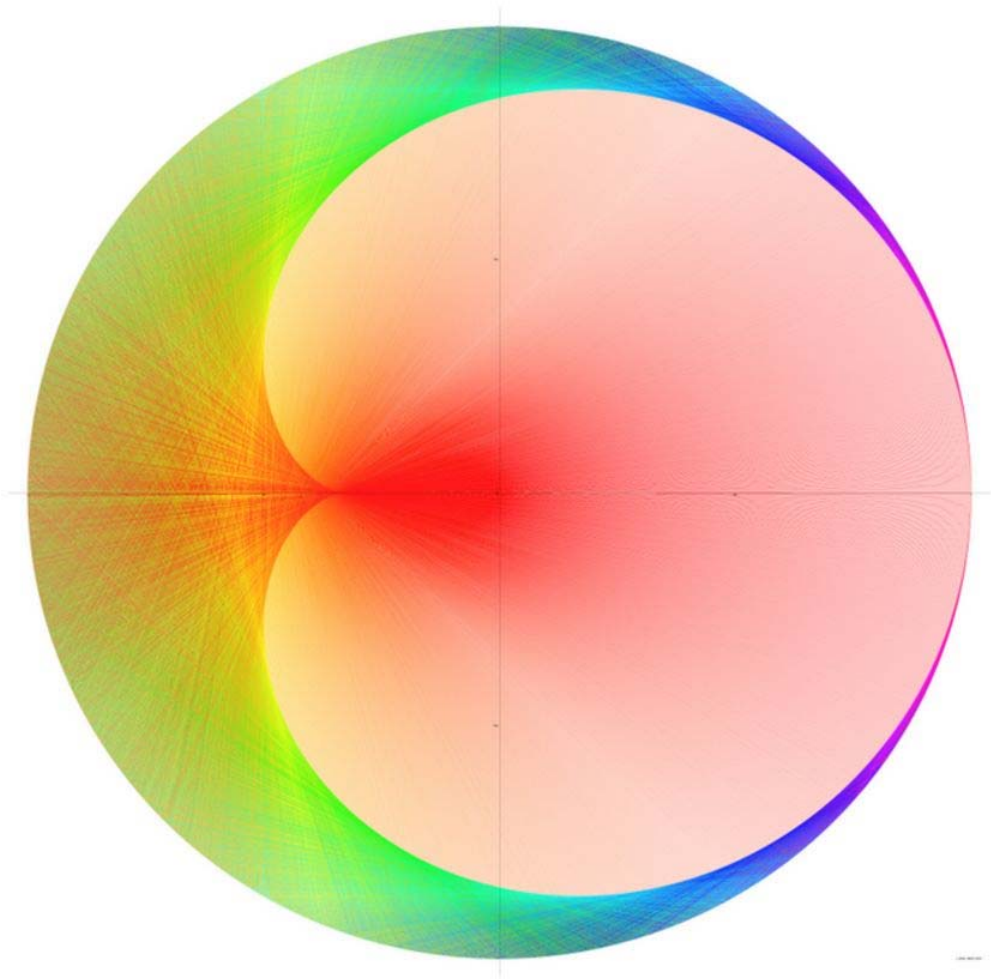
The shape of $b^n \ mod \ p$

By Simon Plouffe
August 26, 2020

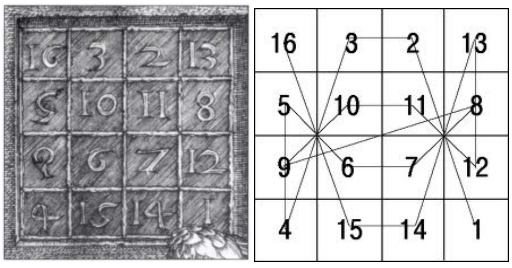
Abstract

This article explores the forms that the values of $1/p$ when p is prime and b is the base. We call b the base for the simple reason that these values are the representation of 1/p in the base of b. To visualize these values, the natural way that I have found is to wrap these on the circle, subdividing it into $p-1$ parts. It only remains to join together successive points or values. Another way to look at these values is to look at decimal expansion of 1 / p in that base and move the decimal point to the right. One of the known figures of this representation is the cardioid, it represents 1 / p in base 2. The interesting thing is that if we use other bases by varying p we discover a host of strange designs. The article explains where come these shapes and give a formula to calculate in advance what shape the drawing will have. The article tries to answer a simple question: if the cardioid represents the inverse of a prime number under some conditions then what about other bases like 10?

