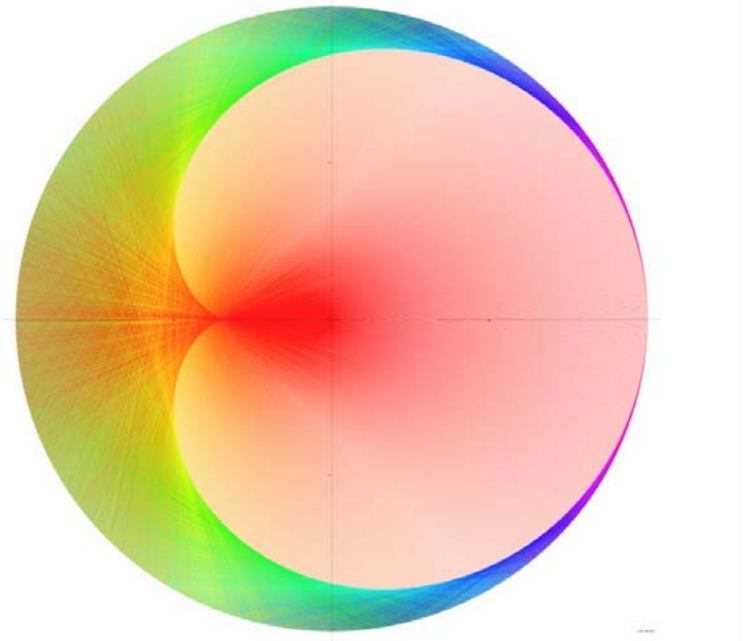
La forme de $b^n \ mod \ p$

Par Simon Plouffe

20 août 2020

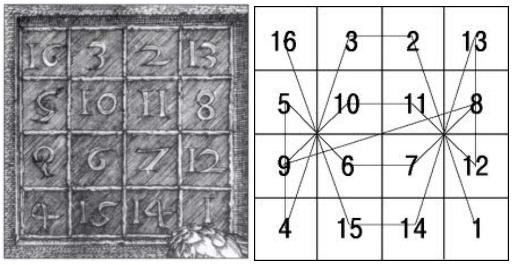


La cardioïde est en fait la représentation de l'inverse d'un nombre premier en base 2, la coloration des segments de droite est une aide pour visualiser : la couleur est proportionnelle à la longueur du segment (et c'est plus joli).

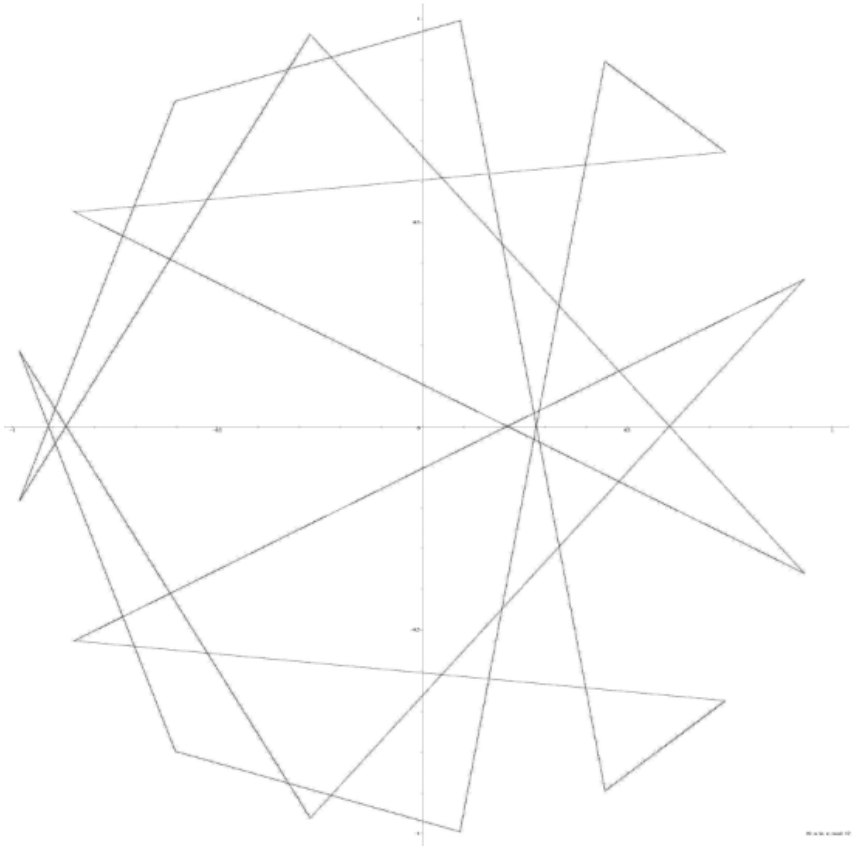
Résumé

Le présent article explore les formes que peuvent prendre les valeurs de $b^n \ mod \ p$ lorsque p est premier et b est la base. On nomme b la base pour la raison simple que ces valeurs sont la représentation de $1/p$ dans la base b. Pour visualiser ces valeurs, la façon naturelle de procéder que j'ai trouvé consiste à *enrouler* ces dernières sur le cercle en le subdivisant en $p-1$ parties. Il ne reste alors qu'à joindre ensemble les points ou valeurs successives. Une autre façon de voir ces valeurs est de considérer le développement décimal (dans la base b) de 1/p et de déplacer le point décimal vers la droite. L'une des figures connues de cette représentation est la cardioïde, elle représente 1/p en base 2. La chose intéressante est que si on utilise d'autres bases en faisant varier p on y découvre une foule de dessins étranges. L'article explique d'où viennent ces formes et donne une formule pour calculer à l'avance la forme que le dessin aura. L'article tente de répondre à une question simple : si la cardioïde représente l'inverse d'un nombre premier (sous certaines conditions) alors qu'en est-il des autres bases comme 10 ?

Le début de cette recherche remonte à 1974 où je cherchais à percer le mystère des carrés magiques. L'un en particulier était celui de Dürer bien connu.

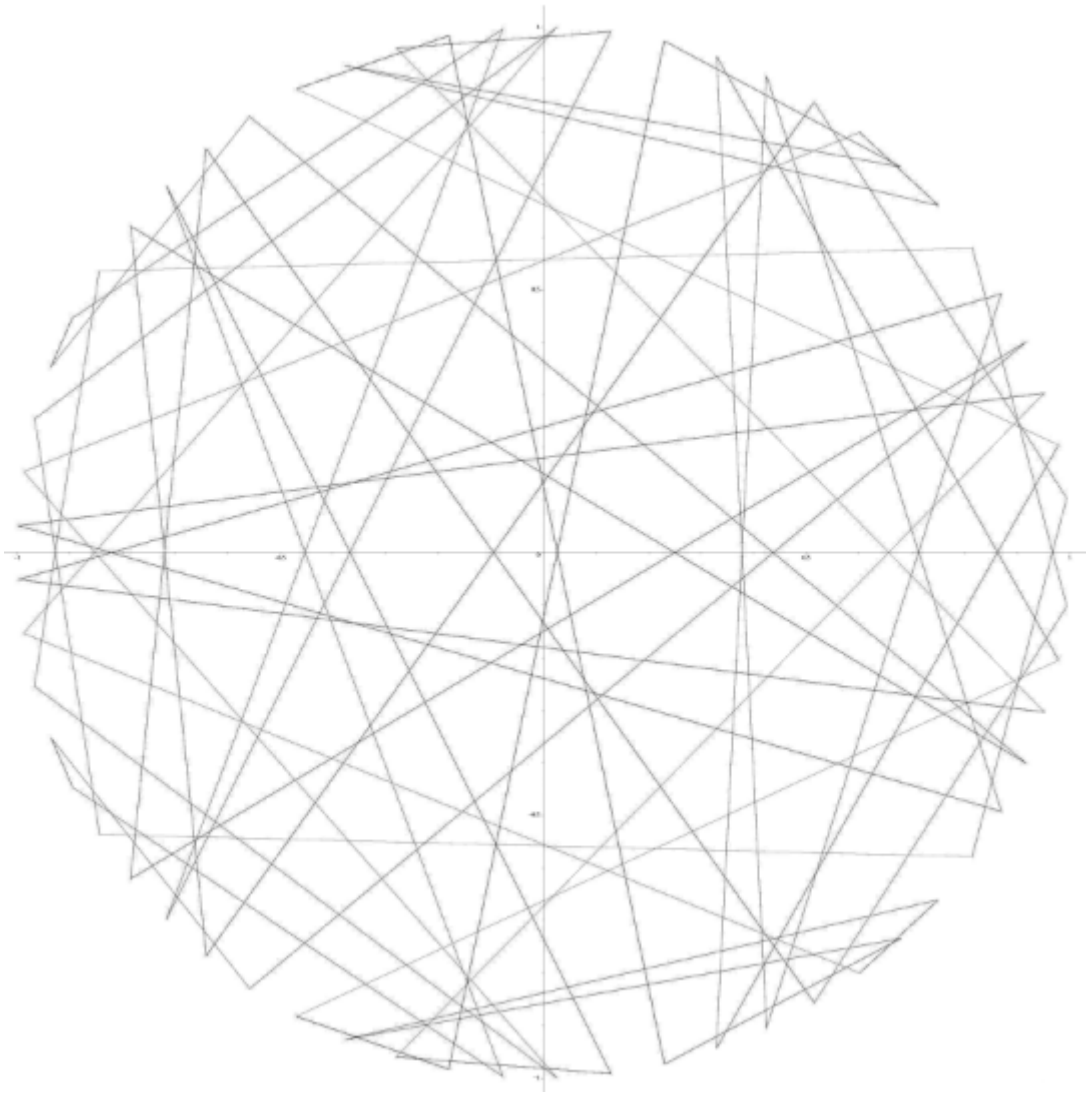


Si on relie les valeurs de 1 à 16 on y voit un motif symétrique intéressant. Mais ce qui me rendait perplexe sont les valeurs de 10^n mod 17. En fait, la suite des résidus de 10^n modulo 17 est presque magique. 1, 10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12, 1, … Ce sont les restes de la division des puissances de 10 avec 17, exactement comme la longue division qu'on apprend à l'école élémentaire. Je me demandais s'il n'y avait pas moyen de trouver une base et un nombre premier permettant de construire un carré magique sans se fatiguer puisque les valeurs de $b^n \ mod \ p$ sont faciles à calculer. C'est alors que j'eut l'idée de mettre ces valeurs sur le cercle de rayon 1 et de voir à quoi ça pouvait ressembler.



