Projet Math-info

Tables de multiplications modulaires

Duc Nguyen DUONG & Louis GAVALDA

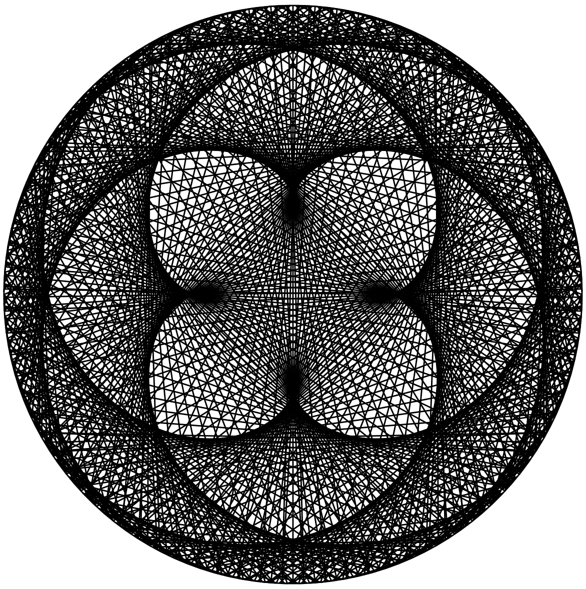
Introduction

Notre sujet

Une **bizarrerie mathématique** : « La face cachée des tables de multiplication » sur YouTube.

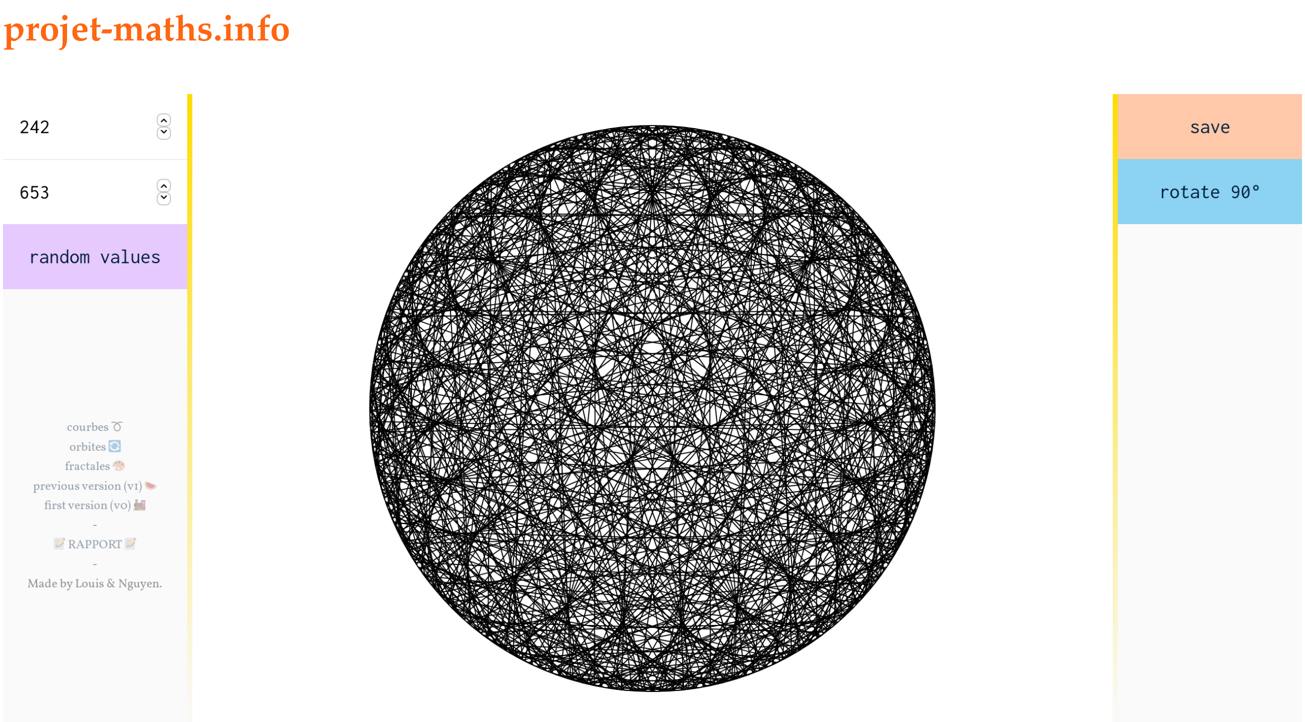
- Procédé de construction permettant de *dessiner* une table de multiplication.
- Apparition de formes géométriques très étonnantes : mais pourquoi ?