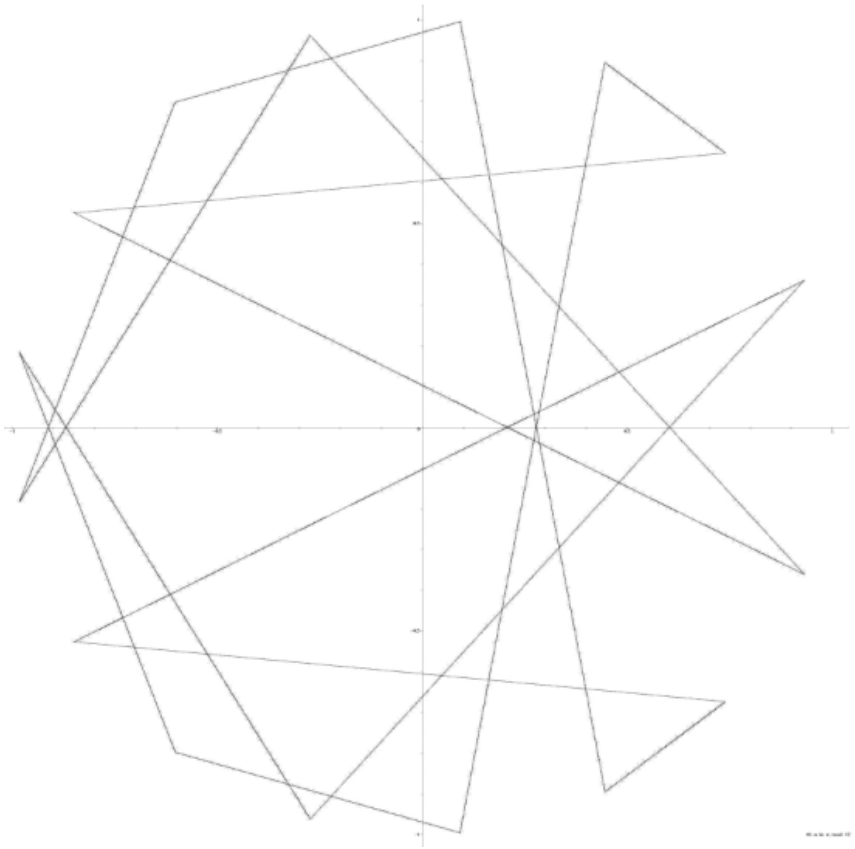


The cardioid is in fact the representation of the inverse of a prime number in base 2, the coloring of line segments is an aid to visualize: the color is proportional to the length of the segment and it looks better.

The beginning of this research goes back to 1974 when I was looking to unravel the mystery of magic squares.