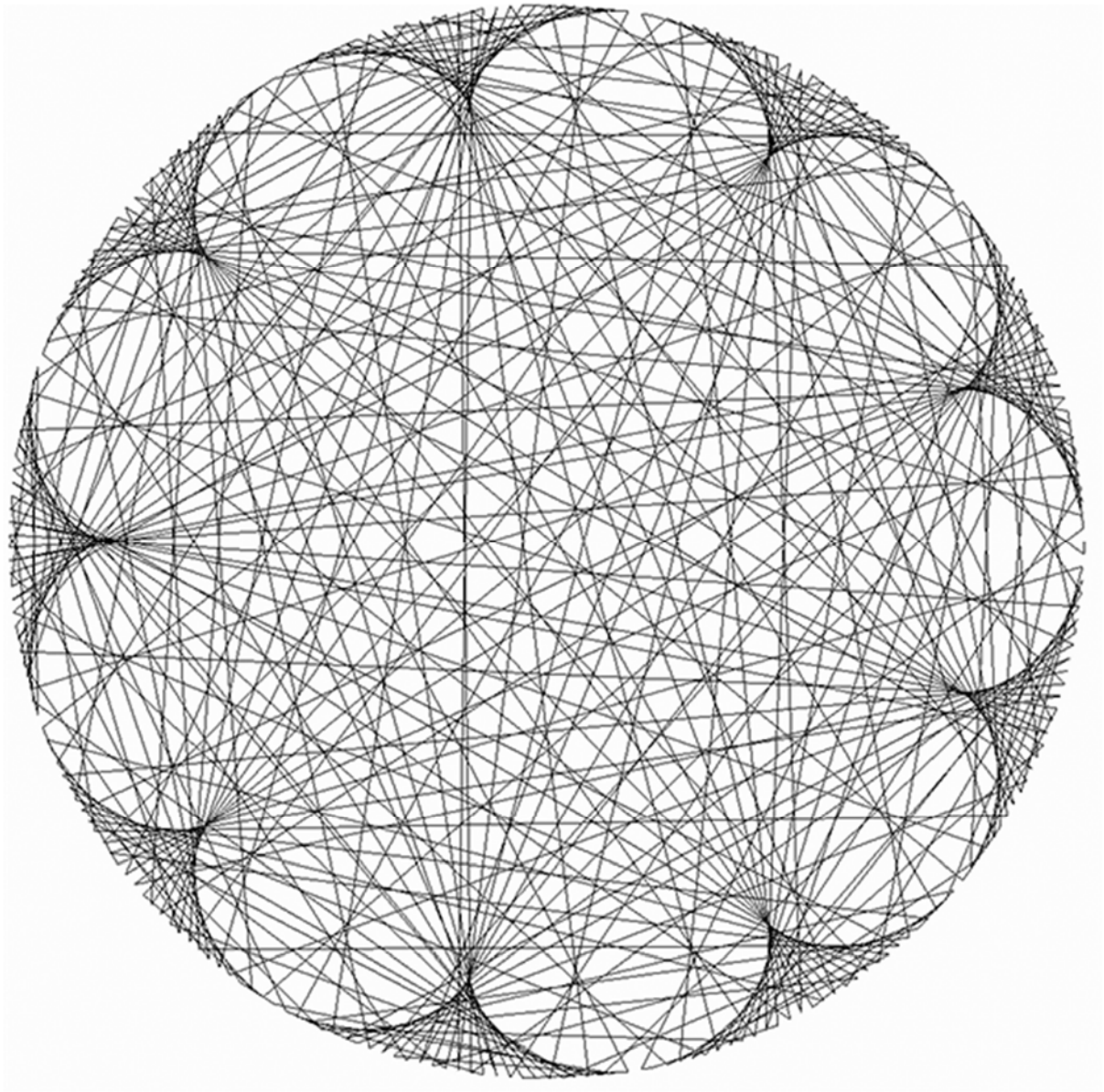
Les résidus de 10^n modulo 17 enroulés autour du cercle.

Ça ne donne pas un carré magique mais le dessin est symétrique. La prochaine étape alors fut de calculer $1/p$ en base 10 mais avec $p = 61$.



La même chose avec le nombre 61 en base 10.

Je calculai alors 1/257 en base 10 pour voir. Je pris ce premier parce que la subdivision du cercle en 256 parties est facilement réalisable à la main (règle est compas).



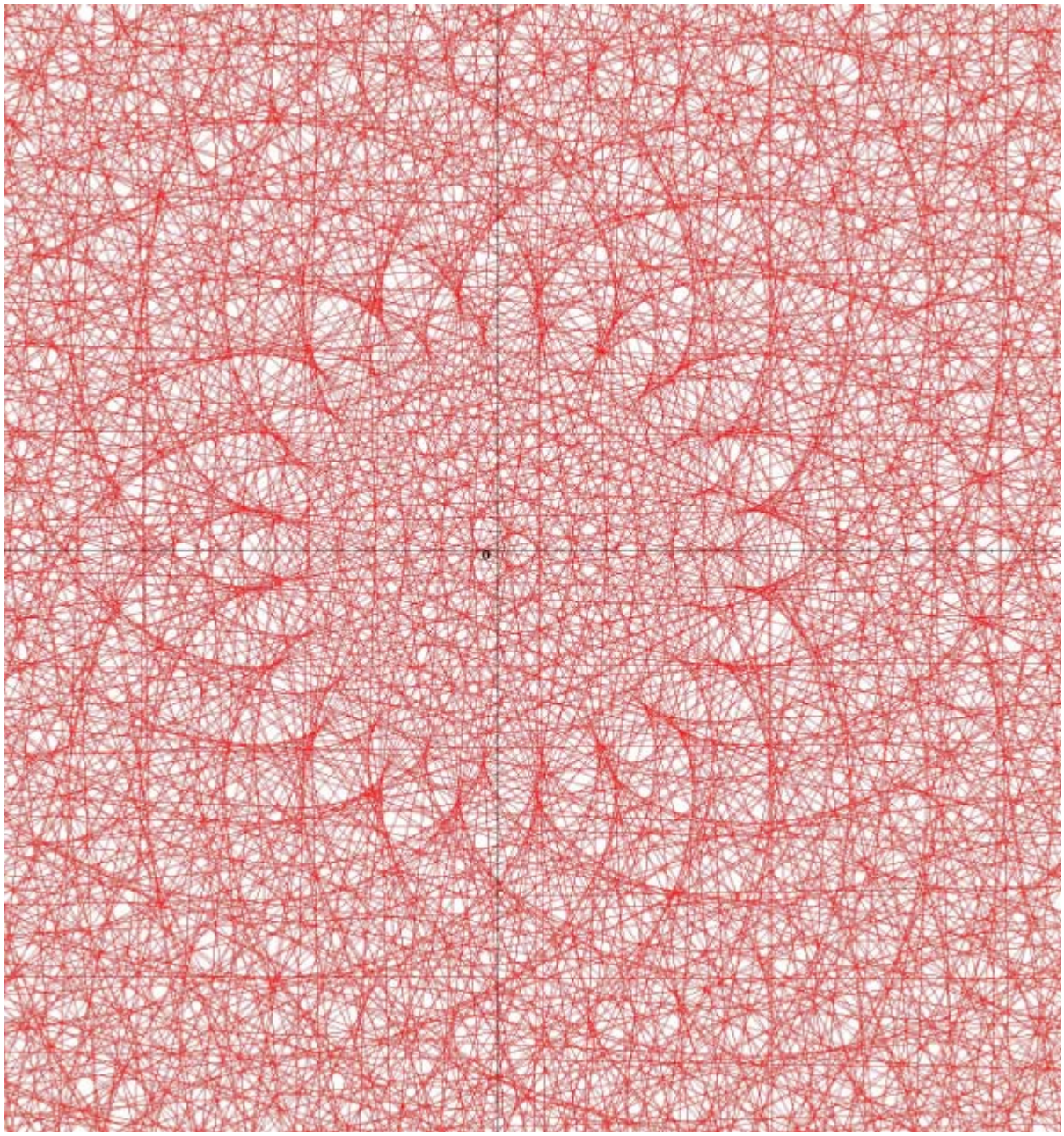
Représentation de 1/257 en base 10

On y distingue 9 pointes, ces 9 pointes s'expliquent par le choix de la base 10. Quelques soit le nombre premier, il y aura toujours $b-1$ pointes, en autant que p soit suffisamment grand pour que ce soit visible et que la base b soit une racine primitive de p. La racine primitive de p est telle qu'il y a $p-1$ résidus mod p. Une bonne question alors fut de compter combien il y a de pointes en tout. Ici on distingue 23 autres pointes, mais d'où viennent ces 23 pointes ? En répétant des expériences avec plusieurs premiers et bases j'arrivai à la formule pour le nombre de sous-pointes P_1 , P_0 étant $b-1$.

