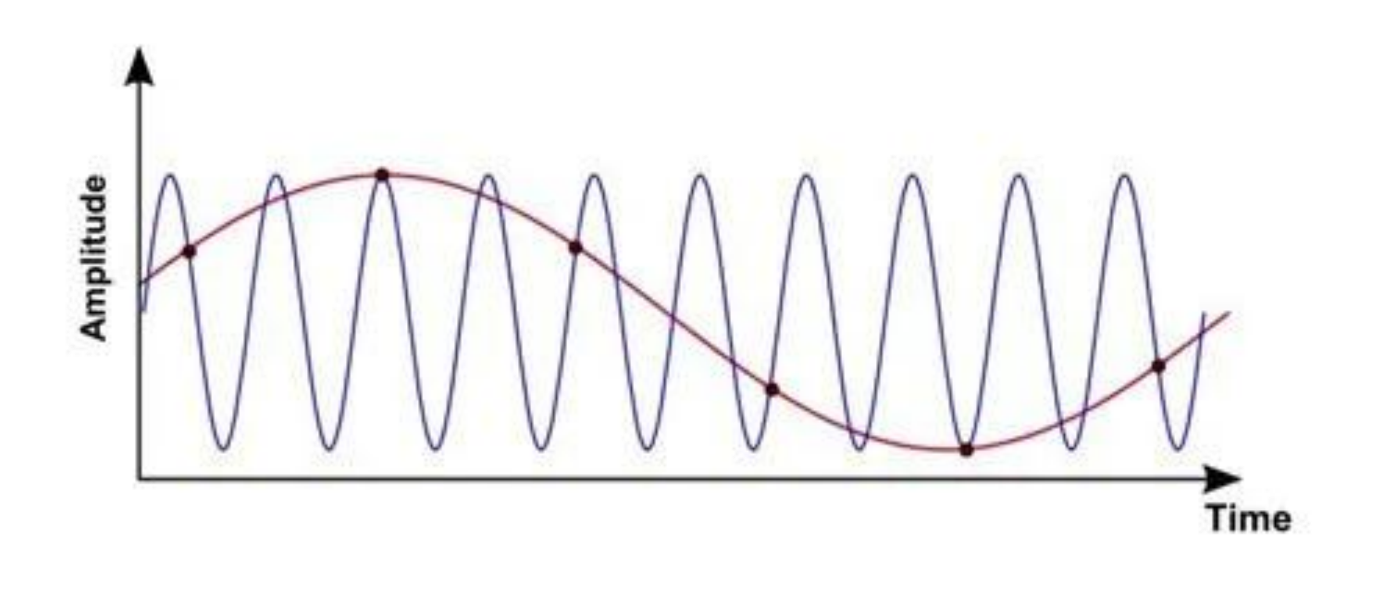
Example:

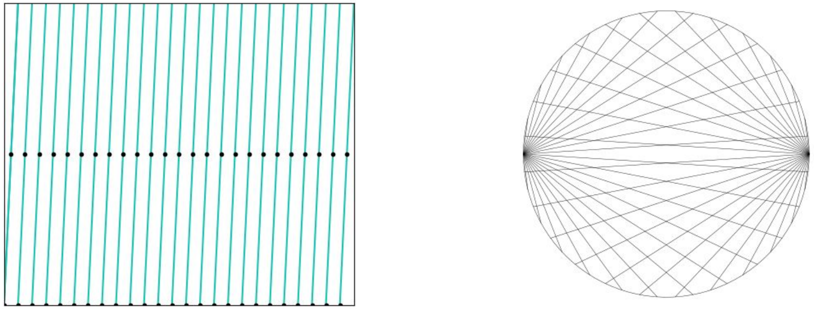
$$\mathcal{P}(3, 2) \quad \text{and} \quad \mathcal{P}(1, 34)$$

$$3 \cdot 34 - 2 \cdot 1 = 100$$

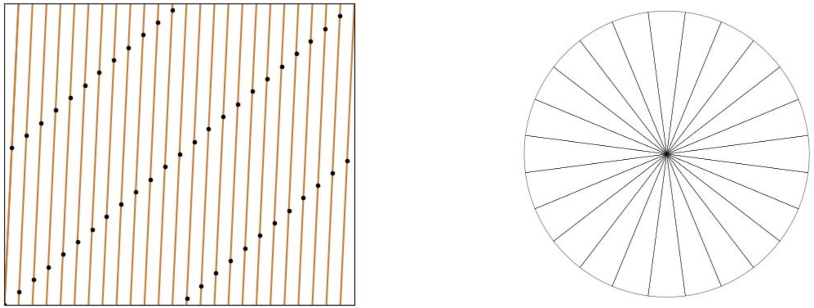
$\Rightarrow$ So $\mathcal{P}(3, 2)$ and $\mathcal{P}(1, 34)$ intersect 100 times!