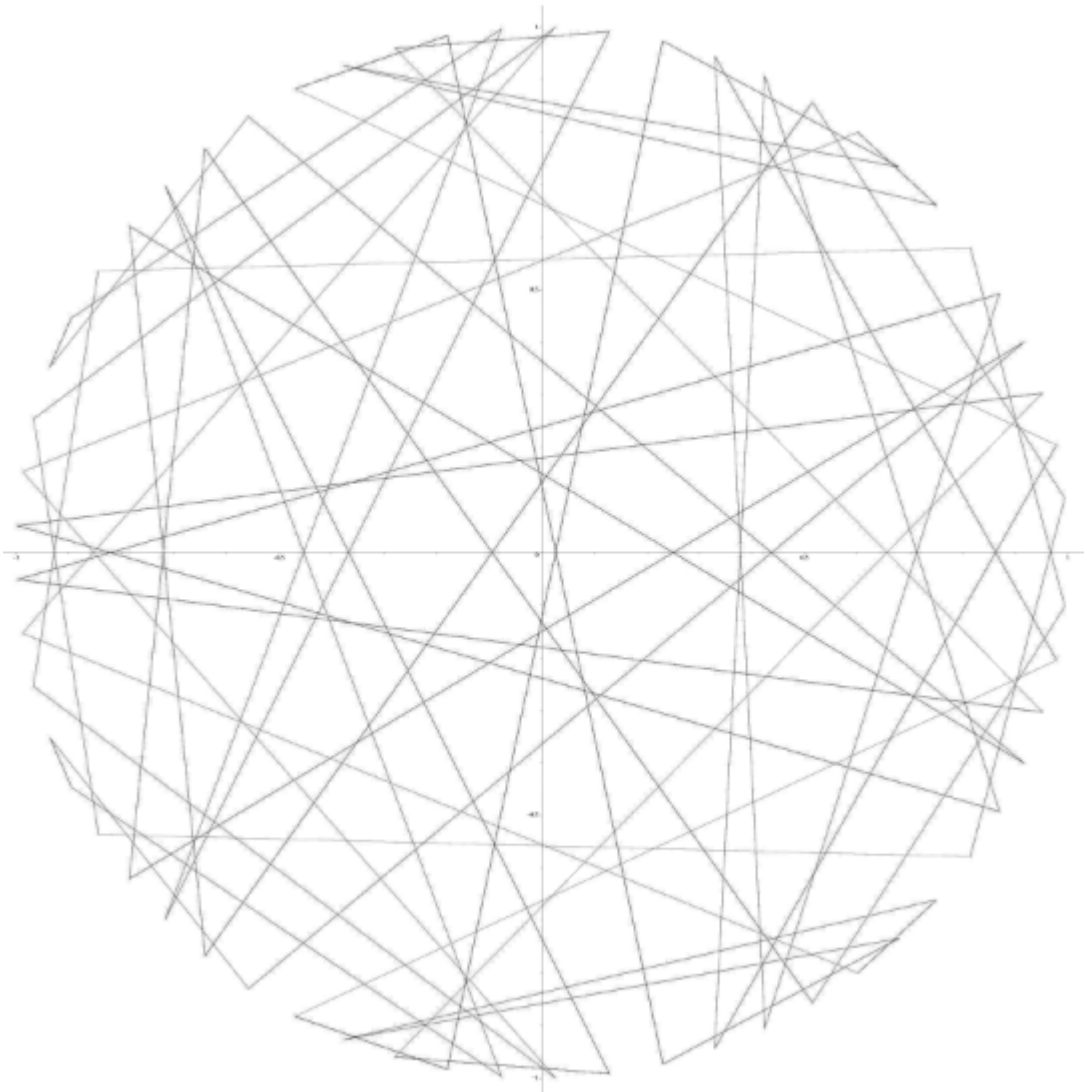


One in particular is the 4×4 magic square of Dürer. If we connect the values from 1 to 16 we see an interesting symmetrical pattern. But which puzzled me are the values of 10^n mod 17. In fact, the following residues of 10 modulo 17 is almost magic. 1, 10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12, 1,… These are the remainder of dividing the powers of 10 with 17, exactly like the long division that we learn in elementary school. I was wondering if there was no way to find a base and a prime number allowing to build a magic square without effort since the values of are easy to calculate. It was then that I had the idea of putting those values on the circle of radius 1 and seeing what it might look like.



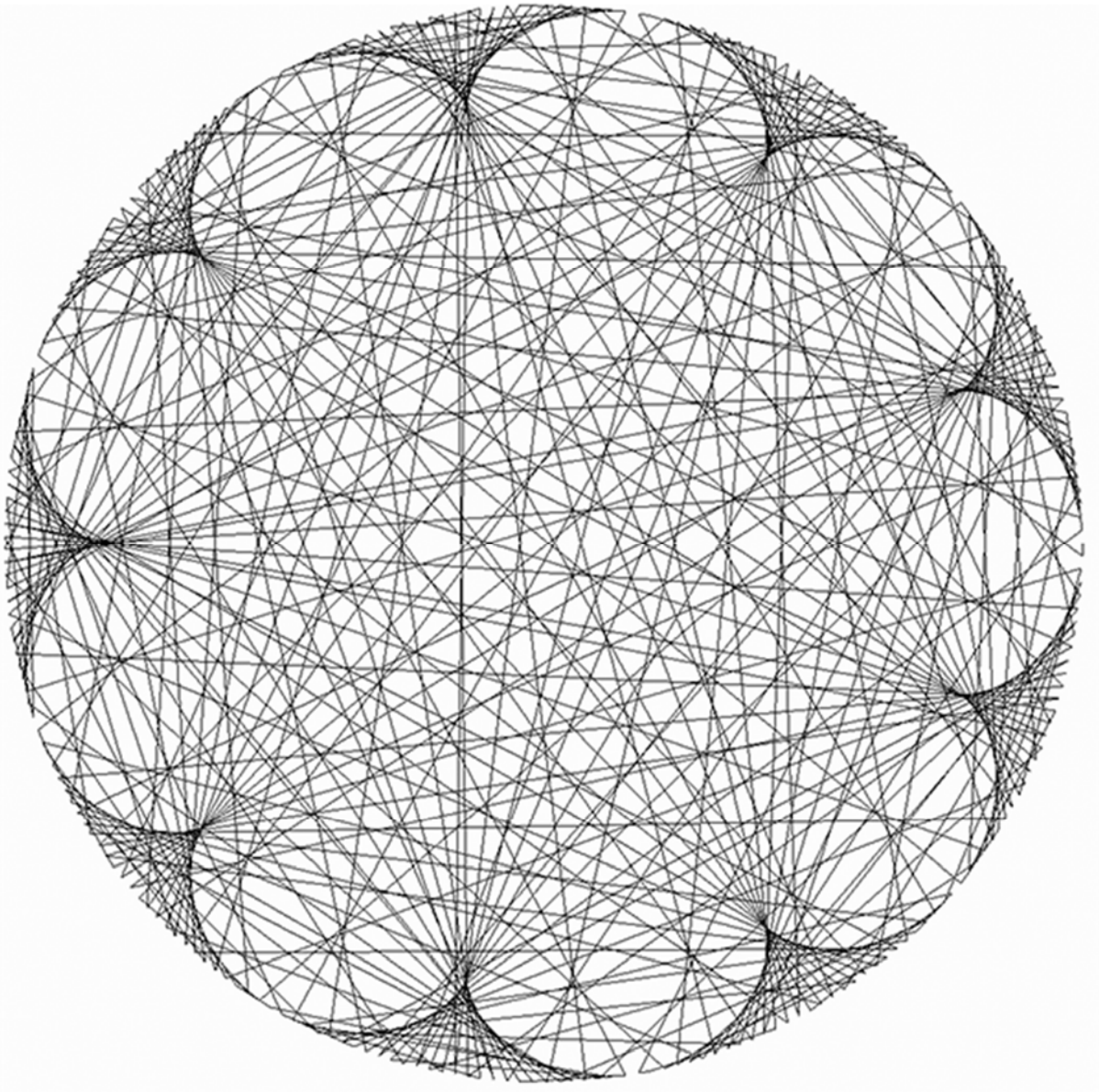
The residues of 10 modulo 17 wrapped around the circle.

