Tables de multiplications modulaires

Projet Maths-Info : Nguyen Duong Duc & Louis Gavalda.
Sous l'encadrement d'Olivier Brunat.

Contents

1 Introduction

1.1 Remerciements

Nous tenons tout d'abord à remercier **Olivier Brunat** : il est l'enseignant-chercheur qui a

encadré notre travail. (C'est aussi lui qui a eu l'idée du sujet !) Malgré son emploi du temps chargé, il s'est toujours montré disponible.

Merci Olivier, pour votre patience et votre état d'esprit résolument positif ; votre soutien nous a permis de beaucoup avancer.

1.2 Choix du sujet

À l'origine du sujet : une vidéo de Mickaël Launay (plus connu sous le pseudonyme de Micmaths) intitulée « La face cachée des tables de multiplication. » Dans celle-ci, l'auteur propose une façon simple de représenter graphiquement n'importe quelle table de multiplication modulo un certain nombre. (Nous formaliserons cette idée par la suite.)

Quel intérêt ? Au moins celui de faire de *jolies maths*, pour reprendre la formule de l'auteur. Suivant les valeurs affectées, on observe, en construisant la figure géométrique associée, l'apparition de figures tout à fait surprenantes, et souvent magnifiques. Leur complexité laisse perplexe lorsqu'on a conscience de la simplicité du procédé de construction — il suffit de savoir compter. Comme pour les automates cellulaires ou les bancs de poissons, on a peine à s'imaginer comment de tels comportements peuvent naître de règles si simples.

Nous tenions tous les deux à travailler sur des mathématiques dont l'application aurait quelque chose de gratifiant pour l'œil ; nous souhaitions que — pour une fois — notre travail puisse intéresser même des non-mathématiciens. Ce souhait est exaucé, car les figures géométriques singulières qui inspirent notre travail piquent la curiosité de tous.

Nous avons — pour satisfaire à la partie *Info* de ce *Projet Maths-Info* — créé un site internet permettant d'afficher, pour tout couple de valeurs, la figure obtenue par le procédé de construction. Notre site est accessible à l'adresse suivante : projet-maths.info. Celui-ci a d'abord été conçu pour appuyer notre travail : il nous a notamment permis de vérifier des hypothèses en visualisant les figures obtenues pour des valeurs précises. Notre site permet d'enregistrer les figures au format SVG (comme celles qui sont présentées dans ce rapport). Les versions précédentes permettent par ailleurs d'utiliser des valeurs non entières pour observer la transition d'une figure à l'autre.

1.3 Rapport

À notre connaissance, cette façon de représenter les tables de multiplication passe pour être une curiosité mathématique : nombre de sites décrivent l'apparition de ces étonnantes formes géométriques, en revanche personne ne nous en explique l'origine.

Dans ce rapport, nous :

- formalisons le procédé de construction de la représentation graphique d'une table de multiplication modulo un certain nombre ;
- donnons et démontrons plusieurs propriétés sur les cycles apparaissant sur les figures ;
- expliquons pourquoi apparaissent les figures géométriques singulières, comme par exemple la cardioïde pour la table de 2 ;
- montrons qu'il semble exister des liens avec d'autres objets mathématiques tout aussi surprenants : les fractales.

2 Caractéristiques algébriques

2.1 Procédé de construction

Comment représente-t-on sur un cercle la table de m modulo M ?

Sur le cercle, on dispose tout d'abord M points, régulièrement espacés (comme le sont les heures sur le cadran d'une horloge) et qu'on numérote, se suivant, de 0 à $M-1$. Pour se simplifier la vie, et s'il n'y a pas d'ambiguïté, on appellera k le k-ème point, et *cadran* la figure formée par le cercle et les points.

Nous pouvons dès lors associer à n'importe quel entier un point du cercle. Le cadran peut être vu comme une représentation graphique de l'anneau $\mathbb{Z}/M\mathbb{Z}$, où chacun des M points du cercle représente une classe d'équivalence. Ainsi un entier n sera représenté par le k-ème point du cadran, où k est le reste dans la division euclidienne de n par M. (On note que les points du cercle pourraient aussi être vus comme les racines de l'unité dans le plan complexe.)

Le procédé de construction est simple :

- 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.

On obtient ainsi la représentation graphique de la table de m modulo M. On notera qu'un point peut tout à fait être relié à lui-même (par un segment de longueur nulle, qui sera donc invisible).

2.2 Exemples de figures obtenues

Quelles que soient les valeurs affectées à m et M, la représentation graphique fait apparaître des formes géométriques vraiment étonnantes. Celles-ci sont en général d'autant plus nettes que les

valeurs de m et M sont grandes.

Pour $m = 2$ (la représentation de la table de 2 modulo M), une cardioïde se dessine :

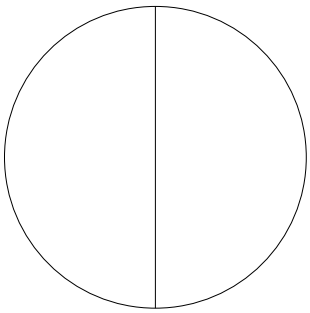


Table de 2 modulo 2.

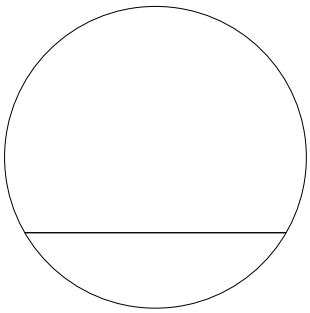


Table de 2 modulo 3.

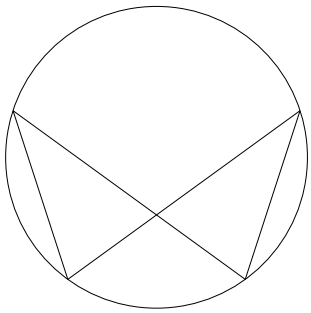


Table de 2 modulo 5.

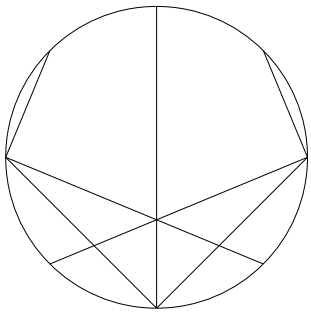


Table de 2 modulo 8.

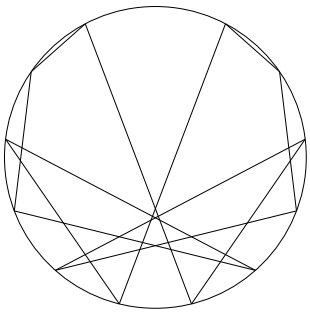


Table de 2 modulo 13.

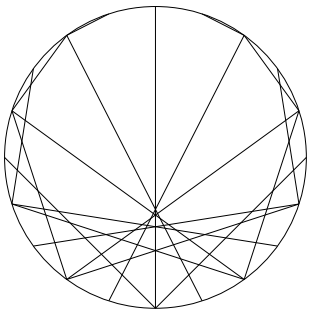


Table de 2 modulo 20.

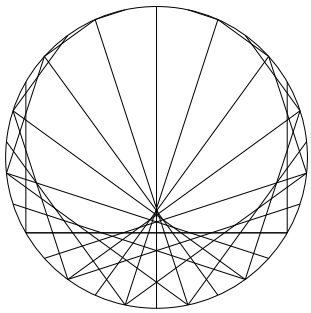


Table de 2 modulo 30.

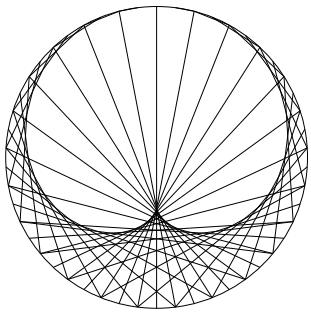


Table de 2 modulo 50.