$$P_1 = (1-b)\left[\frac{p}{b}\right] - b + p + 1$$

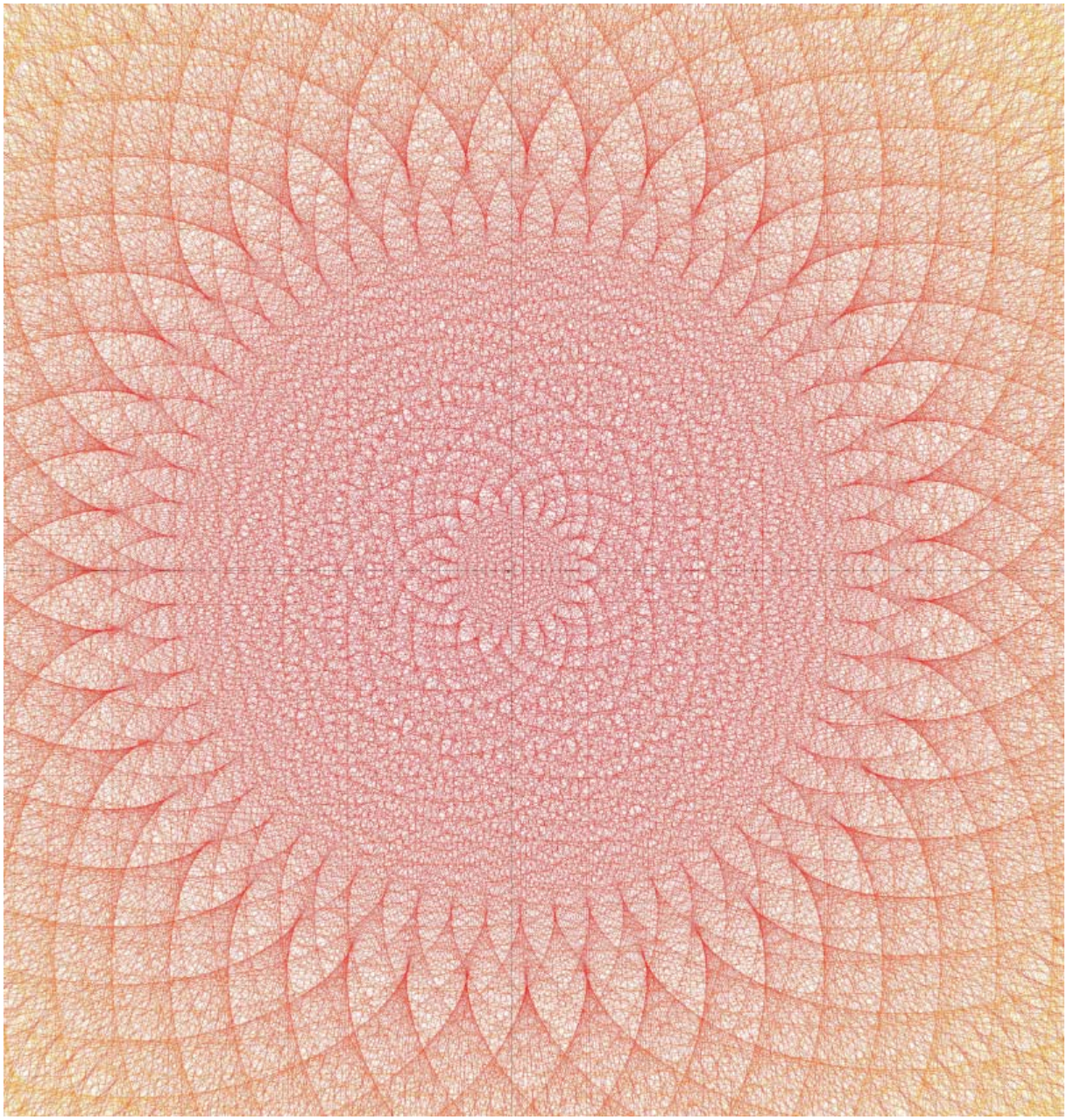
Ici, [ ] est la partie entière. Ça suffisait à l'époque (1979) pour expliquer quelques dessins mais pas tous. Plus tard, les moyens informatiques pour réaliser ces dessins me

permirent d'explorer bien plus loin les valeurs de p et de trouver d'autres groupes de pointes. Par exemple avec p = 10007 et b = 107 on obtient : vue près du centre du dessin.



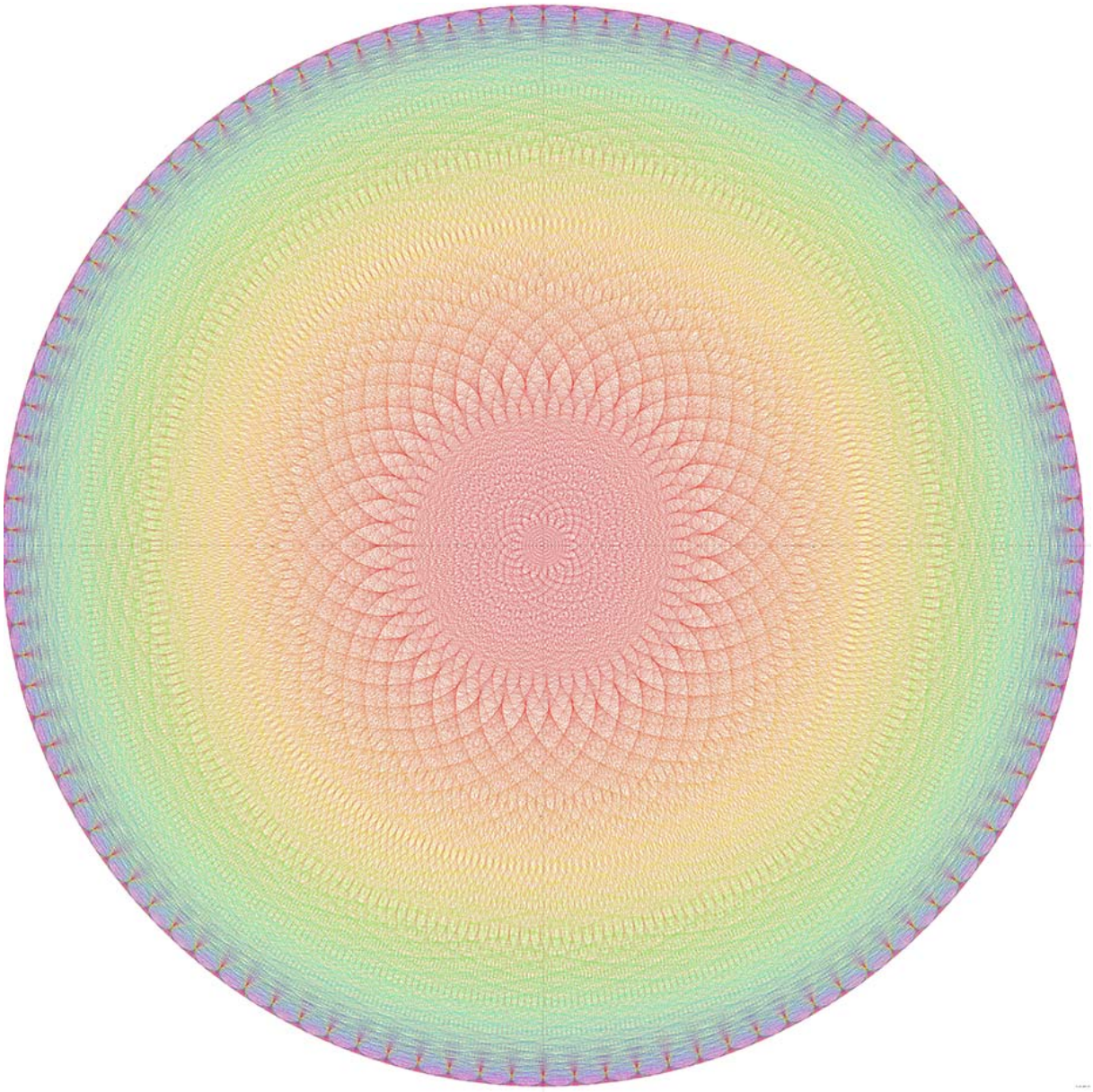
Zoom sur l'image de $107^n \ mod\ 10007$ (colorisée).

J'appelle groupe de pointes : l'ensemble des pics sur un même périmètre (à la même distance du centre du cercle). Ce n'est pas à proprement parler un groupe. On distingue 3 pointes au centre, suivies de 20 et 23 autres pointes. Un zoom à plus petite échelle révèle les 43 pointes calculées selon la formule ; $(1-b)\left[\frac{p}{b}\right]-b+p+1$. Il reste à trouver pourquoi on compte 20 et 23 pointes. Sur le dessin complet on distingue jusqu'à 8 couches de pointes.



En reculant on distingue les 43 pointes P_1, le dessin des droites est colorisé avec une couleur proportionnelle à la longueur, ce qui facilite la visualisation.

Ce qui semble se dégager est que les nombreuses séries de pointes sont générées à partir de $P_0 = b - 1$ et $P_1 = (1 - b)\left[\frac{p}{b}\right] - b + p + 1$ uniquement.