It does not give a magic square but the drawing is symmetrical. The next step then was to calculate 1 / in base 10 but with 61.



The same thing with the number 61 in base 10.

I then calculated 1/257 in base 10 to see. I took this first because the subdivision of the circle into 256 parts is easily done by hand ruler is compass.

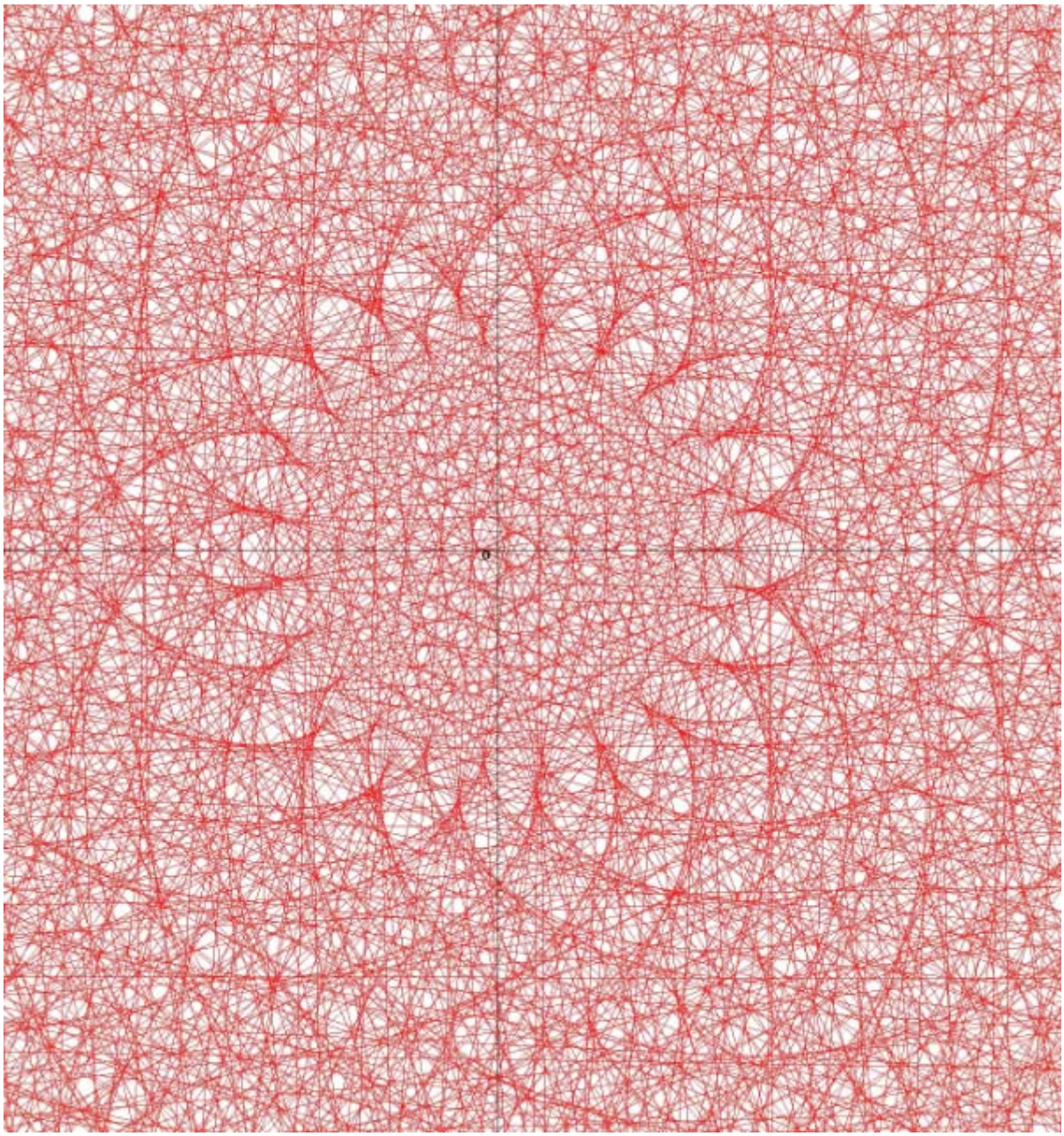


Representation of $1/257$ in base 10

There are 9 spikes, these 9 spikes can be explained by the choice of the base 10. Whatever the prime number may be, there will always be $(base - 1)$ spikes, as long as p is large enough so that it is visible and that the base b is a primitive root of p. The primitive root of p is such that there are $p - 1$ residues mod p. A good question then was to count how many spikes there are in all. Here we can see 23 other spikes, but where do these 23 points come from? By repeating experiments with several prime and bases I arrived at the formula for the number of sub-spikes P_1 , P_0 being $b - 1$.