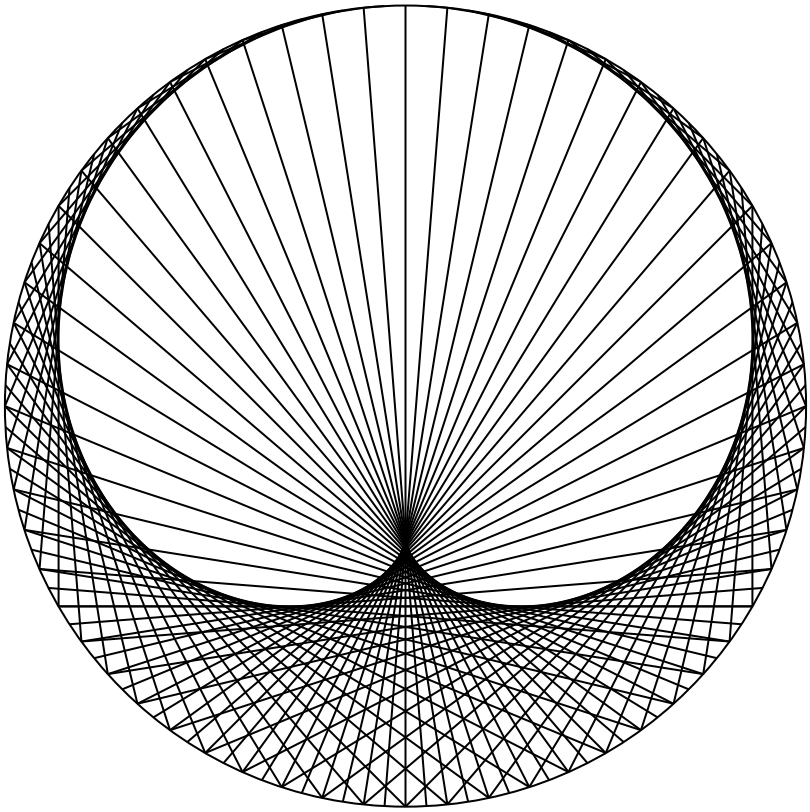


Table de 2 modulo 120.

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

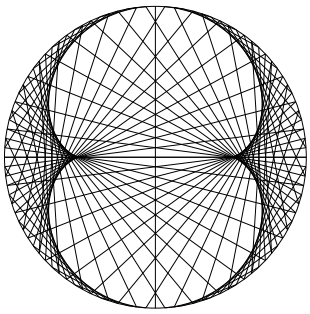


Table de 3 modulo 100.

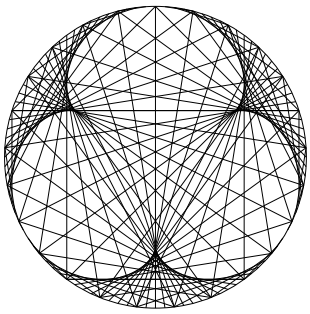


Table de 4 modulo 100.

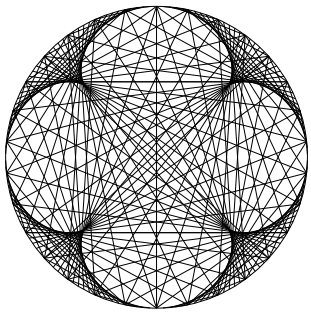


Table de 5 modulo 150.

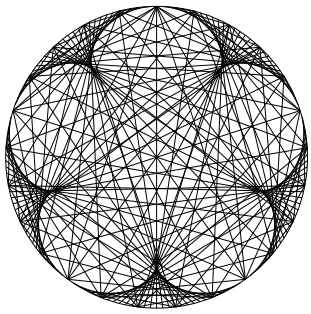


Table de 6 modulo 150.

Les arrondis contrarient l'intuition : ils paraissent incompatibles avec le procédé de construction dans la mesure où celui-ci consiste uniquement à tracer des traits. Pour certaines valeurs, les figures obtenues sont particulièrement remarquables :

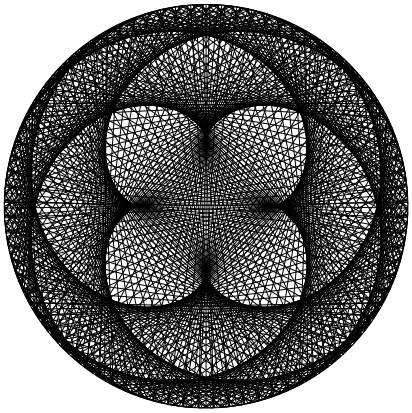


Table de 166 modulo 656.

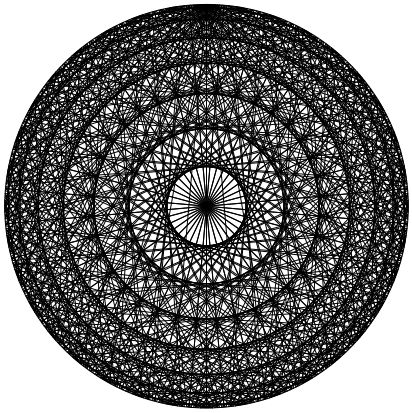


Table de 757 modulo 576.

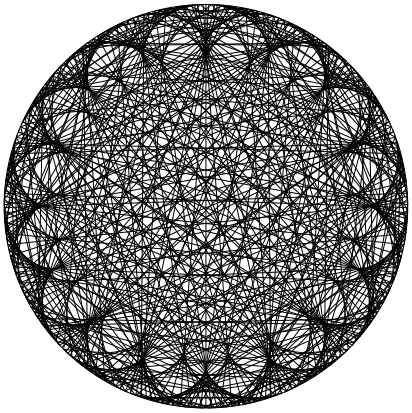


Table de 230 modulo 442.

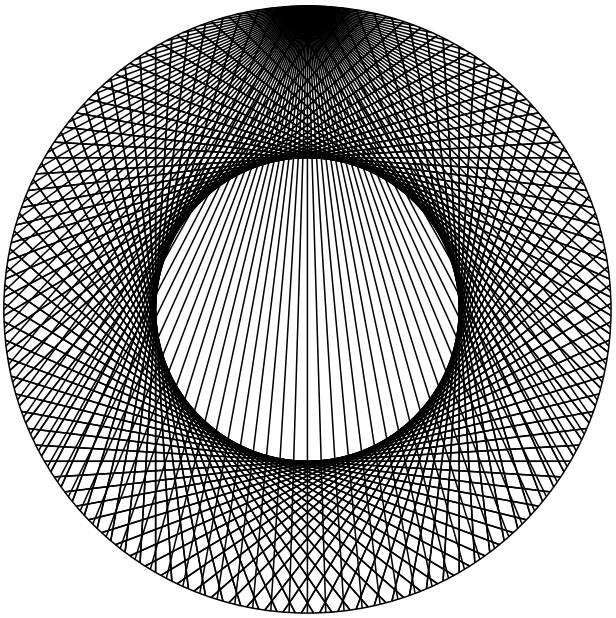


Table de 521 modulo 312.

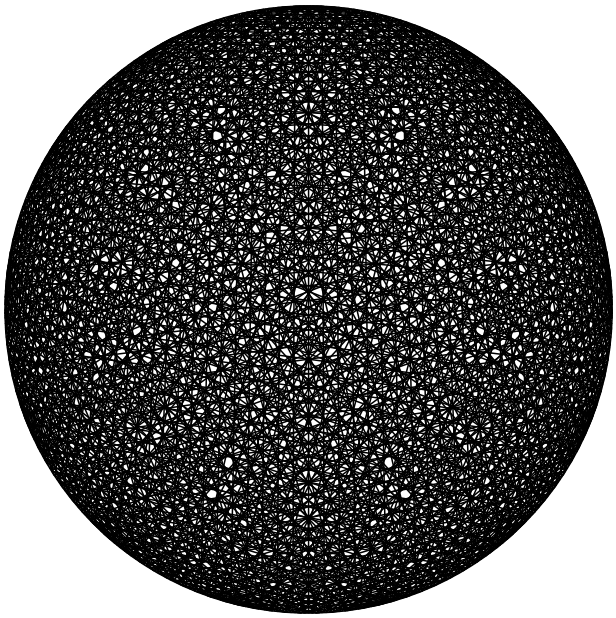


Table de 726 modulo 848.

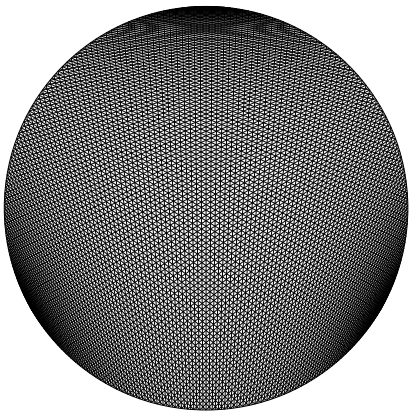


Table de 410 modulo 412.