Notre sujet



Représentation graphique de la table de 166 modulo 656.

Le site internet



Caractéristiques algébriques

Procédé de construction

- partir du n-ème point du cadran ;
- calculer $k = n \times m$;
- relier d'un segment les points n et $\bar{k}$, où $\bar{k}$ est la classe d'équivalence de k dans $\mathbb{Z}/M\mathbb{Z}$;
- recommencer pour chaque autre point.

La cardioïde

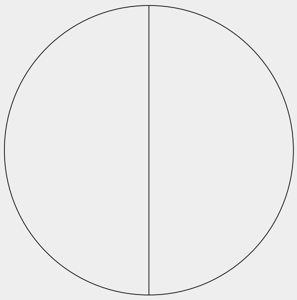


Table de 2 *modulo* 2.

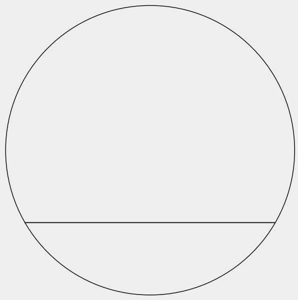


Table de 2 *modulo* 3.

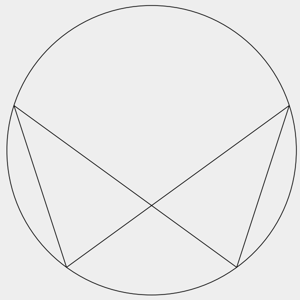


Table de 2 *modulo* 5.

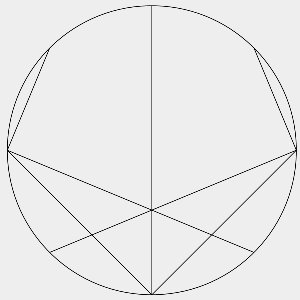


Table de 2 *modulo* 8.

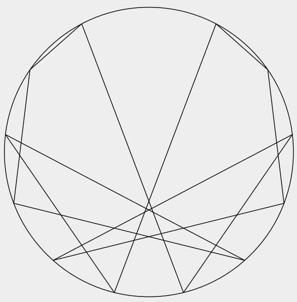


Table de 2 *modulo* 13.

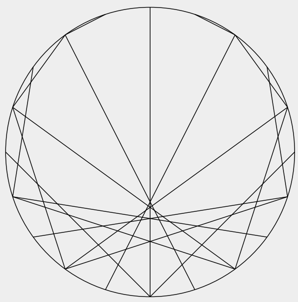


Table de 2 *modulo* 20.

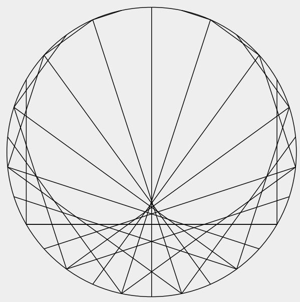


Table de 2 *modulo* 30.

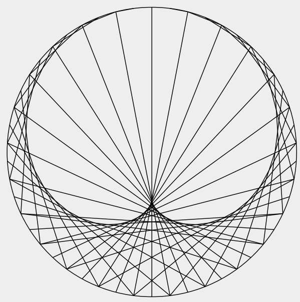


Table de 2 *modulo* 50.

Épicycloïdes

On finit même par s'apercevoir que le procédé de construction fait systématiquement apparaître une courbe à $m-1$ pétales.

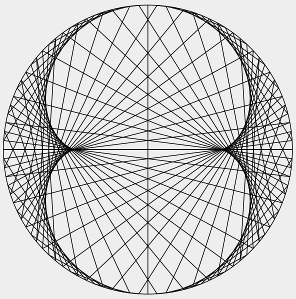


Table de 3 modulo 100.