Aliasing

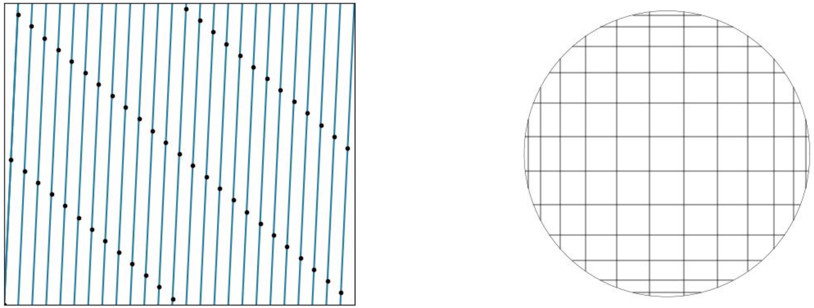




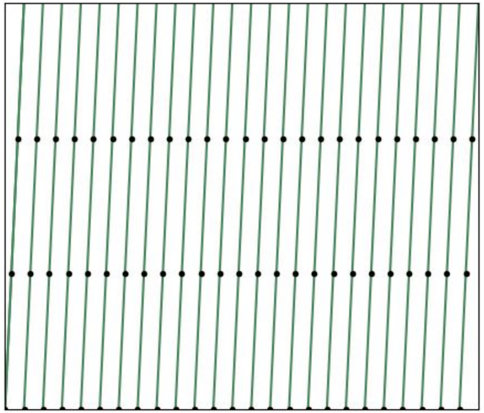
$m = 2a$

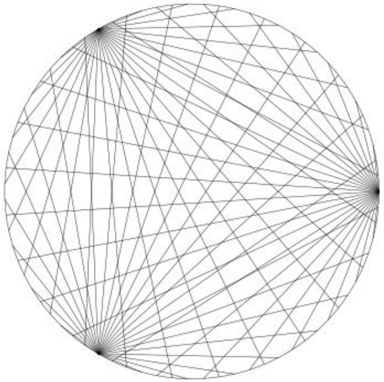


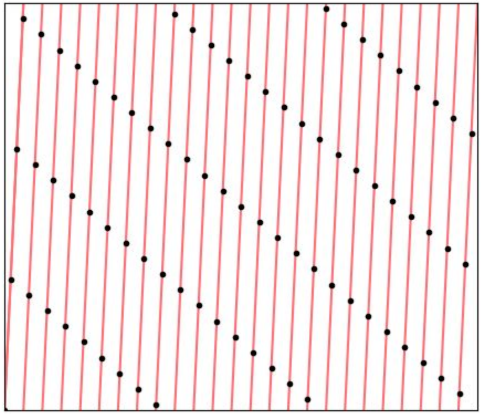
$m = 2a - 2$

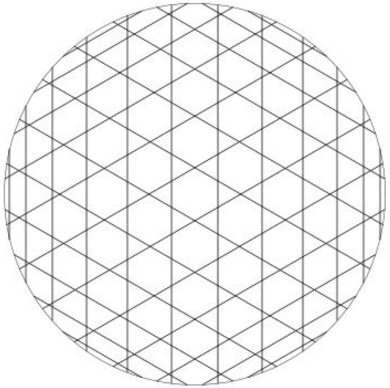


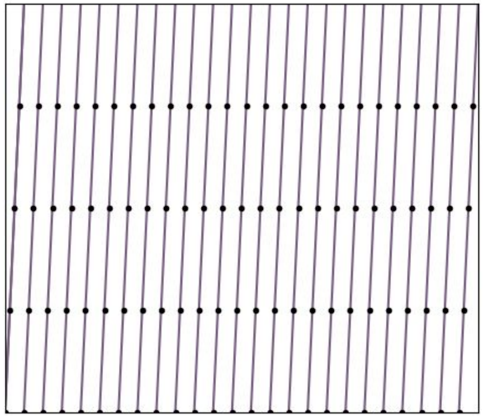
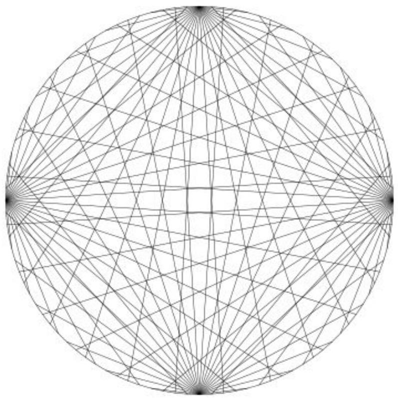