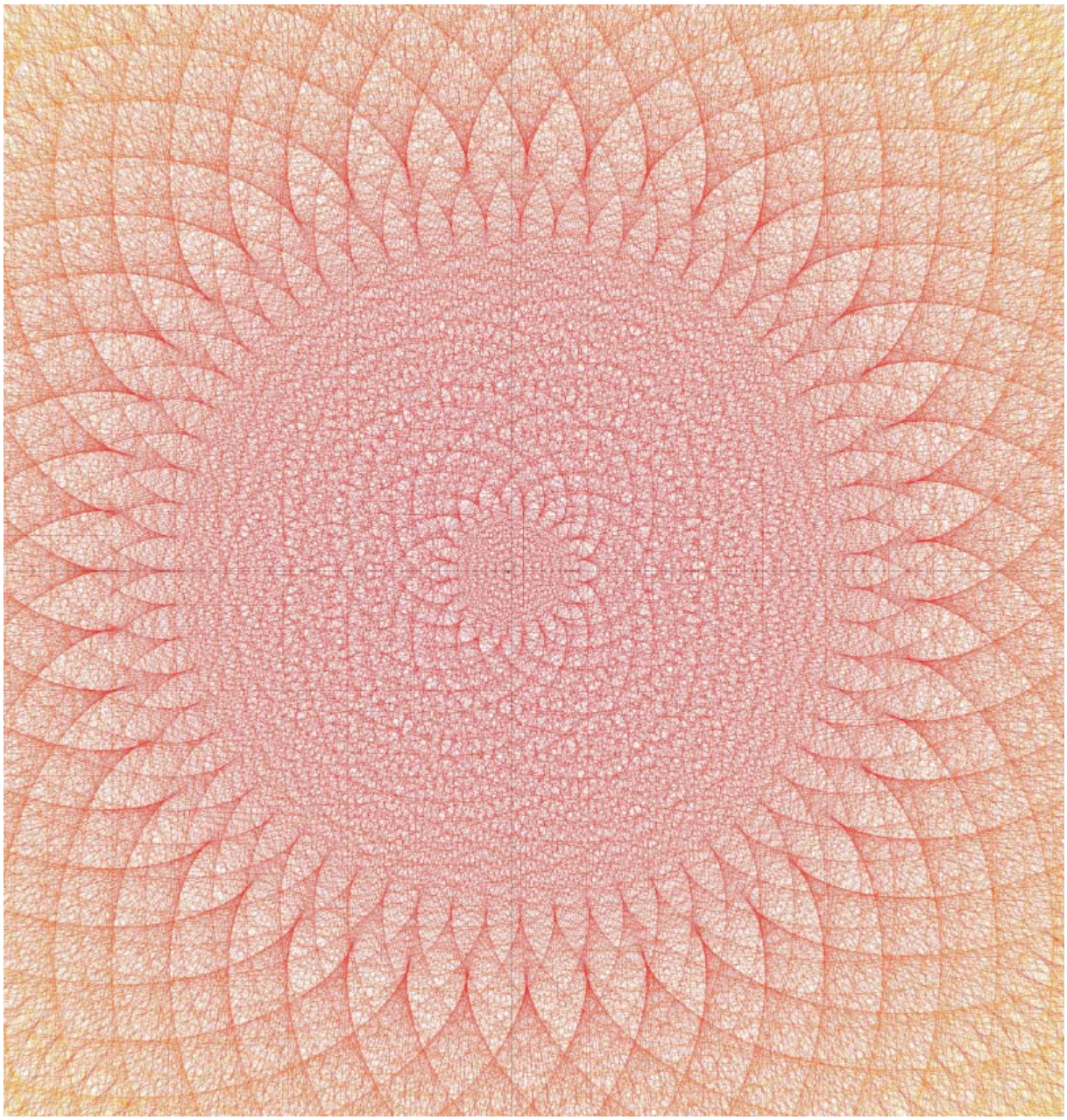
$$P_1 = (1 - b)\left[\frac{p}{b}\right] - b + p + 1$$

Here [ ] is the floor function or integer part. That was enough at the time 1979 to explain some drawings but not all. Later, the computer resources to make these drawings allowed me to explore the values of p much further and to find other groups of spikes. For example, with $p = 10007$ and $b = 107$ we obtain: view near the center of the drawing.