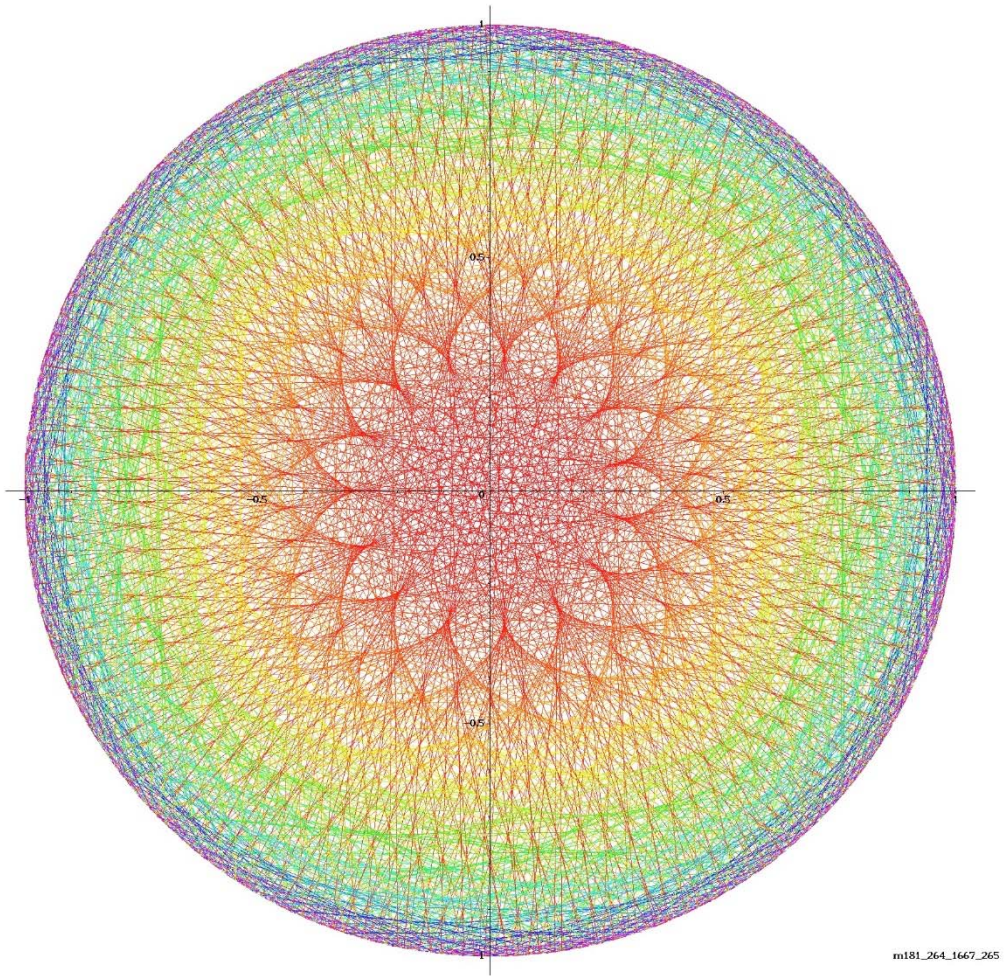


Dessin complet de $107^n \ mod\ 10007$

Les 2 quantités de P_0 et P_1 suffisent à expliquer tous les groupes ou ensembles de pointes. Il suffit de considérer les différences des multiples de P_0 et P_1, c'est-à-dire l'ensemble $E_{P_0} = \{ P_0, 2P_0, 3P_0, 4P_0, ...\}$ et l'ensemble $E_{P_1} = \{ P_1, 2P_1, 3P_1, 4P_1, ...\}$, les différences absolues entre les deux et de prendre la liste des plus petites valeurs. Il suffit d'avoir les 10 ou 20 premiers termes de ces 2 ensembles.

Dans notre cas, $P_0 = 106$ et $P_1 = 43$. Les ensembles sont :
$E_{P_0} = \{106, 212, 318, 424, 530, 636, 742, 848, 954, 1060, ...\}$ et
$E_{P_1} = \{43, 86, 129, 172, 215, 258, 301, 344, 387, 430, ...\}$ on procède alors à toutes les différences entre chaque paire d'éléments pour obtenir une liste croissante. Cette liste est la liste des groupes de pointes.

La liste finale est donc : {3, 6, 17, 20, 23, 26, 37, 40, 43, 100, 106 } en enlevant les multiples d'un même nombre la liste épurée devient : {3, 17, 20, 23, 26, 37, 40, 43, 106} . Les 2 nombres, $P_0 = 106$ et $P_1 = 43$ sont donc les générateurs des groupes de pointes qui apparaissent dans le dessin. Il faut comprendre aussi qu'il y a une limite à la précision et l'identification d'un groupe de pointes, elles ne sont pas forcément très visibles. Pour valider l'hypothèse à propos de P_0 et P_1, on prend un échantillon de premiers et de bases. Pour simplifier le problème nous choisirons des bases qui sont racines primitives de p.



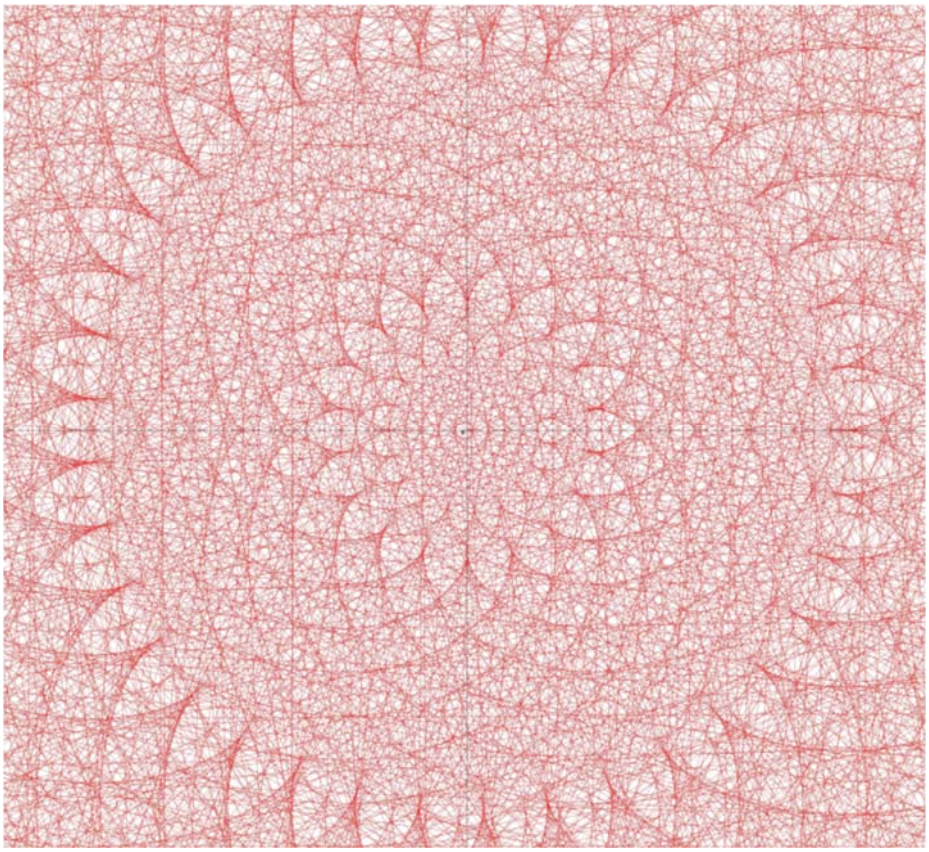
Avec $265^n \ mod\ 1667$ les valeurs de $P_0 = 264$ et $P_1 = 181$

Après calcul on a les nombres {15, 23, 38, 53, 68, 83, 98, 113, 128, 136, 151, 166, 181}. On arrive à compter un groupe de 15 pointes et un groupe de 38 faciles à compter. Bien moins visible est le groupe de 23 pointes plus au centre. Selon le principe établi on doit avoir 264 pointes sur le pourtour du cercle et 181 pointes secondaires (P_1), elles se trouveraient un peu plus loin sur le pourtour. On atteint la limite de visibilité mais ça semble bien fonctionner. Les 181 pointes sont trop confuses pour être comptées correctement.