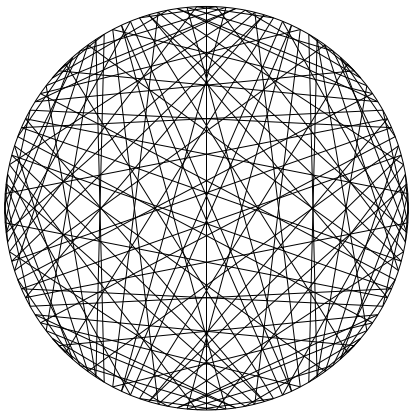


Table de 37 modulo 130.

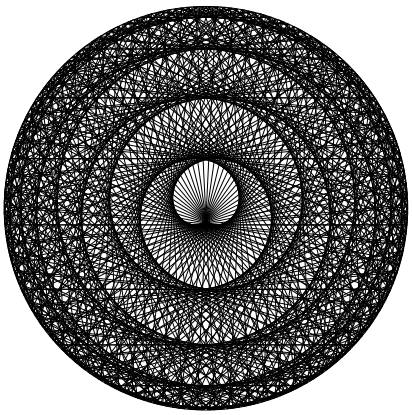


Table de 189 modulo 627.

Qu'est-ce qui provoque l'émergence de ces formes ? Dans la suite de ce rapport, nous apportons des éléments de réponse qui expliquent ce comportement.

2.3 Propriétés des cycles

On s'intéresse dans ce qui suit à la représentation graphique de la table de m modulo M. Soit $0 \leq k \leq M-1$ un point du cadran.

On suppose que $pgcd(m, M) = 1$ (c'est-à-dire que m et M sont premiers entre eux). $\bar{m} \in (\mathbb{Z}/M\mathbb{Z})^\times$.

Le sous-groupe $\langle \bar{m} \rangle$ de $(\mathbb{Z}/M\mathbb{Z})^\times$ agit sur $\mathbb{Z}/M\mathbb{Z}$ par :

$$\begin{aligned} \langle \bar{m} \rangle \times \mathbb{Z}/M\mathbb{Z} &\longrightarrow \mathbb{Z}/M\mathbb{Z}, \\ (\bar{m}^j, \bar{k}) &\longmapsto \overline{m^j k} \end{aligned}$$

Une précision : $(\mathbb{Z}/M\mathbb{Z})^\times$ agit sur $\mathbb{Z}/M\mathbb{Z}$ par $(\bar{x}, \bar{k}) \longmapsto \overline{xk}$. L'action de groupe ci-dessus d'obtient simplement par restriction au sous-groupe $\langle \bar{m} \rangle \subseteq (\mathbb{Z}/M\mathbb{Z})^\times$.

Les résultats connus s'appliquent donc ici.

2.3.1 Orbite d'un élément

L'orbite $\mathcal{O}(\bar{k}) = \{p \in \mathbb{Z}/M\mathbb{Z} \mid \exists k' \in \langle \bar{m} \rangle,\ p = k' \cdot \bar{k}\} = \langle \bar{m} \rangle \cdot \bar{k}$ d'un point $\bar{k}$ se trouve être représentée graphiquement par un *cycle*, c'est-à-dire par l'unique chemin qui part de p pour y revenir (en passant par un nombre fini de points du cadran). Un point relié seulement à lui-même est ainsi seul dans son orbite — c'est toujours le cas pour 0 puisque $\forall j \in \mathbb{Z},\ \bar{m}^j \cdot \bar{0} = \bar{0}$.

Puisque l'application

$$f : \mathbb{Z}/M\mathbb{Z} \longrightarrow \mathbb{Z}/M\mathbb{Z}$$
$$\bar{k} \longmapsto \overline{mk}$$

est bijective (on a supposé que $pgcd(m, M) = 1$), il s'agit d'une permutation de $\mathbb{Z}/M\mathbb{Z}$. On peut ainsi décomposer f en produit de cycles à supports disjoints.

Afin de gagner en clarté, on notera dans la suite $ord_n(\bar{m})$ l'ordre de $\bar{m}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. On pose également

$$d = pgcd(k, M) \text{ et } d' = \frac{M}{pgcd(k, M)}.$$

Le cycle de $\bar{k}$ est $\{\bar{k},\ \overline{mk},\ \overline{m^2k},\ \ldots,\ \overline{m^{s-1}k}\}$. On aimerait en particulier déterminer s, qui est le plus petit entier à vérifier $\overline{m^sk} = \bar{k}$: s'agit de la longueur du cycle (*i.e.* la taille de l'orbite). On sait que s existe par le théorème de décomposition en cycles à supports disjoints.

$$\begin{aligned}
&\bar{m}^s\bar{k} = \bar{k} \\
\iff\ &\bar{m}^s\bar{k} = \bar{k} \\
\iff\ &(\bar{m}^s - 1) \cdot \bar{k} = \bar{0} \\
\iff\ &\exists q \in \mathbb{Z},\ (m^s - 1) \cdot k = qM \\
\iff\ &\exists q \in \mathbb{Z},\ (m^s - 1) \cdot \frac{k}{pgcd(k, M)} = q \cdot d' \\
\iff\ &(\bar{m}^s - \bar{1}) \cdot \overline{\frac{k}{pgcd(k, M)}} = \bar{0} \text{ dans } \frac{\mathbb{Z}}{d'\mathbb{Z}}
\end{aligned}$$

Or on a :

$$pgcd(\frac{k}{pgcd(k, M)}, \frac{M}{pgcd(k, M)}) = 1, \text{ donc}$$
$$\frac{\bar{k}}{pgcd(k, M)} \in (\frac{\mathbb{Z}}{d'\mathbb{Z}})^\times$$

On peut ainsi multiplier par $(\overline{\frac{k}{pgcd(k,M)}})^{-1}$ pour parvenir à

$$\begin{aligned}
&\bar{m}^s\bar{k} = \bar{k} \\
\iff\ &\bar{m}^s - \bar{1} = \bar{0} \text{ dans } \frac{\mathbb{Z}}{d'\mathbb{Z}}
\end{aligned}$$

L'orbite $\mathcal{O}(\bar{k})$ de $\bar{k}$ est donc de cardinal $ord_{d'}(\bar{m})$.

$$\mathcal{O}(\bar{k}) = \{\bar{k},\ \overline{mk},\ \overline{m^2k},\ \ldots,\ \overline{m^{s-1}k}\} \text{ avec } s = ord_{d'}(\bar{m}).$$

2.3.2 Nombre d'orbites

$pgcd(m, M) = 1$.

Soit $d \mid M \iff \exists d' \in \mathbb{N},\ M = dd'$.

L'application

$$\begin{aligned} f_{d'} : (\mathbb{Z}/d'\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/d'\mathbb{Z})^\times \\ \bar{k} &\longmapsto \overline{mk} \end{aligned}$$

est bien définie puisque $pgcd(m, M) = 1$, donc $pgcd(\frac{M}{d}, m) = pgcd(d', M) = 1$, donc $\bar{m} \in (\mathbb{Z}/d'\mathbb{Z})^\times$. De plus, $f_{d'}$ est bijective de réciproque $\bar{k} \longmapsto \bar{m}^{-1}\bar{k}$.

Tous les cycles de $f_{d'}$ sont de longueur $ord_{d'}(\bar{m})$ (voir partie précédente).

❧

L'application Φ :

$$\begin{aligned} \{\text{orbites de } \mathbb{Z}/M\mathbb{Z}\} &\longrightarrow \{\text{cycles de } f_{d'},\ d' | M \text{ (dans la décomposition en cycles disjoints)}\} \\ \mathcal{O} &\longmapsto \text{cycle de } f_{d'} \text{ de } \bar{k}/pgcd(k, M) \end{aligned}$$

est bien définie. ($\bar{k} \in \mathcal{O}$, et on rappelle que $d' = \frac{M}{pgcd(k,M)}$.)

Il s'agit de montrer que $d' = \frac{M}{pgcd(k,M)}$ et le cycle de $\overline{\frac{k}{pgcd(k,M)}}$ dans $f_{d'}$ ne dépendent pas du choix de $\bar{k} \in \mathcal{O}$.

Ceci est vrai puisque m et M sont premiers entre eux, donc par Gauss on a $pgcd(mk, M) = pgcd(m, M)$.