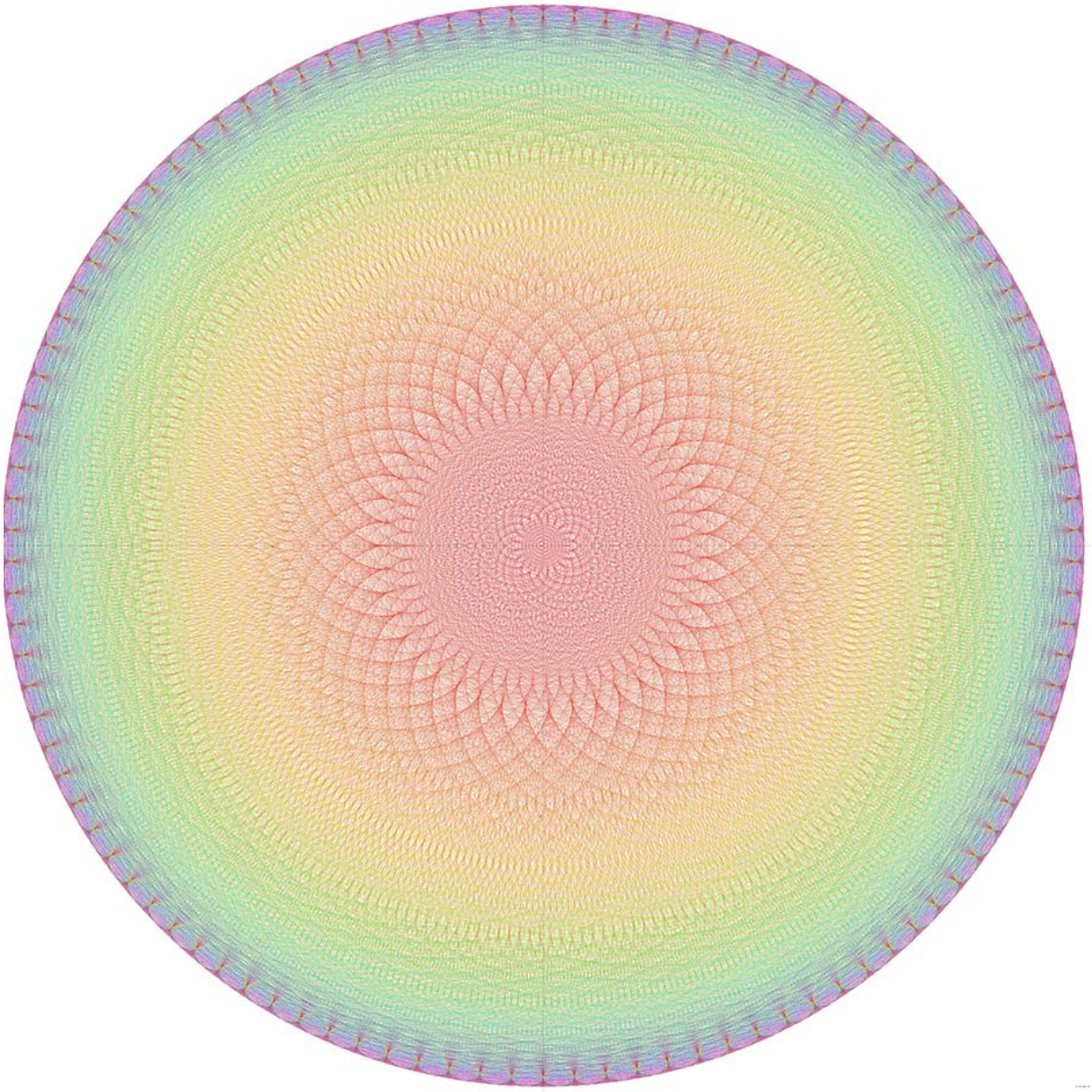
Zoom on the colorized image of 107^{n} mod 10007

I call group of points: all the peaks on the same perimeter at the same distance from the center of the circle. It is not strictly speaking a group. There are 3 spikes in the center, followed by 20 and 23 other spikes. Zooming in to a smaller scale reveals the 43 tips calculated according to the formula.



By zooming out we see 43 spikes (P_1) the lines are colorized according to their length which makes the drawing easier to see.

It remained to find out why we count 20 and 23 spikes. On the complete drawing we can distinguish up to 8 layers of spikes.