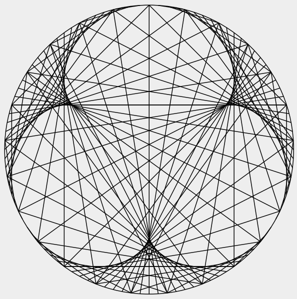


Table de 4 modulo 100.

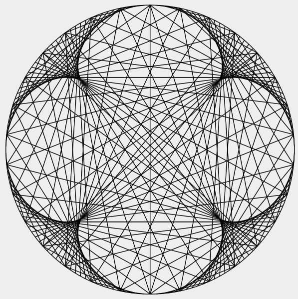


Table de 5 modulo 150.

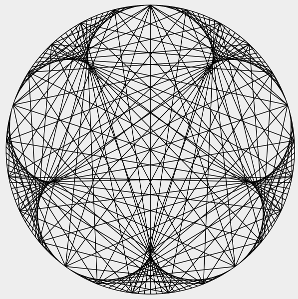


Table de 6 modulo 150.

Pour le plaisir des yeux

Pour certaines valeurs, les figures obtenues sont particulièrement remarquables :

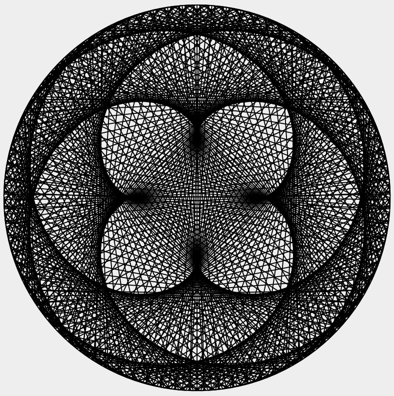


Table de 166 modulo 656.

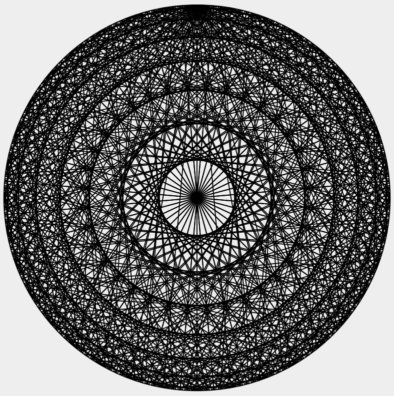


Table de 757 modulo 576.

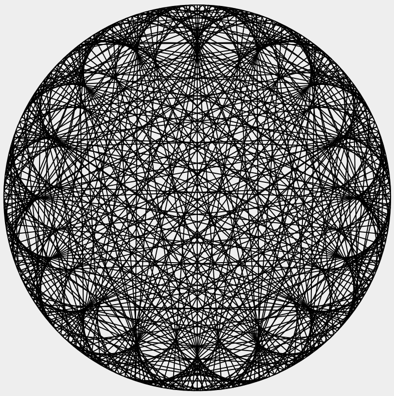


Table de 230 modulo 442.

Pour le plaisir des yeux

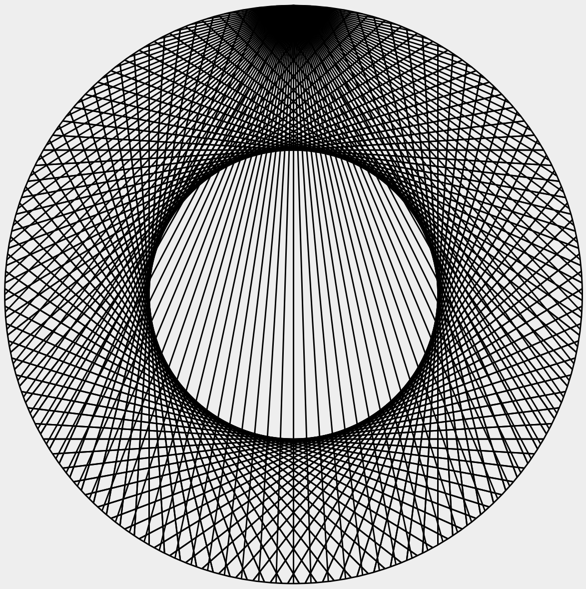


Table de 521 modulo 312.