Soient $\bar{k},\ \bar{k'} \in \mathcal{O}$ (deux éléments de la même orbite). Il existe $i \in \mathbb{N}$ tel que $\bar{k'} = \bar{m}^i\bar{k}$.

$$\overline{\frac{k'}{pgcd(M, k')}} = \overline{\frac{k'}{pgcd(M, k)}} = \overline{m}^i \cdot \overline{\frac{k}{pgcd(M, k)}}$$

car $pgcd(M, k) = pgcd(M, k')$ par ce qui précède.

Donc $\overline{\frac{k'}{pgcd(M,k')}}$ et $\overline{\frac{k}{pgcd(M,k)}}$ sont bien dans le même cycle de $f_{d'}$.

Donc Φ est bien définie.

❧

Montrons maintenant que Φ est injective.

Soient $\mathcal{O}$ et $\mathcal{O}'$ deux orbites tels que $\Phi(\mathcal{O}) = \Phi(\mathcal{O}')$.

Par définition de Φ, on a :

$\Phi(\mathcal{O})$ est un cycle de $f_{d'_{\mathcal{O}}}$ de $\overline{\frac{k_{\mathcal{O}}}{pgcd(k_{\mathcal{O}},M)}}$, où $k_{\mathcal{O}} \in \mathcal{O}$.

$\Phi(\mathcal{O}')$ est un cycle de $f_{d'_{\mathcal{O}}}$ de $\overline{\frac{k_{\mathcal{O}'}}{pgcd(k_{\mathcal{O}'},M)}}$, où $k_{\mathcal{O}'} \in \mathcal{O}'$.

Ainsi, si $\Phi(\mathcal{O}) = \Phi(\mathcal{O}')$, alors $d'_{\mathcal{O}} = d'_{\mathcal{O}'}$ et $\overline{\frac{k_{\mathcal{O}}}{pgcd(k_{\mathcal{O}},M)}}$ et $\overline{\frac{k_{\mathcal{O}'}}{pgcd(k_{\mathcal{O}'},M)}}$ sont dans le même cycle de $f_{d'_{\mathcal{O}}}$.

C'est-à-dire que $\exists j \in \mathbb{N}$ tel que $\overline{\frac{k_{\mathcal{O}'}}{pgcd(k_{\mathcal{O}'},M)}} = \bar{m}^j \cdot \overline{\frac{k_{\mathcal{O}}}{pgcd(k_{\mathcal{O}},M)}}$.

Or $d'_{\mathcal{O}} = d'_{\mathcal{O}'} \iff pgcd(k_{\mathcal{O}'}, M) = pgcd(k_{\mathcal{O}}, M)$, d'où :

$$\overline{\frac{k_{\mathcal{O}'}}{pgcd(k_{\mathcal{O}}, M)}} = \bar{m}^j \cdot \overline{\frac{k_{\mathcal{O}}}{pgcd(k_{\mathcal{O}}, M)}}$$

C'est-dire :

$$\exists q \in \mathbb{Z},\ \overline{\frac{k_{\mathcal{O}'}}{pgcd(k_{\mathcal{O}}, M)}} = m^j \cdot \frac{k_{\mathcal{O}}}{pgcd(k_{\mathcal{O}}, M)} + q d'_{\mathcal{O}}$$

Or $d'_{\mathcal{O}} = \frac{n}{pgcd(k_{\mathcal{O}},M)}$, d'où :

$\frac{k_{\mathcal{O}'}}{pgcd(k_{\mathcal{O}},n)} = m^j \frac{k_{\mathcal{O}}}{pgcd(k_{\mathcal{O}},M)} + \frac{n}{pgcd(k_{\mathcal{O}},M)} \cdot q$ et en multipliant par $pgcd(k_{\mathcal{O}}, M)$ et en regardant dans $\mathbb{Z}/M\mathbb{Z}$, on obtient :

$\overline{k}_{\mathcal{O}'} = \overline{m}^j \overline{k}_{\mathcal{O}}$ dans $\mathbb{Z}/n\mathbb{Z}$ i.e $\mathcal{O} = \mathcal{O}'$.

D'où l'injectivité de Φ.

❧

Montrons maintenant que Φ est surjective :

Soit $d'|M$ et c un cycle de $f_{d'}$.

Soit $\bar{k} \in c$. Alors $pgcd(k, d') = 1$.

Posons $d = \frac{M}{d'}$. On a $0 \leq k < \frac{M}{d}$, donc $0 \leq kd < M$ et $pgcd(kd, M) = pgcd(kd, dd') = d \cdot pgcd(k, d') = d$.

Or $\frac{M}{pgcd(kd,M)} = \frac{dd'}{pgcd(kd,dd')} = \frac{dd'}{pgcd(k,d')} = \frac{dd'}{d} = d'$

$\Phi(\mathcal{O}(\overline{kd}))$ = cycle de $\overline{\frac{kd}{pgcd(kd,M)}} = \bar{k}$ de $f_{d'}$.

Donc $\Phi(\mathcal{O}(\overline{kd})) = c$, où $\mathcal{O}(\overline{kd})$ est l'orbite de $\overline{kd}$.

D'où la surjectivité de Φ.

❧

Ainsi Φ est bijective. Donc :

$|\{\text{orbites de } \mathbb{Z}/n\mathbb{Z} \text{ sous f}\}| = |\{\text{cycles de } f_{d'} \ ; d'|M\}| = |\sqcup_{d'|n} \{\text{cycles de } f_{d'}\}|$.

Donc $|\{\text{orbites}\}| = \sum_{d'|M} |\{\text{cycles de } f_{d'}\}|$.

Or tous les cycles de $f_{d'}$ ont la même taille, qui vaut $ord_{d'}(\bar{m})$.

Il y a donc $\frac{|(\mathbb{Z}/d'\mathbb{Z})^\times|}{ord_{d'}(\bar{m})}$ cycles dans la décomposition de $f_{d'}$, c'est à dire $\frac{\varphi(d')}{ord_{d'}(\bar{m})}$.

D'où $|\{\text{orbites}\}| = \sum_{d'|M} \frac{\varphi(d')}{ord_{d'}(\bar{m})}$, où φ est l'indicatrice d'Euler.

On a ainsi établi le nombre précis d'orbites dans la figure construite.

3 Origine des formes géométriques

Les formes géométriques qui se dessinent spontanément ressemblent beaucoup à certaines courbes définies par des équations paramétriques. On voit notamment apparaître des épicycloïdes : la représentation de la table de 2 nous donne par exemple une cardioïde.

3.1 Problème

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 $u(t)$.

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 $\{\Delta_t \mid t \in I\}$.

En rajoutant quelques hypothèses, nous verrons que l'on peut 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.

Rappelons que dans ce cas, le point de coordonné $f(t)$ admet une tangente de vecteur directeur $f'(t) = \begin{pmatrix} x'(t) \\ y'(t) \end{pmatrix}$.

3.2 Proposition

Si on suppose que $t \longmapsto A(t)$ et $t \longmapsto u(t)$ sont C^1, et qu'en plus $det(u(t), u'(t)) \neq 0$, alors il existe une unique courbe $\mathcal{C}$ vérifiant l'équation paramétrique $f : I \longrightarrow \mathbb{R}^2$ de classe C^1 donnée par :

$$\forall t \in I,\ f(t) = A(t) + \frac{det(A'(t), u(t))}{det(u(t), u'(t))} \cdot u(t)$$

3.3 Preuve

On procède par analyse-synthèse : Supposons que $\mathcal{C}$ existe.

On a alors $u \in C \iff \begin{cases} \exists t \in I,\ u \in \Delta_t \\ \Delta_t \text{ est tangente à } \mathcal{C} \text{ en } u \end{cases}$

Soit $f(t)$ les coordonnées de u dans le repère. Comme $u \in \Delta_t$, il existe $\lambda(t) \in \mathbb{R}$ tel que $f(t) = A(t) + \lambda(t) \cdot u(t)$.

Supposons que $t \longmapsto \lambda(t)$ est C^1. En particulier f est C^1.

De plus, Δ_t tangente à $\mathcal{C}$ en u se traduit par : $\overrightarrow{Of'(t)}$ et $u(t)$ sont colinéaires $\iff$ $det(\overrightarrow{Of'(t)}, u(t)) = 0$.