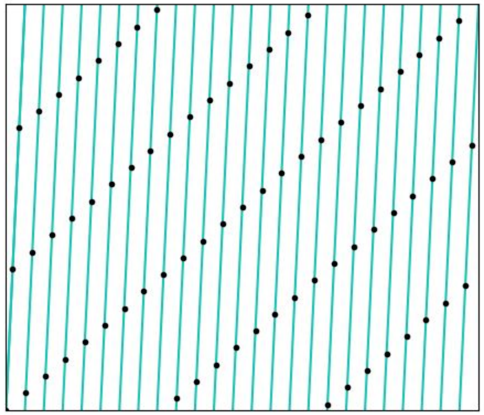
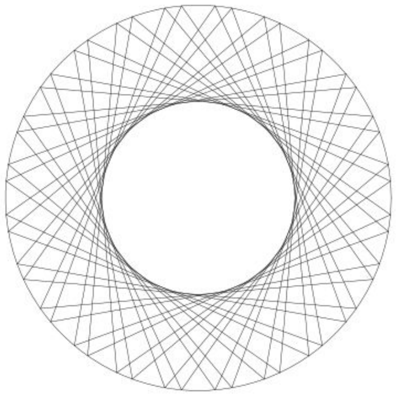
$m = 2a + 2$

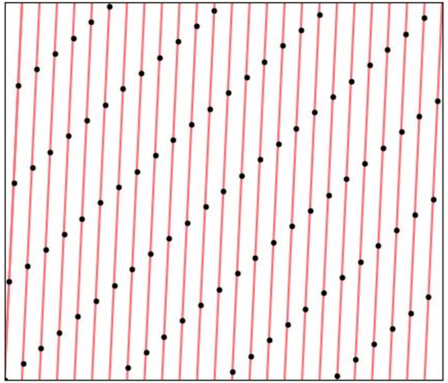
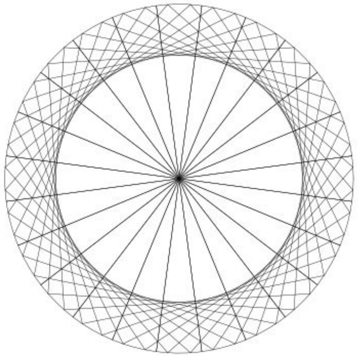
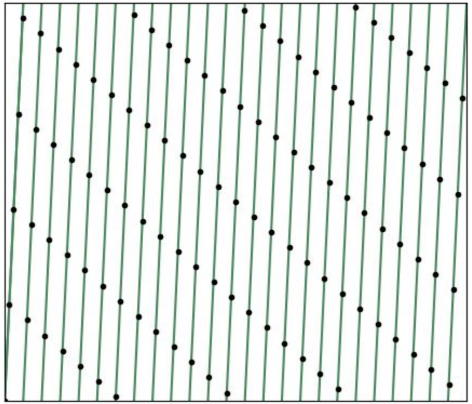
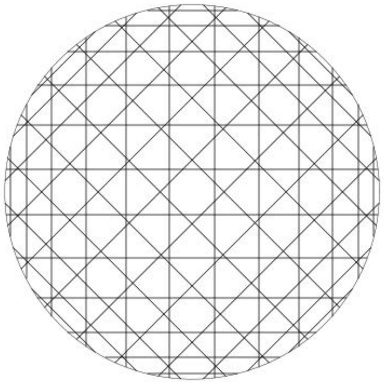








Thanks for coming!

more details

craft instructions