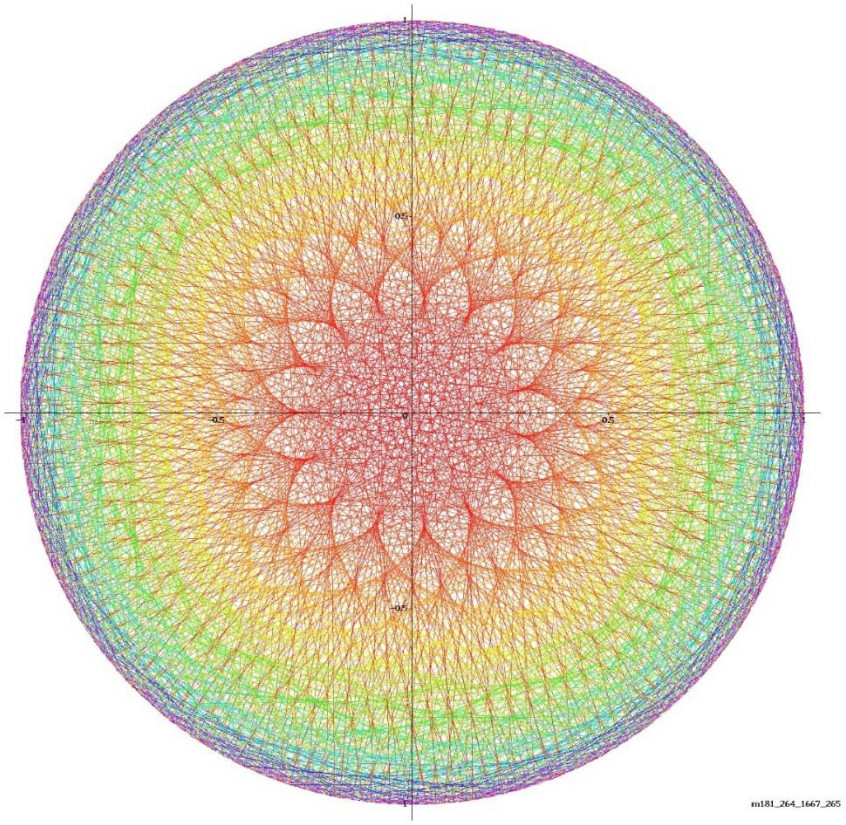
Drawing of $107^n \ mod$ 10007 or 1/10007 in base 107.

What seems to emerge is that the many sets of spikes are generated from $P_0 = b - 1$ and $P_1 = (1-b)\left[\frac{p}{b}\right] - b + p + 1$ only, P_1 may be negative but it does not change the rules. The 2 quantities of P_0 and P_1 are sufficient to explain all the groups or sets of spikes. It suffices to consider the differences of the multiples of P_0 and P_1. Let's call the set $E_{P_0} = \{ P_0, 2P_0, 3P_0, 4P_0, \ldots\}$ and the set $E_{P_1} = \{ P_1, 2P_1, 3P_1, 4P_1, \ldots\}$, then by having all the absolute differences between the 2 sets absolute differences between the two and take the list of smallest values. The first 20 first numbers are enough to list all the possible harmonics. I call harmonics that list of numbers. In this example with $107^n \ mod$ 10007 we have $P_0 =$

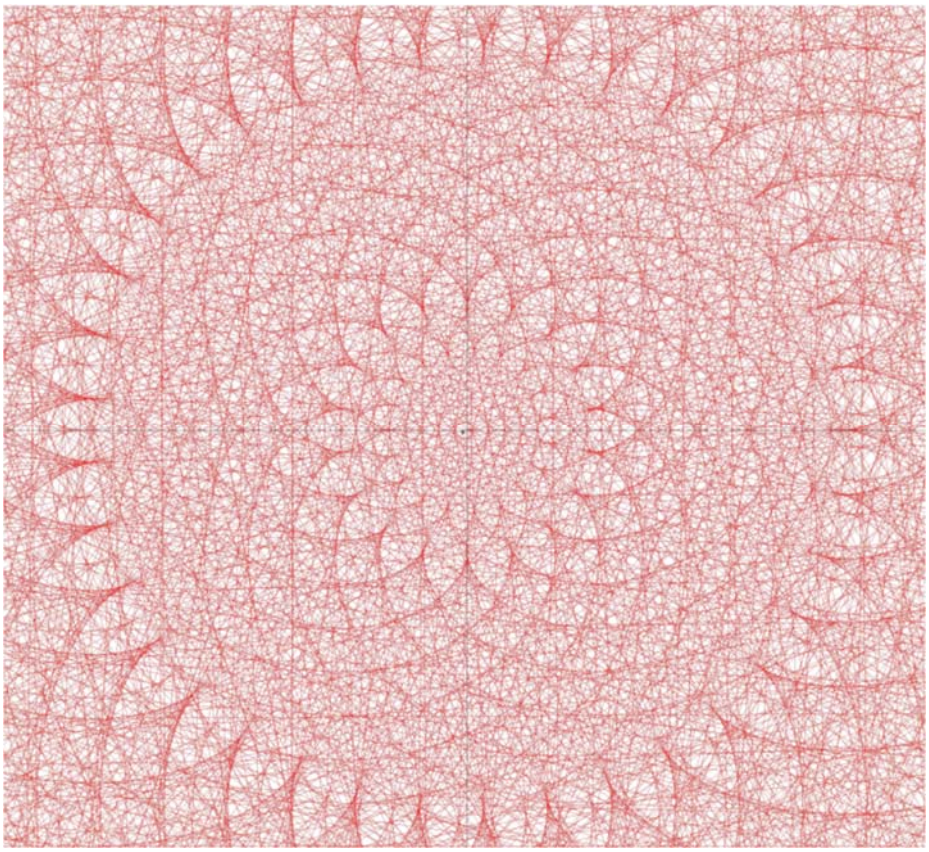
106 and $P_1 = 43$. From which we get the 2 lists {106, 212, 318, 424, 530, 636, 742, 848, 954, 1060} and {43, 86, 129, 172, 215, 258, 301, 344, 387, 430}. The final list is then {3, 6, 17, 20, 23, 26, 37, 40, 43, 100, 106} by removing the multiples of the same number the purified list becomes:

{3, 17, 20, 23, 26, 37, 40, 43, 106}.