Or $f'(t) = A'(t) + \lambda'(t)u(t) + \lambda(t)u'(t)$et la bilinéarité du déterminant donne :

$$\begin{aligned} det(\overrightarrow{Of'(t)}, u(t)) &= det(A'(t) + \lambda'(t) \cdot u(t) + \lambda(t) \cdot u'(t), u(t)) \\ &= det(A'(t), u(t) + \lambda'(t) \cdot det(u(t), u(t)) + \lambda(t) \cdot det(u'(t), u(t)) \\ &= det(A'(t), u(t) + \lambda(t) \cdot det(u'(t), u(t)) \end{aligned}$$

car $\lambda'(t) \cdot det(u(t), u(t)) = 0$ (déterminant alterné).

D'où $\lambda(t) \cdot det(u'(t), u(t)) = -det(A'(t), u(t))$, c'est-à-dire

$$\lambda(t) = \frac{det(A'(t),\ u(t))}{det(u(t), u'(t))}$$

car $det(u(t),\ u'(t)) \neq 0$.

Ainsi $f(t) = A(t) + \frac{det(A'(t),\, u(t))}{det(u(t),\, u'(t))} \cdot u(t)$.

Réciproquement, soit $\mathcal{C}$ la courbe d'équation paramétrique f donnée par la formule ci-dessus. Alors f est C^1. De plus, si $u \in C$, alors il existe $t \in I$ tel que u est de coordonnées $f(t)$ (car f est une équation paramétrique de $\mathcal{C}$) et $f(t) \in \Delta_t$ (pour $\lambda = \frac{det(A'(t),\, u(t))}{det(u(t),\, u'(t))}$).

Il reste à vérifier que $f'(t)$ et $u(t)$ sont colinéaires. Or le calcul précédent donne :

$$\begin{aligned} det(\overrightarrow{Of'(t)}, u(t)) &= det(A'(t), u(t)) + \frac{det(A'(t),\ u(t))}{det(u(t),\ u'(t))} \cdot det(u'(t), u(t)) \\ &= \frac{det(u(t), u'(t)) \cdot det(A'(t), u(t)) + det(A'(t), u(t)) \cdot det(u'(t), u(t))}{det(u(t), u'(t))} \\ &= \frac{-det(u'(t), u(t)) \cdot det(A'(t), u(t)) + det(A'(t), u(t)) \cdot det(u'(t), u(t))}{det(u(t), u'(t))} \\ &= 0 \end{aligned}$$

D'où le résultat.

❧

Soit $m \in \mathbb{N}^*$. Appliquons la proposition précédente à la droite Δ_t ($t \in \mathbb{R}$) passant par $A(t) = \begin{pmatrix} cos(t) \\ sin(t) \end{pmatrix}$ et $A(mt)$.

$u(t) = \overrightarrow{A(t)A(mt)} = \begin{pmatrix} cos(mt) - cos(t) \\ sin(mt) - sin(t) \end{pmatrix}$ est un vecteur directeur de Δ_t et on a $t \longmapsto A(t)$ et $t \longmapsto u(t)$ toutes les deux C^1.

$$u'(t) = \begin{pmatrix} sin(t) - msin(mt) \\ mcos(mt) - cos(t) \end{pmatrix}$$

De plus :

$$\begin{aligned} det(u(t), u'(t)) &= det \begin{pmatrix} cos(mt) - cos(t) & sin(t) - m \cdot sin(mt) \\ sin(mt) - sin(t) & m \cdot cos(mt) - cos(t) \end{pmatrix} \\ &= m \cdot cos^2(mt) - cos(t) \cdot cos(mt) - mcos(t) \cdot cos(mt) + cos^2(t) \\ &\quad - (sin(t) \cdot sin(mt) - sin^2(t) - m \cdot sin^2(mt) + m \cdot sin(t) \cdot sin(mt)) \\ &= m(cos^2(mt) + sin^2(mt)) + cos^2(t) + sin^2(t) \\ &\quad - (m+1)(cos(t) \cdot cos(mt) + sin(t) \cdot sin(mt)) \\ &= (m+1)(1 - cos(m-1)t) \neq 0 \ \text{ si } t \neq 0 \ [2\pi] \end{aligned}$$

Si $t \in]0, 2\pi[$, alors $det(u(t), u'(t)) \neq 0$et on peut appliquer la proposition.

La courbe d'équation paramétrique $f(t) = \begin{pmatrix} cos(t) \\ sin(t) \end{pmatrix} + \frac{det(A'(t),\, u(t))}{det(u(t),\, u'(t))} \cdot u(t)$ admet donc la droite $(A(t), A(mt))$ comme tangente.

Or :

$$\begin{aligned} det(A'(t), u(t)) &= \begin{vmatrix} -sin(t) & cos(mt) - cos(t) \\ cos(t) & sin(mt) - sin(t) \end{vmatrix} \\ &= sin^2(t) - sin(t) \cdot sin(mt) + cos^2(t) - cos(t) \cdot cos(mt) \\ &= 1 - (cos(t) \cdot cos(mt) + sin(t) \cdot sin(mt)) \\ &= 1 - (cos(m-1) \cdot t) \\ &= 1 - cos((m-1) \cdot t) \end{aligned}$$

D'où :

$$\begin{aligned} f(t) &= \begin{pmatrix} cos(t) \\ sin(t) \end{pmatrix} + \frac{1 - cos((m-1)t)}{(m+1)(1-cos(m-1)t)} \cdot \begin{pmatrix} cos(mt) - cos(t) \\ sin(mt) - sin(t) \end{pmatrix} \\ &= \begin{pmatrix} cos(t) \\ sin(t) \end{pmatrix} + \frac{1}{m+1} \cdot \begin{pmatrix} cos(mt) - cos(t) \\ sin(mt) - sin(t) \end{pmatrix} \\ &= \frac{1}{m+1} \cdot \begin{pmatrix} m \cdot cos(t) + cos(mt) \\ m \cdot sin(t) + sin(mt) \end{pmatrix} \end{aligned} .$$

3.4 Remarques

- si $t = 0\ [2\pi]$, les points $A(mt)$ et $A(t)$ sont confondus et ne définissent pas de droites.
- On s'intéresse aux droites passant par les points e^{it} et e^{mit}. Soit M_k le point d'affixe $e^{\frac{2ik\pi}{n}}$. Il est relié à $M_{k'}$

d'affixe $e^{\frac{2ik'\pi}{n}}$, où k' est le reste dans la division euclidienne de km par n. Appelons q et k' respectivement le quotient et le reste, c'est-à-dire qu'on a $km = qn + k'$. On a alors : $e^{\frac{m2ik\pi}{n}} = e^{\frac{2ik(qn+k')\pi}{n}} = e^{\frac{2ikq\pi + 2ik'\pi}{n}} = e^{\frac{2ikq\pi}{n}} \cdot e^{\frac{2ik'\pi}{n}} = e^{\frac{2ik'\pi}{n}}$. Ainsi $M_{km} = M_{k'}$ et on peut donc bien travailler avec e^{it} et e^{mit} sans tenir compte du reste, c'est-à-dire en identifiant avec la multiplication par m. + $\{\frac{k}{n} \mid k,\ n \in \mathbb{N},\ n \neq 0,\ k < n\}$ est dense dans $]0, 1[$. Donc $\{\frac{2k\pi}{n} \mid n \neq 0,\ k < n\}$ est dense dans $]0, 2\pi[$. Soient $t \in]0, 2\pi[$, k et n tels que $\frac{2k\pi}{n}$ est « proche » de t. Alors $\frac{2mk\pi}{n}$ est « proche » de mt. Ainsi, par continuité de l'exponentielle complexe, $e^{2i\frac{k\pi}{n}}$ est « proche » de e^{it} et $e^{2i\frac{mk\pi}{n}}$ est « proche » de e^{mit}. Géométriquement, la droite $(A(\frac{2k\pi}{n}), A(\frac{2mk\pi}{n}))$ est « proche » de $(A(t), A(mt))$. + Pour m = 2, l'équation de $\mathcal{C}$ est $f(t) = \frac{1}{3}\begin{pmatrix} 2cos(t) + cos(2t) \\ 2sin(t) + sin(2t) \end{pmatrix}$, ce qui nous donne bien une cardioïde. La formule proposée par Wikipédia est à une dilatation près (le facteur a) :

$$\begin{cases} x(t) = cos(t) \cdot (1 + cos(t)) = \frac{1}{2} + \frac{2cos(t) + cos(2t)}{2} \\ y(t) = sin(t) \cdot (1 + cos(t)) = \frac{2sin(t) + sin(2t)}{2} \end{cases}$$