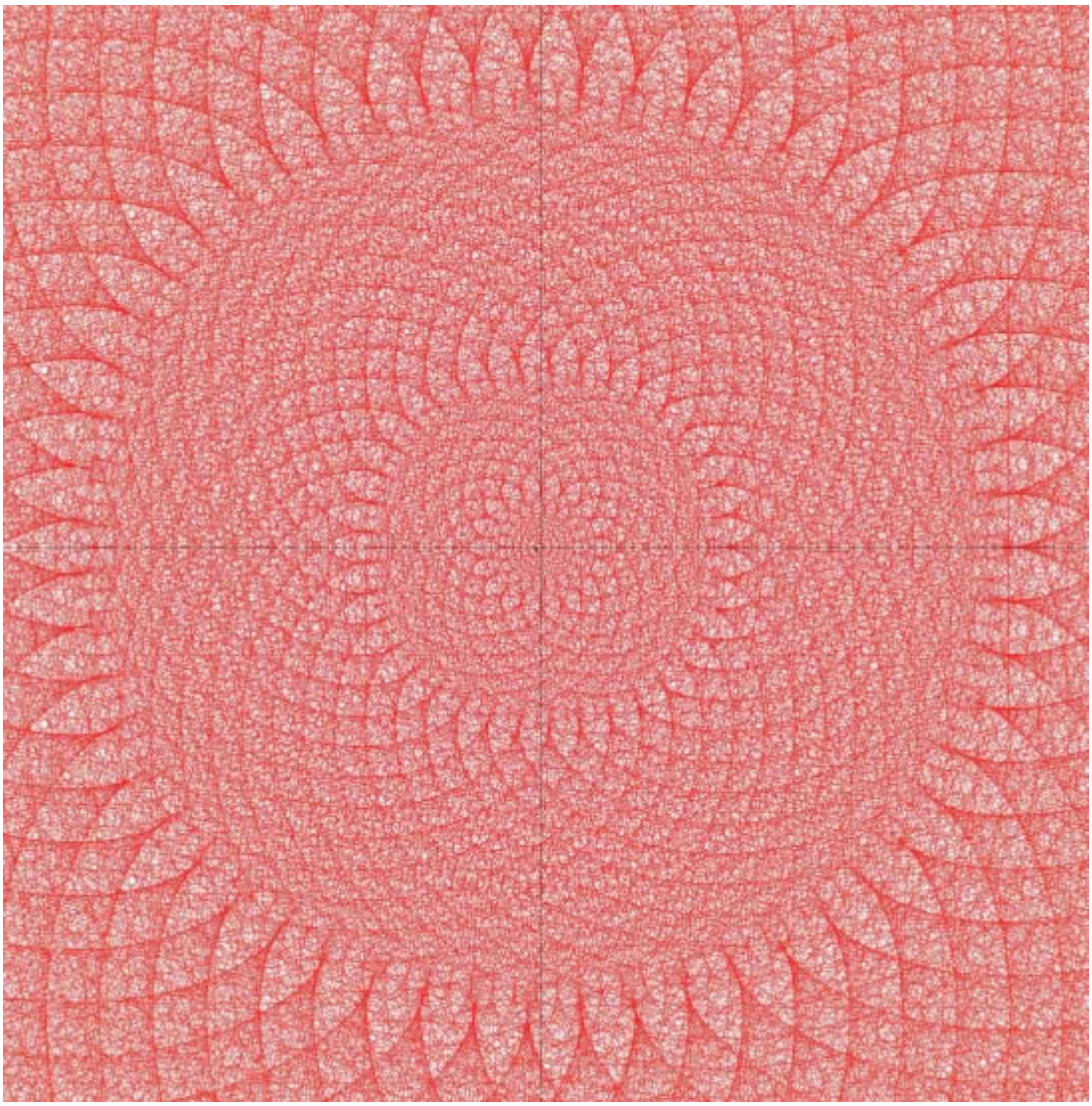
Il y a quand même une limite mécanique à représenter ces graphes sur ordinateur. La limite est le nombre de droites simultanées sur un même dessin. Avec p = 65537 par exemple le centre du dessin est indéchiffrable. Même avec une image de 32768 × 32768 (plus de 1 milliard de pixels), c'est trop pour une seule image. Je pourrais tenter la construction avec une image bien plus grande en format brut (RAW) mais ça devient ingérable même prises individuellement avec Photoshop. Sur un seul dessin, la limite est à peu près p autour de 100 000.

J'ai donc choisi un nombre premier assez grand (10037) pour voir toutes les harmoniques de ces étranges dessins. Il y a 4606 racines primitives de 10037. Dit autrement, le nombre premier 1/10037 exprimé par les 4606 bases différentes génère les dessins (voir plus loin et le site web). Également, j'ai exploré tous les nombres premiers jusqu'à 100000 avec la base 240. L'hypothèse que P_0 *et* P_1 sont suffisants pour expliquer toutes les 'harmoniques' est validée puisque si on prend des premiers tels que $P_0 = 92$ et $P_1 = 239$ par exemple on obtient bien le même dessin avec les harmoniques calculées avec la formule. Selon le calcul on devrait avoir des ensembles de pointes suivants : 1, 17, 18, 19, 20, 35, 36, 37, 38, 54, 55, 56, 57, 72,… Si on teste avec de grands nombres premiers on vérifie que le dessin est bel et bien le même et qu'on aperçoit de plus en plus d'harmoniques qui sont exactement celles qui ont été calculées à l'avance :

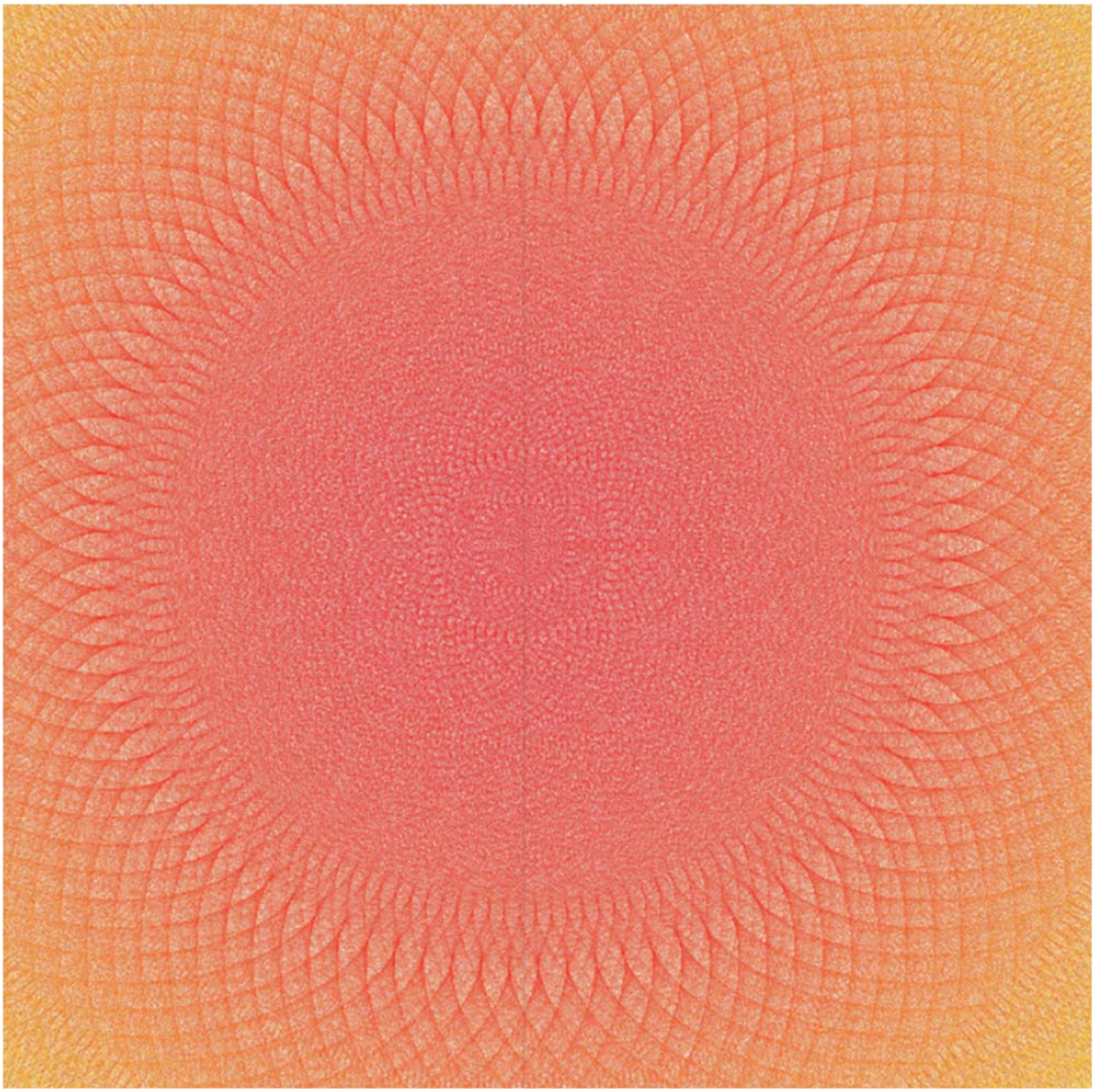
Ici avec p = 14009, on obtient bien $P_0 = 92$ et $P_1 = 239$ et le centre de l'énorme dessin de 1 milliard de pixels nous donne : Une pointe au centre 18 et 19 pointes.