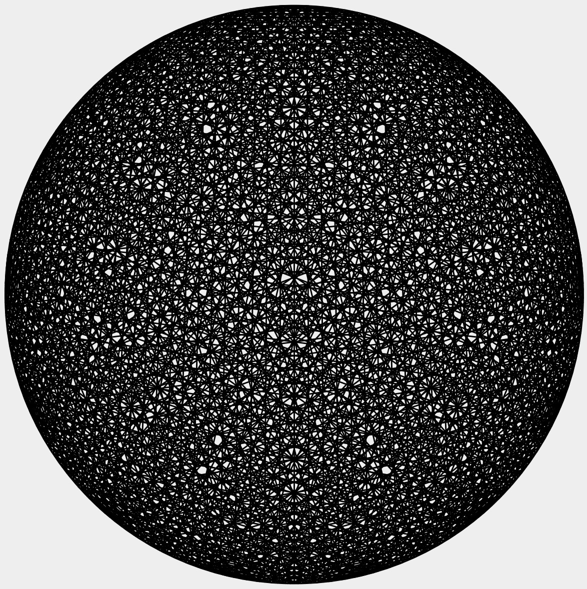


Table de 726 modulo 848.

Pour le plaisir des yeux

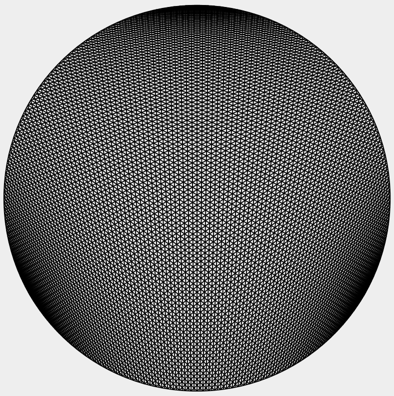


Table de 410 modulo 412.

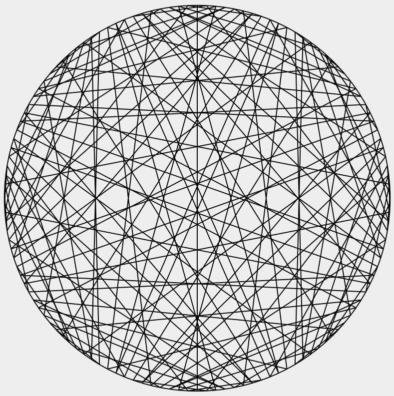


Table de 37 modulo 130.

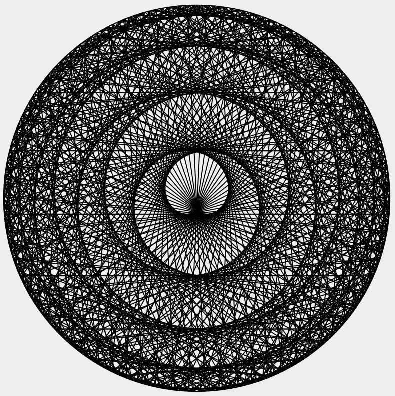


Table de 189 modulo 627.

Résultats obtenus sur les cycles

On s'intéresse à la **table de n modulo m** :

- Si n et m sont premiers entre eux, il y a exactement $\frac{\varphi(n)}{ord_{n'}(\bar{m})}$ orbites de taille $ord_{n'}(\bar{m})$.
- Si n est premier, il y a exctement $\frac{n-1}{ord_{n'}(\bar{m})}$ orbites de taille $ord_{n'}(\bar{m})$.

Origine des formes géométriques

Apparition des courbes

Le procédé de construction **ne peut pas** dessiner les courbes : il ne fait que relier des points.

A-t-on affaire à de la magie ?

Apparition des courbes

Non, c'est une **illusion d'optique** !