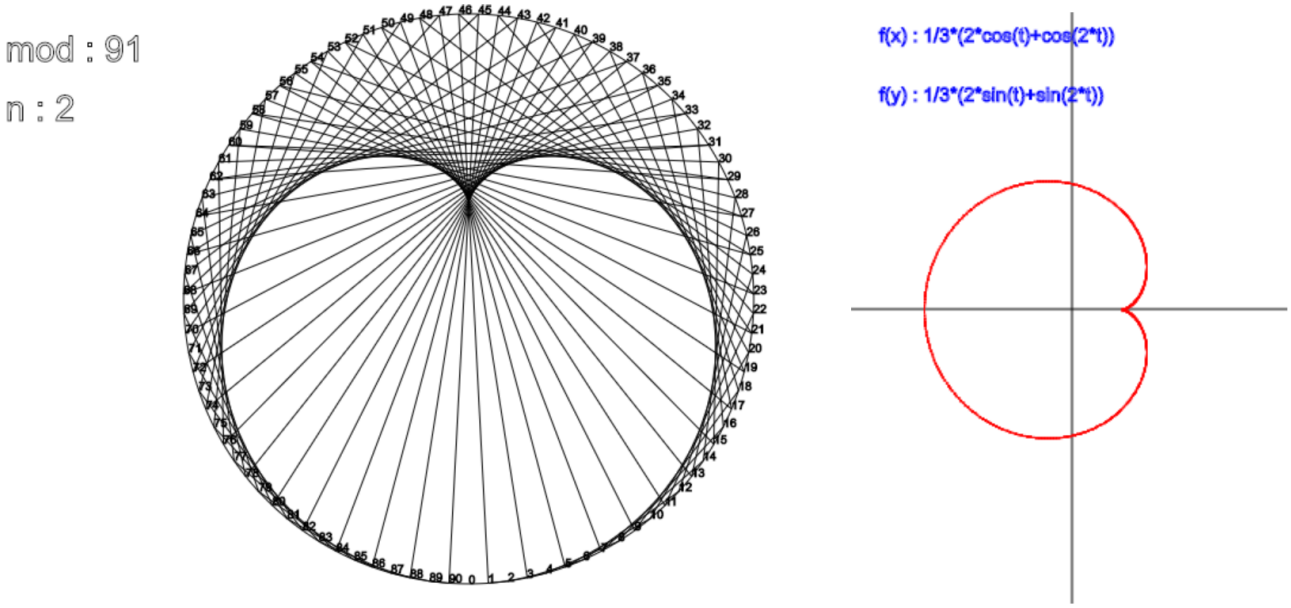
$$\text{soit } \begin{pmatrix} x(t) \\ y(t) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} + \frac{3}{2} f(t).$$

3.5 Exemples

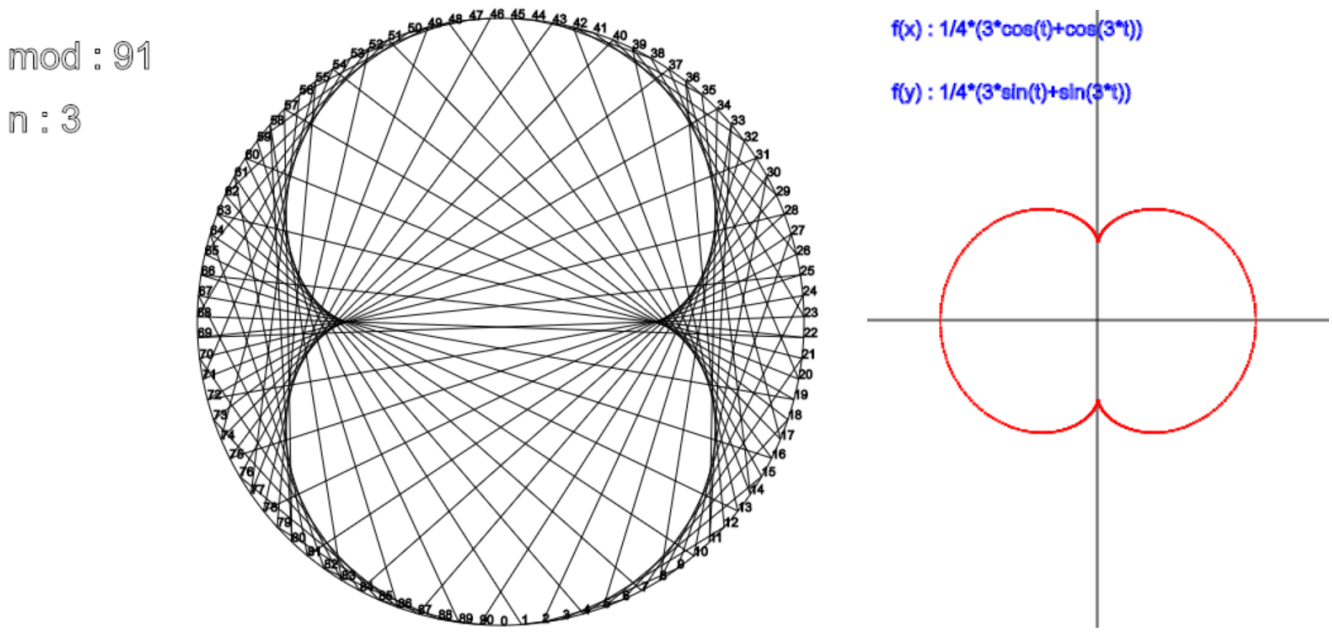
Grâce au résultat obtenu, nous pouvons tracer les équations paramétriques et les comparer aux

représentations graphiques de certaines tables de multiplication.

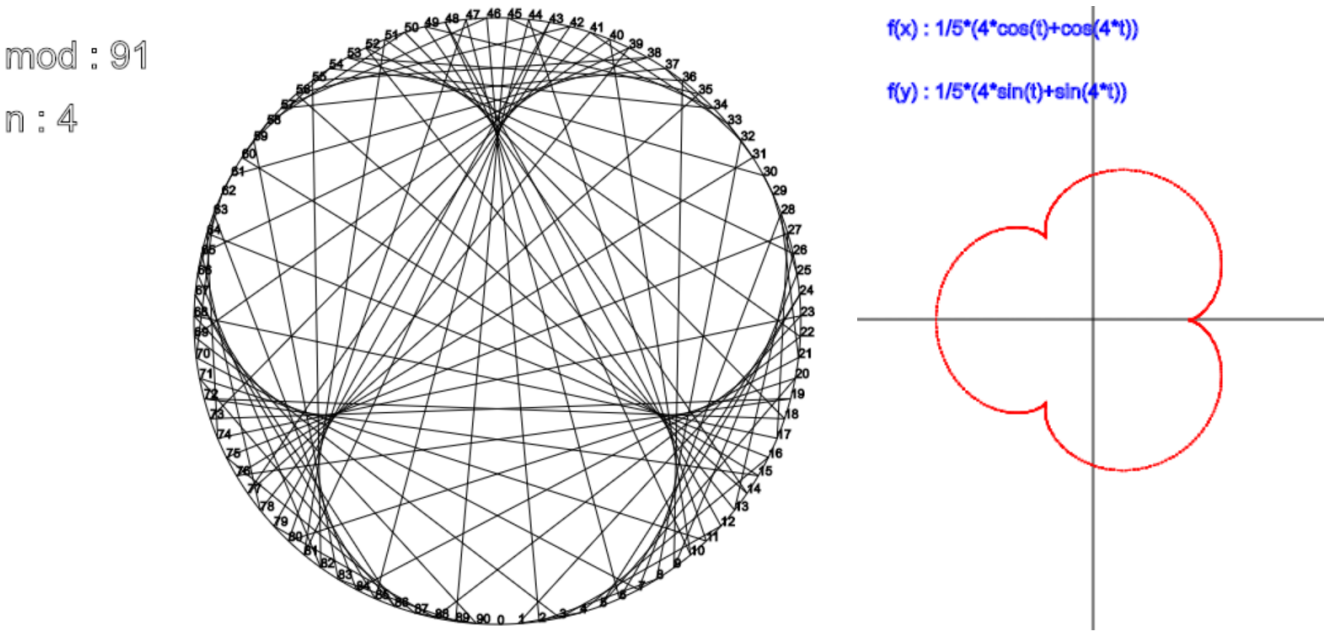
Voici quelques exemples tirés des programmes que nous avons conçus :