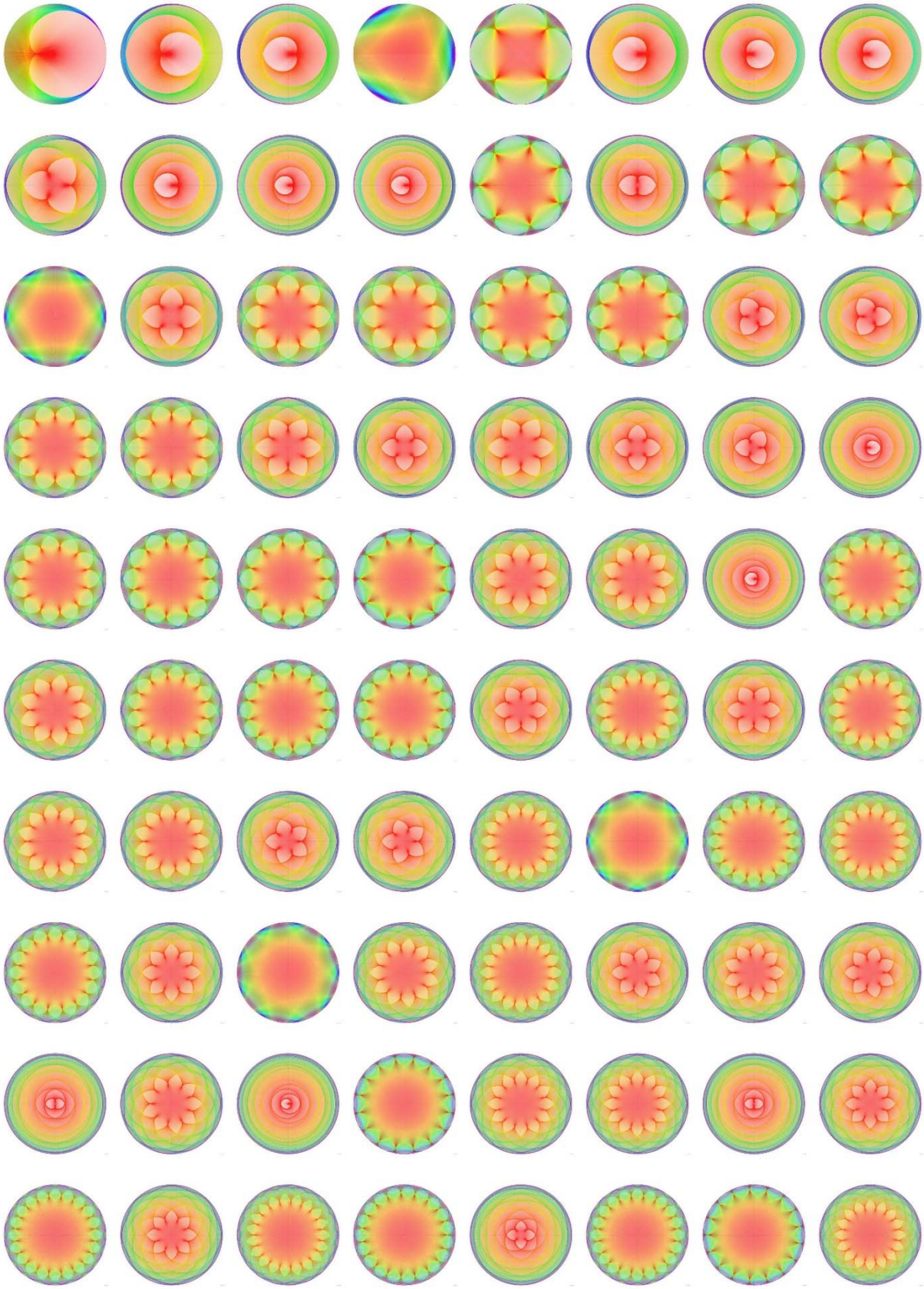


Avec un autre dessin effectué avec le premier = 32173 on a bien 55 pointes.
Plus le nombre premier est grand, plus le nombre d'ensembles grandit et le nombre de pointes de chaque ensemble est bel et bien dans la liste calculée à l'avance.



Un dernier dessin avec le premier 45263 en base 240
Si on compte correctement on y dénombre 92 pointes sur le périmètre :
Il est bien dans la liste [1, 17, 18, 19, 20, 35, 36, 37, 38, 54, 55, 56, 57, 72, 73, 74, 75, 91, 92, 182, 239]



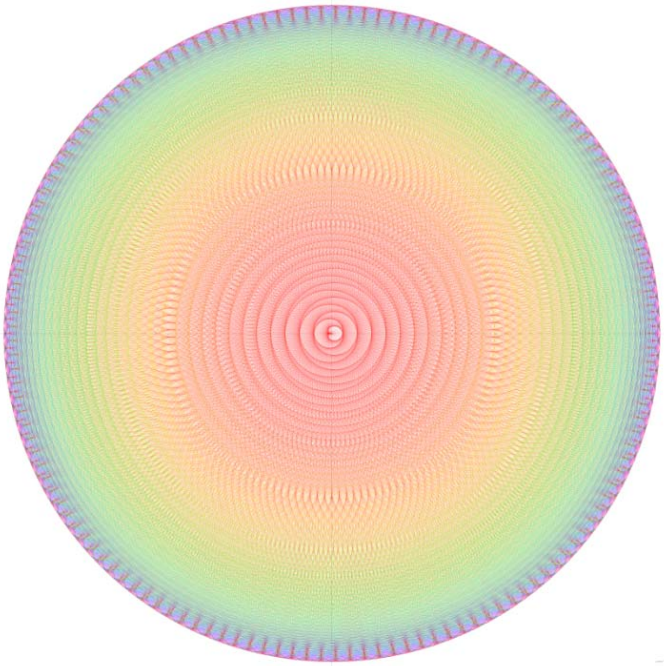


Les 80 premières images de b^n mod 10037

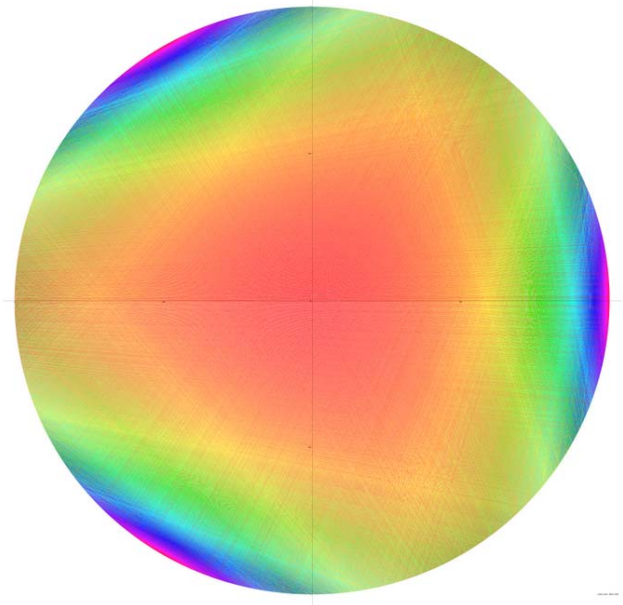
Toutes les autres images sont ici : http ://plouffe.fr/10037

On en déduit les règles suivantes.

1- Si $P_1 = 1$, le nombre de tours sera proportionnel à p/P_0, par exemple avec 140^n mod 10009, on a $10009/139$ aura 72 couches.

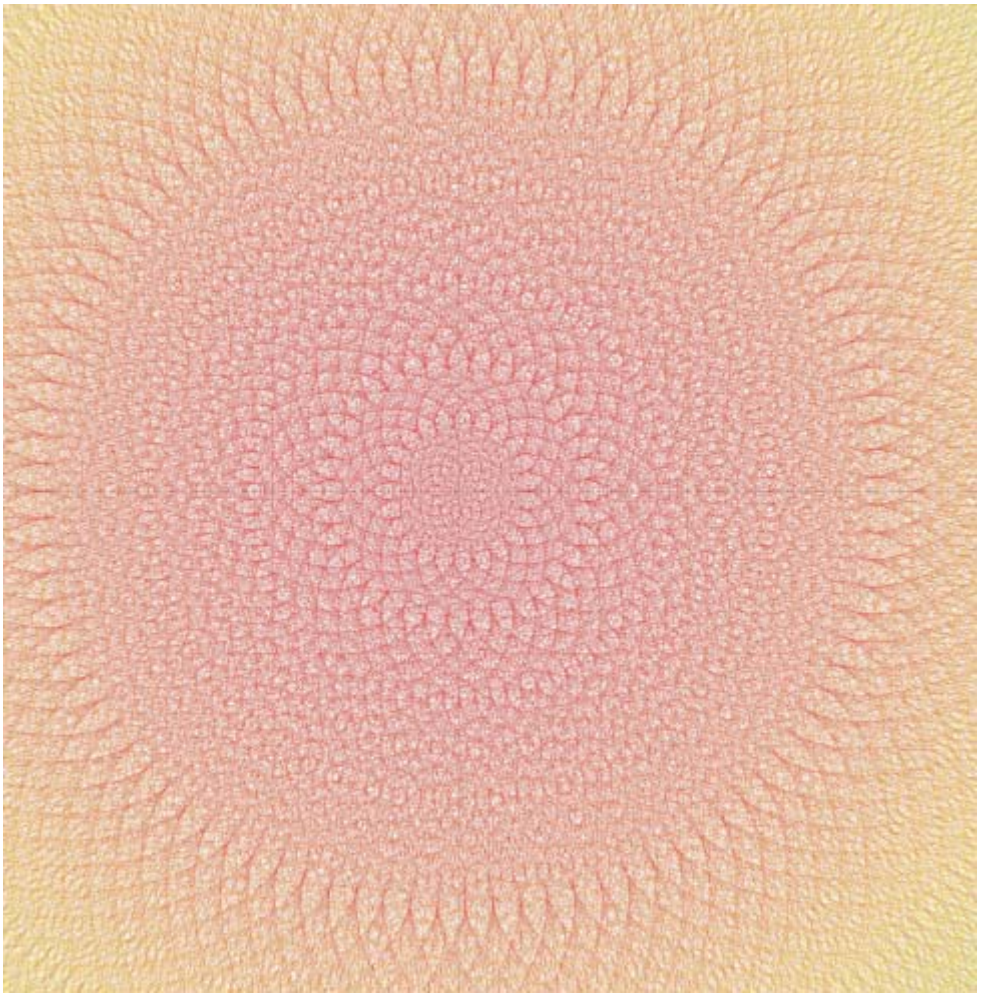


2- Si $P_1 \approx P_0$ les pointes seront seulement visibles comme un ombre à l'extérieur et le nombre de pointes externes sera $|P_1 - P_0|$, comme ici avec 5018^n mod 10037 nous donne P_0=5017 et P_1=5014 , on a bien 3 pointes diffuses.



3- Plus la base est grande plus le dessin sera riche en harmoniques. En prenant la base = 2 on obtient toujours une cardioïde et si p augmente la richesse du dessin

est la même mais plus précise, il n'y a pas d'harmoniques complexes. Si la base est 60 par exemple, déjà au centre on voit plein d'harmoniques, dans certains dessins on compte jusqu'à 10 groupes différents de pointes.