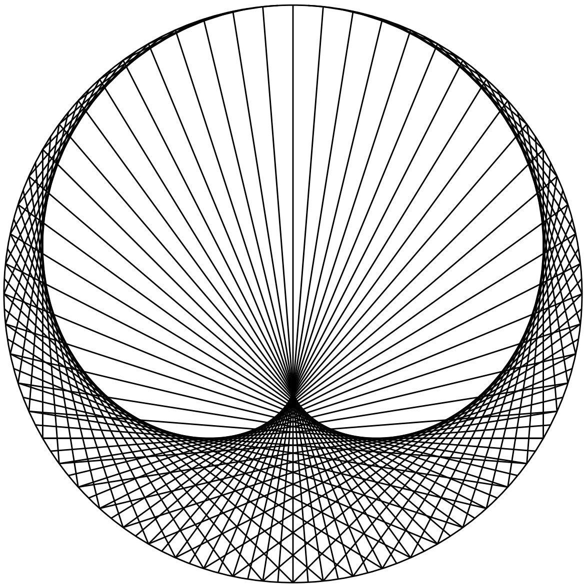


Table de 2 modulo 120 : la cardioïde.

Courbes bien connues

Exemple de ***caustique*** *: l'enveloppe des rayons lumineux subissant une réflexion ou un réfraction sur une surface.*

Une piste ?

De là **notre intuition** : la courbe apparaît lorsqu'elle est *enveloppée* d'un nombre suffisamment important de **tangentes**.

Problème posé

Soit $(O, \vec{i}, \vec{j})$.

Soit $I \subseteq \mathbb{R}$. Pour tout $t \in I$, on se donne :

- un point A(t) du plan ;
- un vecteur $u(t) \in \mathbb{R}^2$.

On note Δ_t la droite passant par $A(t)$ et de vecteur directeur $u(t)$.

Problème posé

On cherche une courbe $\mathcal{C}$ telle que :

- $\forall t \in I, \Delta_t$ est une tangente à $\mathcal{C}$;
- $\forall u \in \mathcal{C}$, u a une tangente appartenant à $\{\Delta_t \mid t \in I\}$.

Résultats

Nous démontrons qu'il est possible de construire une telle courbe $\mathcal{C}$ de représentation paramétrique $f : I \longrightarrow \mathbb{R}^2,\ t \longmapsto \begin{pmatrix} x(t) \\ y(t) \end{pmatrix}$ de classe C^1.

Résultats

Le procédé de construction *dessine* alors bien la courbe.

Lorsque le nombre de points sur le cercle est suffisamment grand, les lignes *tendent* vers les tangentes à la courbe : la figure apparaît.

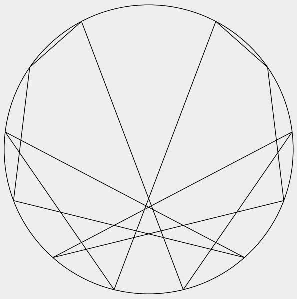


Table de 2 modulo 13.

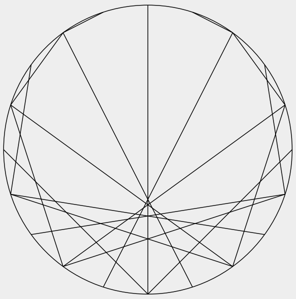


Table de 2 modulo 20.

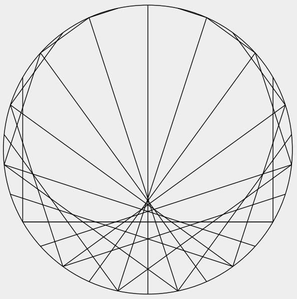


Table de 2 modulo 30.

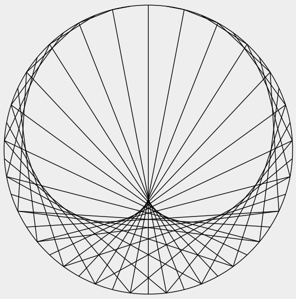


Table de 2 modulo 50.

Fractales et ensembles de Mandelbrot

Définition

L'**ensemble de Mandelbrot généralisé** est une fractale définie comme l'ensemble des points c du plan complexe pour lesquels la suite de nombres complexes définie par récurrence par (avec $d \in \mathbb{N}$) :

$$\begin{cases} z_0 = 0 \\ z_{n+1} = z_n^d + c \end{cases}$$

est **bornée**.