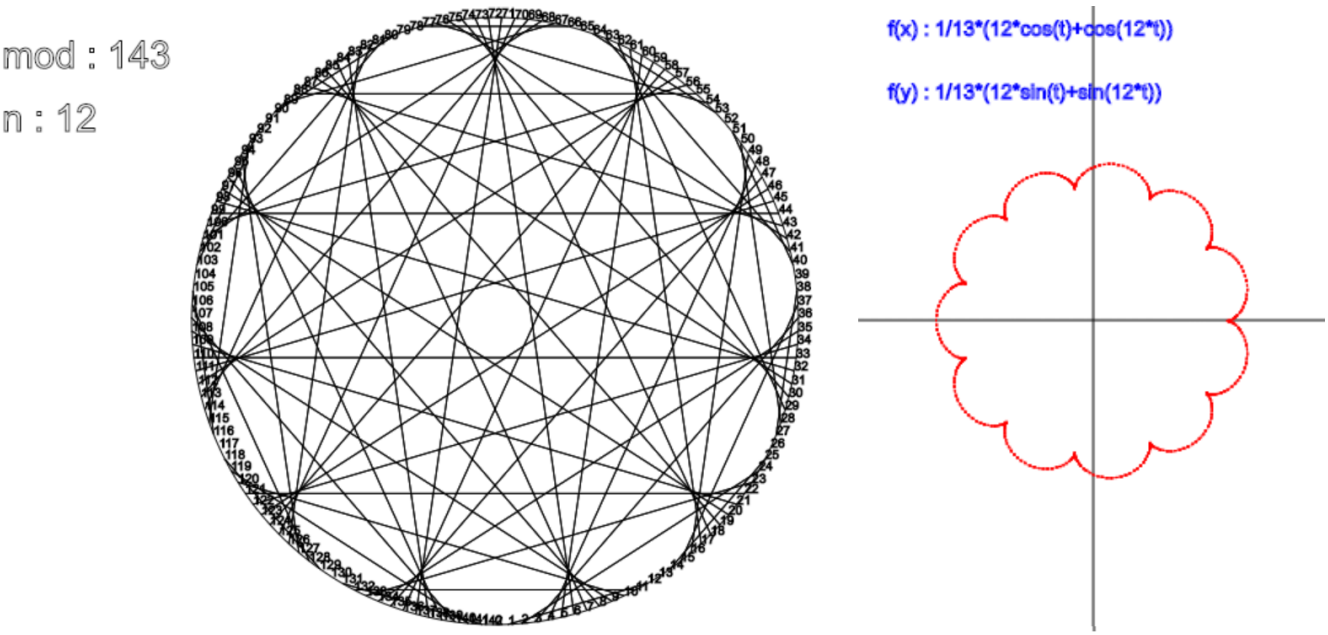
La table de de 2 modulo 91, avec la courbe d'équation paramétrique $f(t) = \frac{1}{3}\begin{pmatrix} 2cos(t) + cos(2t) \\ 2sin(t) + sin(2t) \end{pmatrix}$.



La table de de 3 modulo 91, avec la courbe d'équation paramétrique $f(t) = \frac{1}{4}\begin{pmatrix} 3cos(t) + cos(3t) \\ 3sin(t) + sin(3t) \end{pmatrix}$.



La table de 4 modulo 91, avec la courbe d'équation paramétrique $f(t) = \frac{1}{5}\begin{pmatrix} 4cos(t) + cos(4t) \\ 4sin(t) + sin(4t) \end{pmatrix}$.



La table de 12 modulo 143, avec la courbe d'équation paramétrique $f(t) = \frac{1}{13}\begin{pmatrix} 12cos(t) + cos(12t) \\ 12sin(t) + sin(12t) \end{pmatrix}$.

Les figures obtenues sont bien les mêmes.

4 Fractales et ensembles de Mandelbrot généralisés

On remarque que les fractales produites à partir des ensembles de Mandelbrot ressemblent beaucoup aux figures obtenues par le procédé de construction.

4.1 Définition

En mathématiques, 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 :

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

est bornée.

4.2 Algorithme(s) de construction

Définition de la fractale utilisée pour l'algorithme (équivalente à la définition précédente) :

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 :

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

Pour déterminer si le point C appartient ou non à l'ensemble de Mandelbrot généralisé, on commence par calculer les termes des suites (x_n) et (y_n). Prenons deux exemples concrets de l'ensemble de Mandelbrot d'ordre 2 (en arrondissant les résultats) définis par :

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

- 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 $M_0(0, 0)$, $M_1(0.1, 0.2)$, $M_2(0.07, 0.24)$, $M_3(0.0473, 0.234)$, $M_4(0.0477, 0.222)$, $M_5(0.0529, 0.221)$.

Nous allons nous intéresser à la distance $OM_n = \sqrt{x_n^2 + y_n^2}$, c'est-à-dire à la distance qui sépare le point M_n de l'origine du repère, et nous pouvons constater que deux situations peuvent se présenter :

- soit la distance OM_n augmente infiniment, autrement dit les suites (x_n) et (y_n) divergent vers l'infini ;
- soit la distance OM_n est bornée, autrement dit les suites (x_n) et (y_n) sont bornées.

Évidemment, tout cela n'est que conjecture car nous n'avons calculé que les 6 premiers termes de chaque suite. Toutefois, un résultat que l'on admettra permet d'affirmer que si la distance OM_n devient supérieure à 2 à partir d'un certain rang, alors la suite M_n diverge et la distance OM_n tends vers l'infini. En revanche, si pour une valeur de n suffisamment grande, la distance OM_n reste inférieure à 2, alors on pourra considérer que les deux suites sont bornées et que cette distance OM_n est bornée (minorée par 0 et majorée par 2).

La règle de prise de décision quant à l'appartenance de $C(c_x, c_y)$ à l'ensemble de Mandelbrot généralisé est alors la suivante :

- soit le point M_n « s'éloigne » infiniment de l'origine, auquel cas le point C n'appartient pas à l'ensemble de Mandelbrot généralisé (ce qui est le cas du point $C(1, 1)$ dans l'exemple précédént) ;
- 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 généralisé (c'est le cas du point $C(0.1, 0.2)$ dans l'exemple précédent).

Dans nos programmes, nous utilisons l'algorithme suivant. Soit I_{max} le nombre de termes de la suite M_n définie comme ci-dessus :

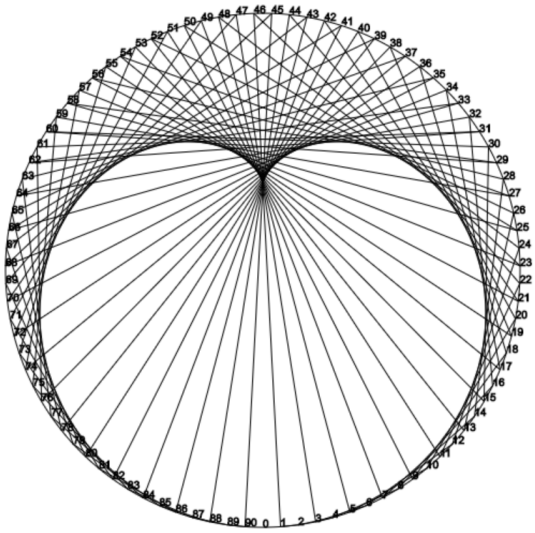
```
Pour chaque pixel C de coordonnées (x,y):
|Tant que la distance OM_n < 2 et que n < I_max:
||Calculer les coordonnées de M_n
||Affecter à n la valeur n+1
|Fin Tant que
|Si n = I_max alors:
||Colorier le pixel en noir
|Fin Si
Fin Pour
```