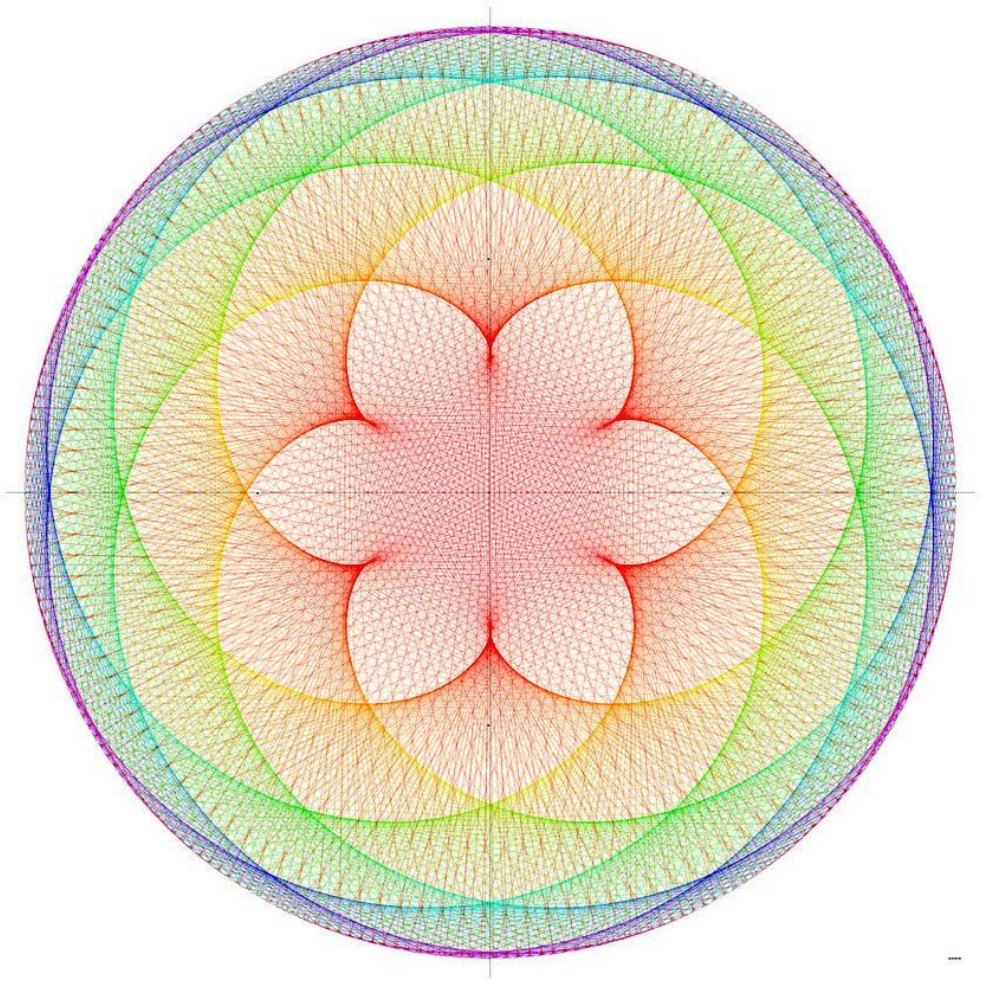


Ici avec $60^n \bmod 10007$

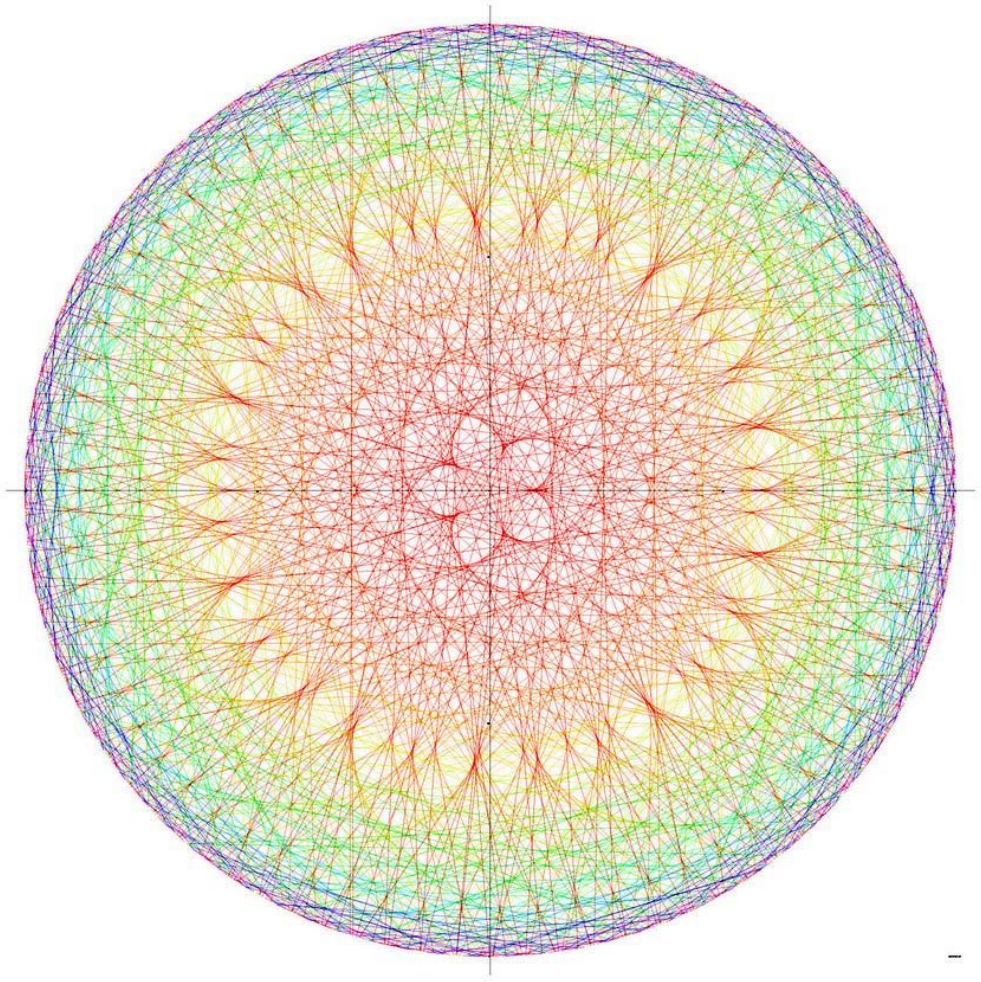
4- Les groupes de pointes ne sont pas des sous-groupes du groupe cyclique pour une bonne raison. Les pointes sont regroupées sur un même périmètre en paquets à peu près égaux. Si on parlait de groupe et de sous-groupe on aurait un nombre précis d'éléments, ce n'est pas le cas. Par exemple, $63^n \bmod 10037$ a en son centre 7 pointes distinctes qui contiennent environ 1433 droites chacune, étant donné que $10036 = 4 \cdot 13 \cdot 193$ ce sera forcément le cas la plupart du temps. Les harmoniques dans ce cas sont : 7, 8, 13, 14, 15, 20, 21, 22, 27, 28… .

J’ai donc choisi la base 240 pour avoir un maximum d’effets et avec une taille de graphiques allant jusqu’à 32768 × 32768, ce qui représente plus de 1 milliard de pixels.

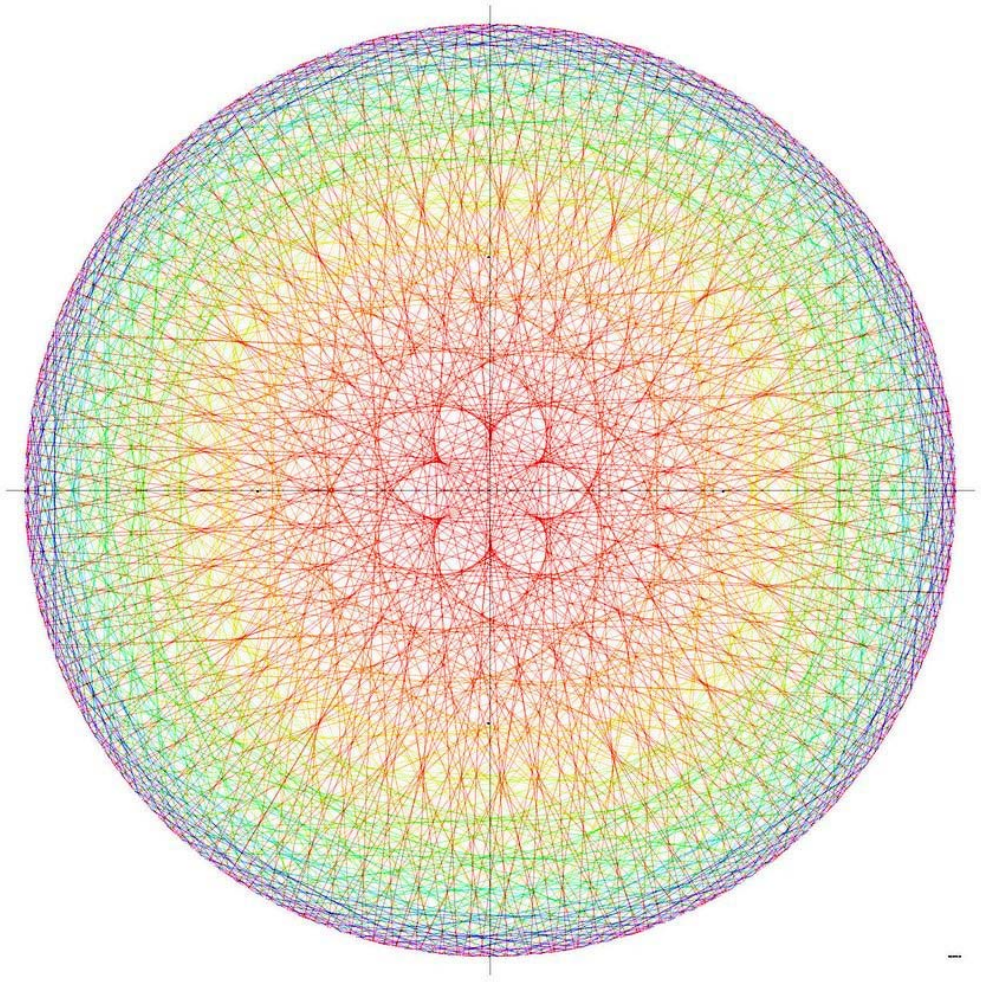
Voici les quelques cas de figures faites avec la base 240 pour certains nombres premiers.