Algorithme(s) de construction

Définition de la fractale utilisée pour l'algorithme : Soit $C(c_x, c_y)$ un point donné du plan muni d'un repère $(O, \vec{i}, \vec{j})$. Pour tout entier naturel n, on construit, à partir des coordonnées de ce point C, une suite de point $M_n(x_n, y_n)$ défini par les relations de récurrence suivantes :

$$\begin{cases} x_0 = y_0 = 0 \\ z_0 = x_0 + iy_0 \\ z_{n+1} = z_n^d + (c_x + ic_y) \\ x_{n+1} = Re(z_{n+1}) \\ y_{n+1} = Im(z_{n+1}) \end{cases}$$

Algorithme(s) de construction

L'ensemble de **Mandelbrot** d'ordre 2:

$$\begin{cases} x_0 = y_0 = 0 \\ x_{n+1} = x_n^2 - y_n^2 + c_x \\ y_{n+1} = 2x_n y_n + c_y \end{cases}$$

Algorithme(s) de construction

Exemples :

- soit $C(1,1)$, alors la suite des points (M_n) construite à partir de ce point C est $M_0(0,0)$, $M_1(1,1)$, $M_2(1,3)$, $M_3(-7,7)$, $M_4(1,-97)$, $M_5(-9047,-193)$.
- soit $C(0.1,0.2)$, alors la suite des points (M_n) construite à partir de ce point C est $M_0(0,0)$, $M_1(0.1,0.2)$, $M_2(0.07,0.24)$, $M_3(0.0473,0.234)$, $M_4(0.0477,0.222)$, $M_5(0.0529,0.221)$.

Algorithme(s) de construction

Deux situations peuvent se présenter :

- soit la distance OM_n augmente infiniment,
- soit la distance OM_n est **bornée**.

Algorithme(s) de construction

La règle de prise de décision :

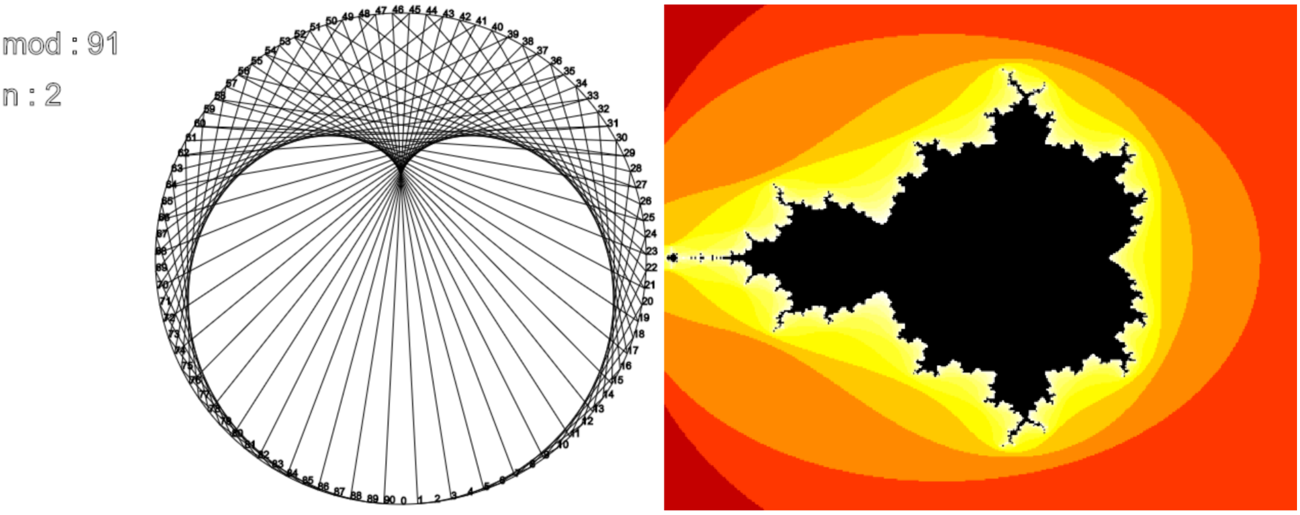
- soit le point M_n « s'éloigne » infiniment de l'origine, auquel cas le point C n'appartient pas à l'ensemble de Mandelbrot,
- soit le point M_n « reste » au voisinage de l'origine, c'est-à-dire dans un cercle de centre 2 et de rayon 2, auquel cas le point C appartient à l'ensemble de Mandelbrot.