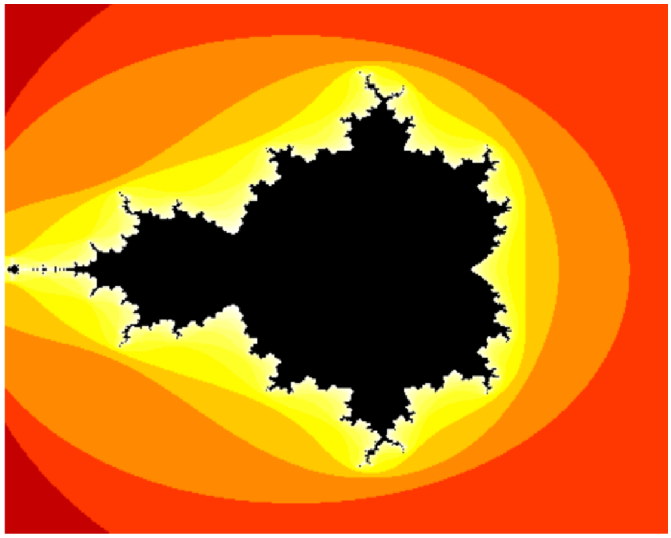
4.3 Exemples

En reproduisant les ensembles de Mandelbrot à des ordres différents grâce à l'algorithme précédent, on retrouve de nouveau des similiudes entre les figures comme ci-dessous:

mod : 91

n : 2

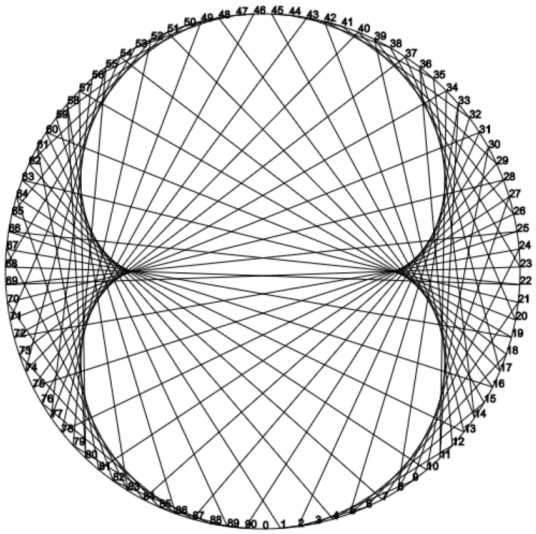


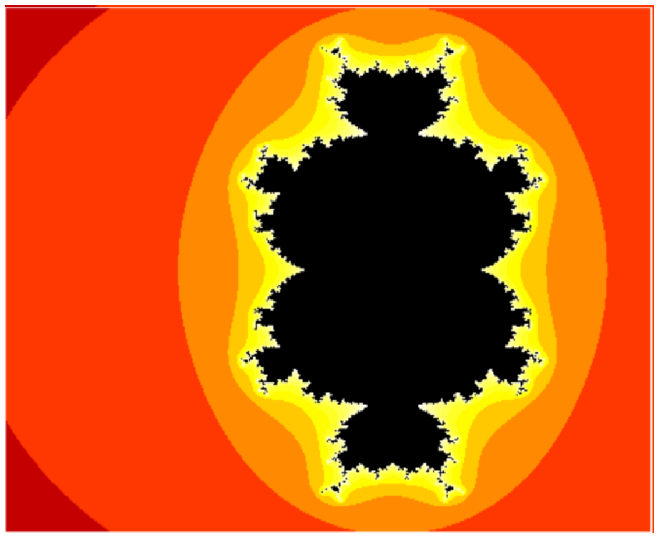


La table de 2 modulo 91, avec l'ensemble de Mandelbrot généralisé défini par $z_{n+1} = z_n^2 + c$.

mod : 91

n : 3

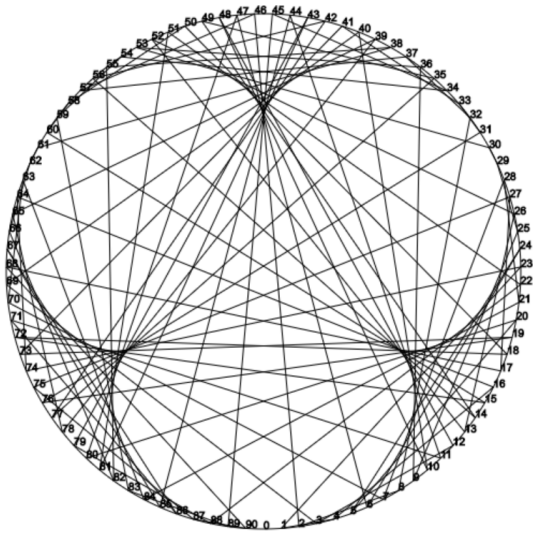


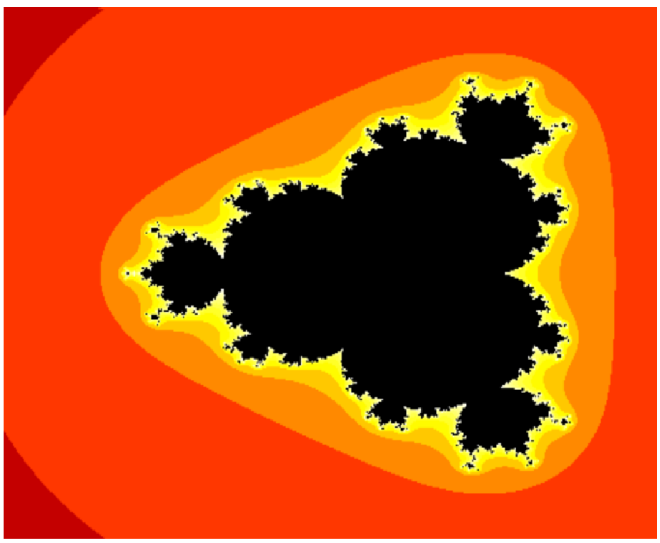


La table de 3 modulo 91, avec l'ensemble de Mandelbrot généralisé défini par $z_{n+1} = z_n^3 + c$.

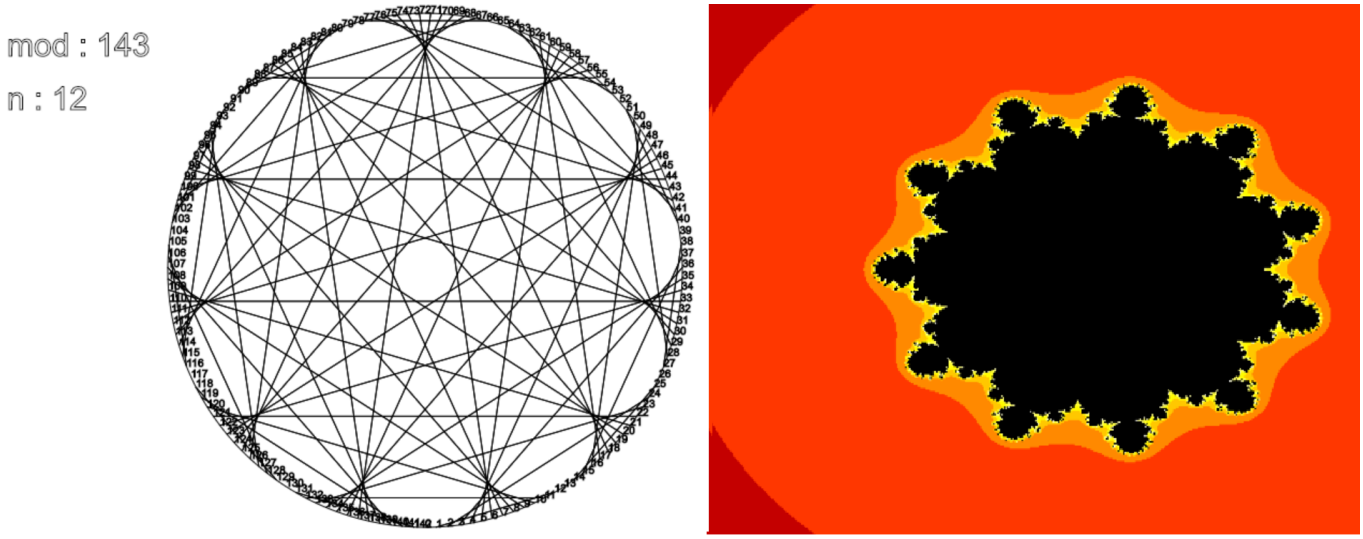
mod : 91

n : 4





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



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

Nous ne proposons aucune explication ; nous tenions seulement à faire remarquer cette coïncidence (si toutefois on peut parler de *coïncidence* en mathématiques).