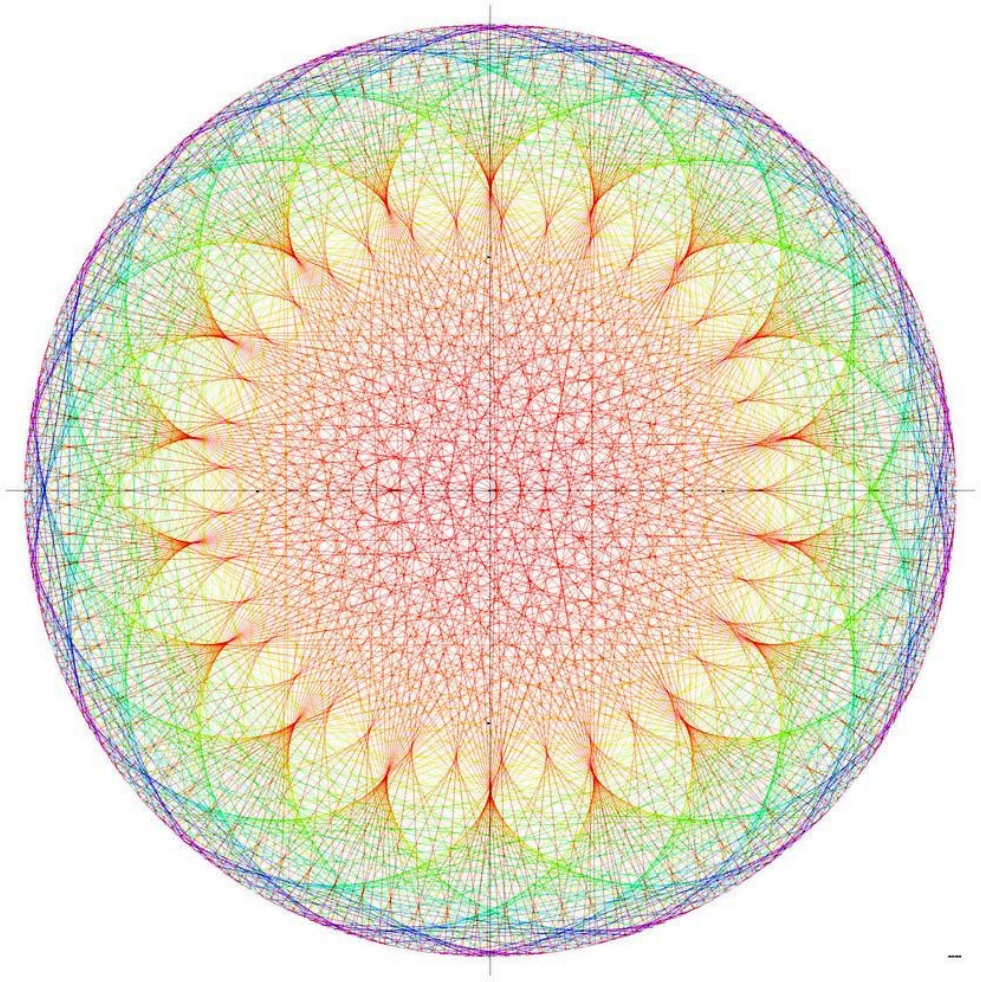
Simon Plouffe 2020: base = 240 , prime = 1667, P1 = 6, harmonics = 6, 95



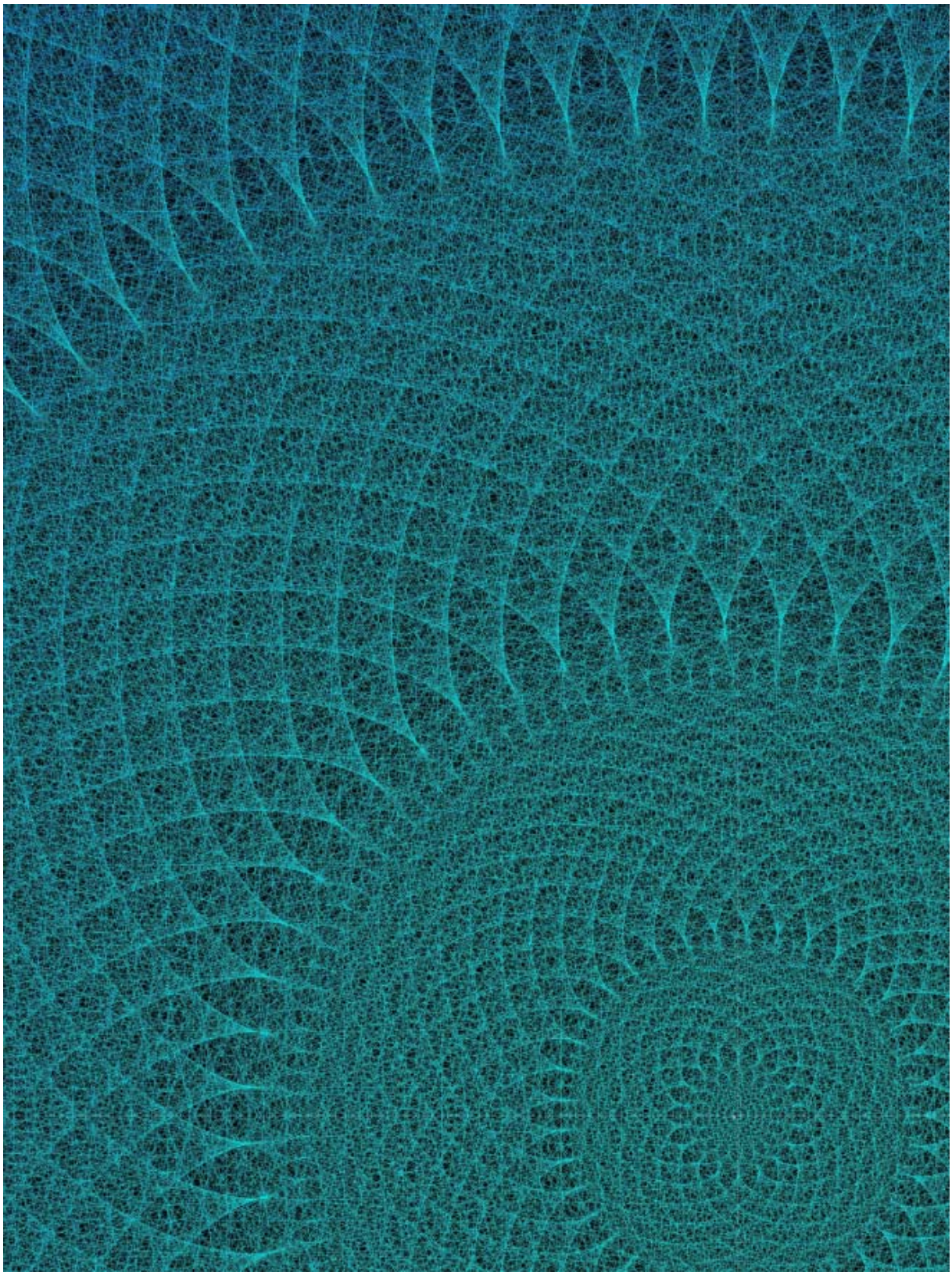
Simon Plouffe 2020: base = 240 , prime = 887, P1 = 69, harmonics = 5, 10, 15, 17, 22, 27, 32, 37, 42,



Simon Plouffe 2020: base = 240 , prime = 991, P1 = 204, harmonics = 6, 12, 17, 18, 23, 29, 35, 41, 47,



Simon Plouffe 2020: base = 240 , prime = 1103, P1 = 92, harmonics = 1, 17, 18, 19, 20, 35, 36, 37, 38,



Près du centre de 240^n mod 26437 en couleurs inversées pour une meilleure visibilité
$P_0 = 239, P_1 = 92$
Le nombre de pointes sont parmil la liste des harmonique: 1, 17, 18, 19, 20, 35, 37, 54, 55, 56, 57, 72, 73, 74, 75, 91, 92

Bibliographie :

[1] Plouffe, Simon , *the reflection of light rays in a cup of coffee,* Notes de 1995. https://vixra.org/pdf/1409.0045v1.pdf

[2] Animation avec une base variable, https://www.youtube.com/watch?v=13be44CqrrI

[3] Multiplication Tables : https://www.youtube.com/watch?v=qhbuKbxJsk8

[4] Plouffe, Simon, Films sur les congruences enroulées sur un cercle : https://www.youtube.com/results?search_query=plouffe314

[5] Plouffe, Simon, Formes générées avec le premier 1229

https://www.youtube.com/watch?v=cQU_E3jsDYw

[6] Plouffe, Simon, expérience à grande échelle avec la base 240 : http://plouffe.fr/premiers%20base%20240C/

[7] Plouffe, Simon, expériences avec le premier 10037

http://plouffe.fr/10037/