Algorithme utilisé

```
Pour chaque pixel C de coordonnées (x,y):
|Tant que la distance OM_n < 2 et que n < I_max:
||Calculer les coordonnées de M_n
||Affecter à n la valeur n+1
|Fin Tant que
|Si n = I_max alors:
||Colorier le pixel en noir
|Fin Si
Fin Pour
```

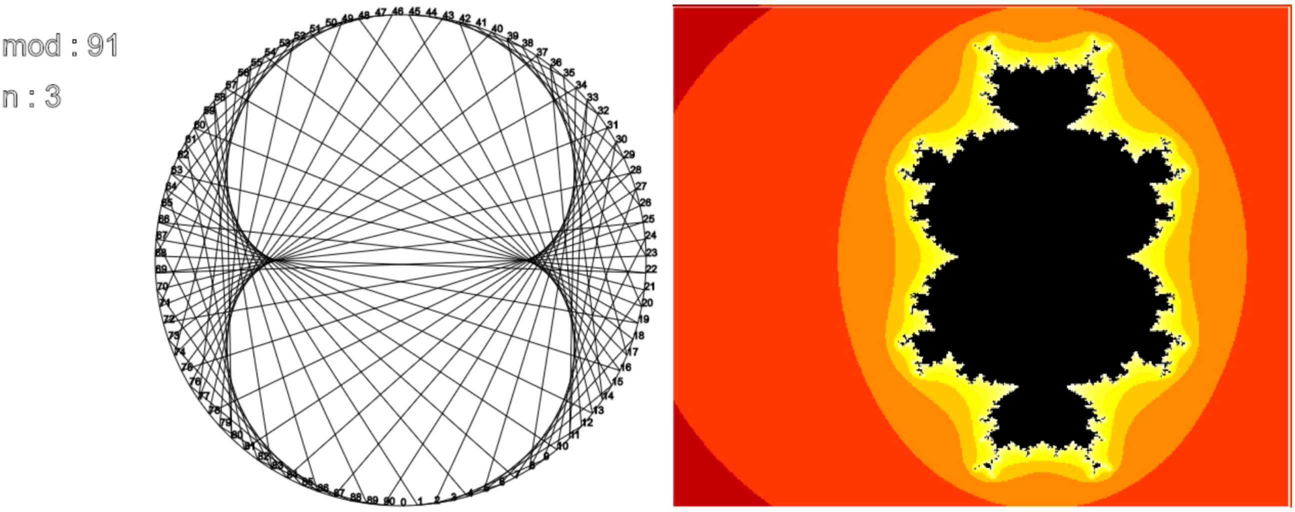
Similitudes avec les fractales

Comme un air de famille, non ?



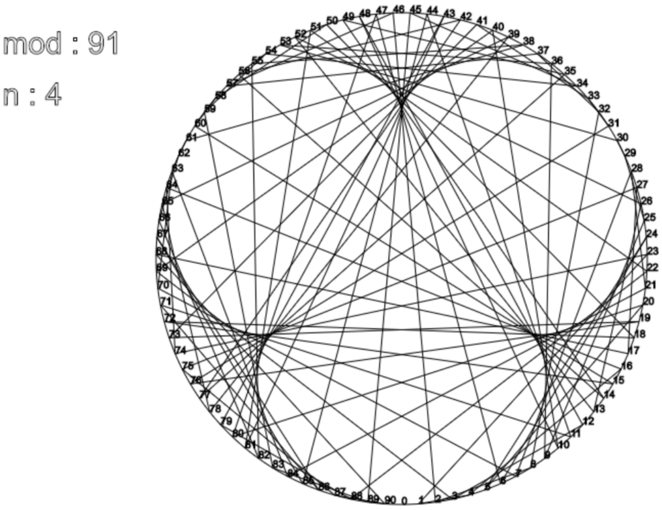
La table de 2 modulo 91, avec l'ensemble de Mandelbrot généralisé défini par $z_{n+1} = z_n^2 + c$.

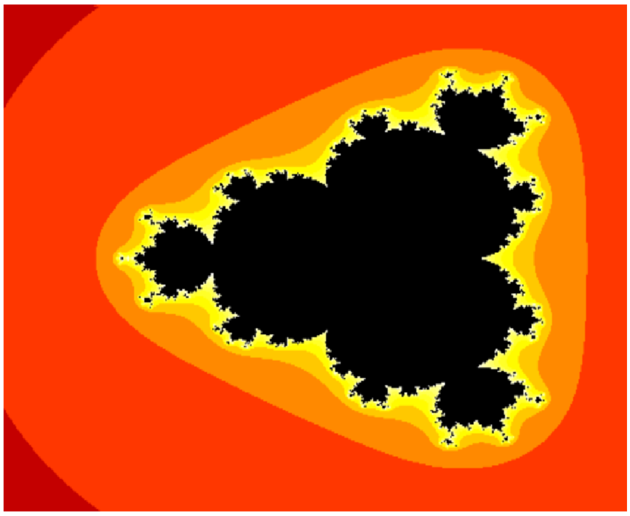
Similitudes avec les fractales



La table de 3 modulo 91, avec l'ensemble de Mandelbrot généralisé défini par $z_{n+1} = z_n^3 + c$.

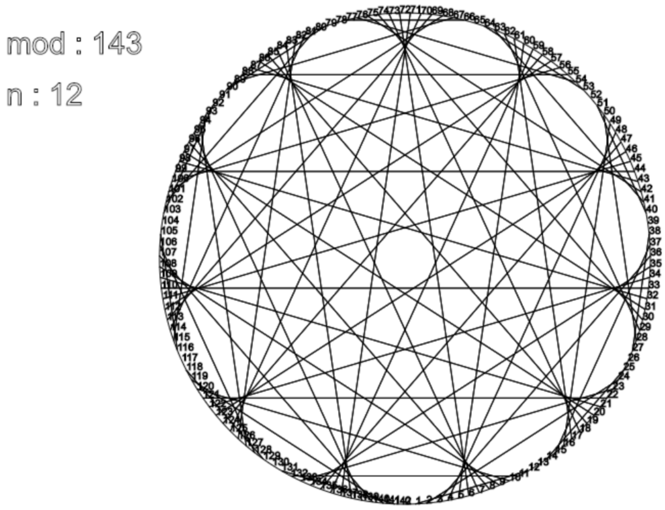
Similitudes avec les fractales

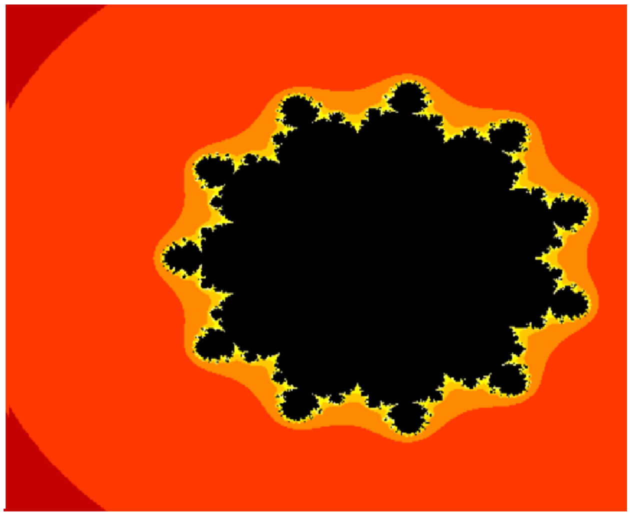




La table de [*4 modulo 91*]*, avec l'ensemble de Mandelbrot généralisé défini par* $z_{n+1} = z_n^4 + c$.

Similitudes avec les fractales





Le table de 12 modulo 143, avec l'ensemble de Mandelbrot généralisé défini par $z_{n+1} = z_n^{12} + c$.