These harmonics are the ones we see on the previous figure. The 2 numbers 106 and 43 are therefore the generators of the groups of spikes which appear in the drawing. It should also be understood that there is a limit to the precision and the identification of a group of spikes, they are not necessarily very visible. To validate the hypothesis about P_0 and P_1 and, we take a sample of primes and bases. To simplify the problem, we will choose bases which are primitive roots of p.

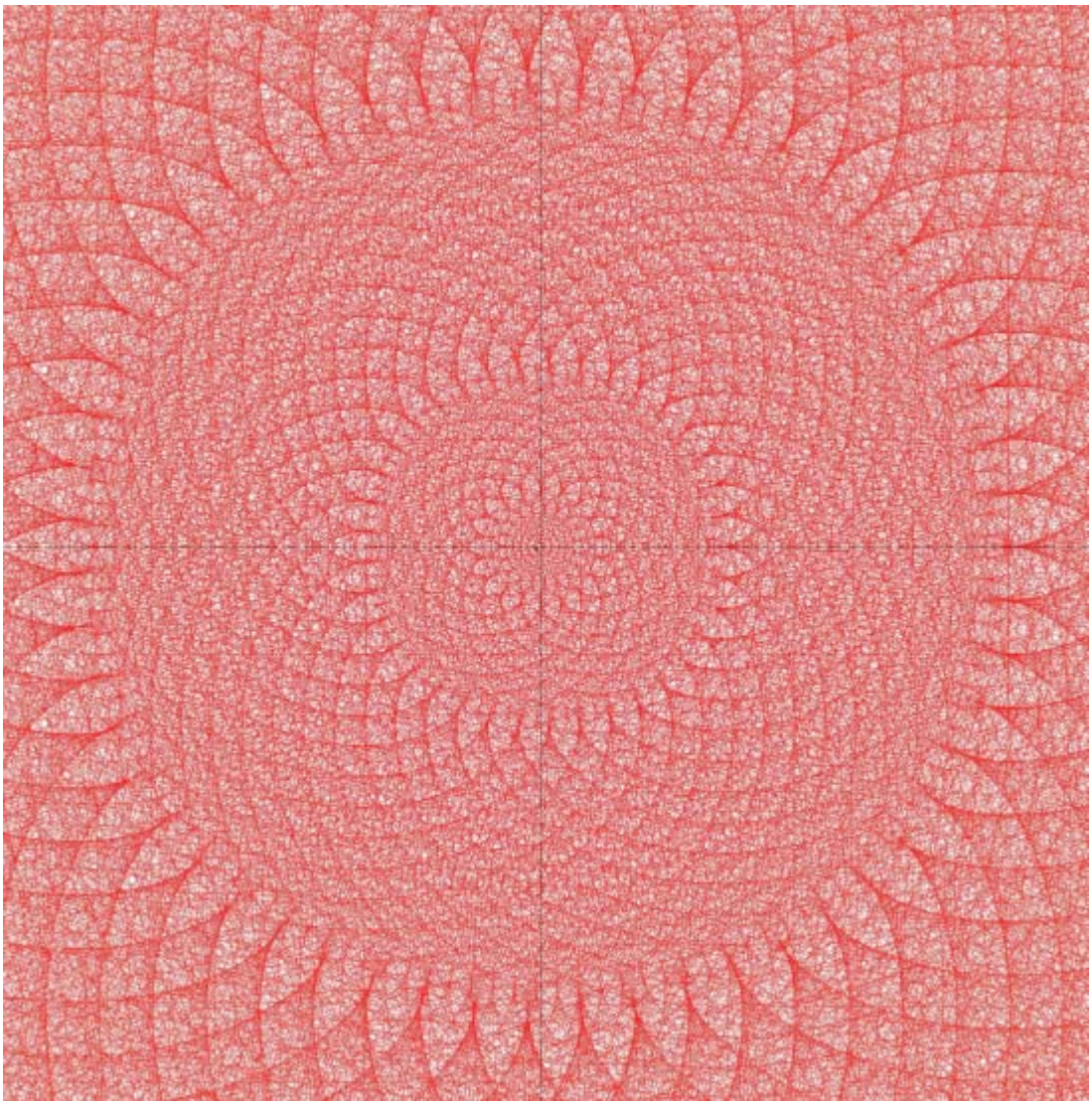


With $265^n \ mod\ 1667$ the values of are $P_0 = 264$ and $P_1 = 181$ the harmonics are {7, 8, 15, 22, 23, 30, 38, 45, 53, 60, 61} and 15 and 38 are visible.

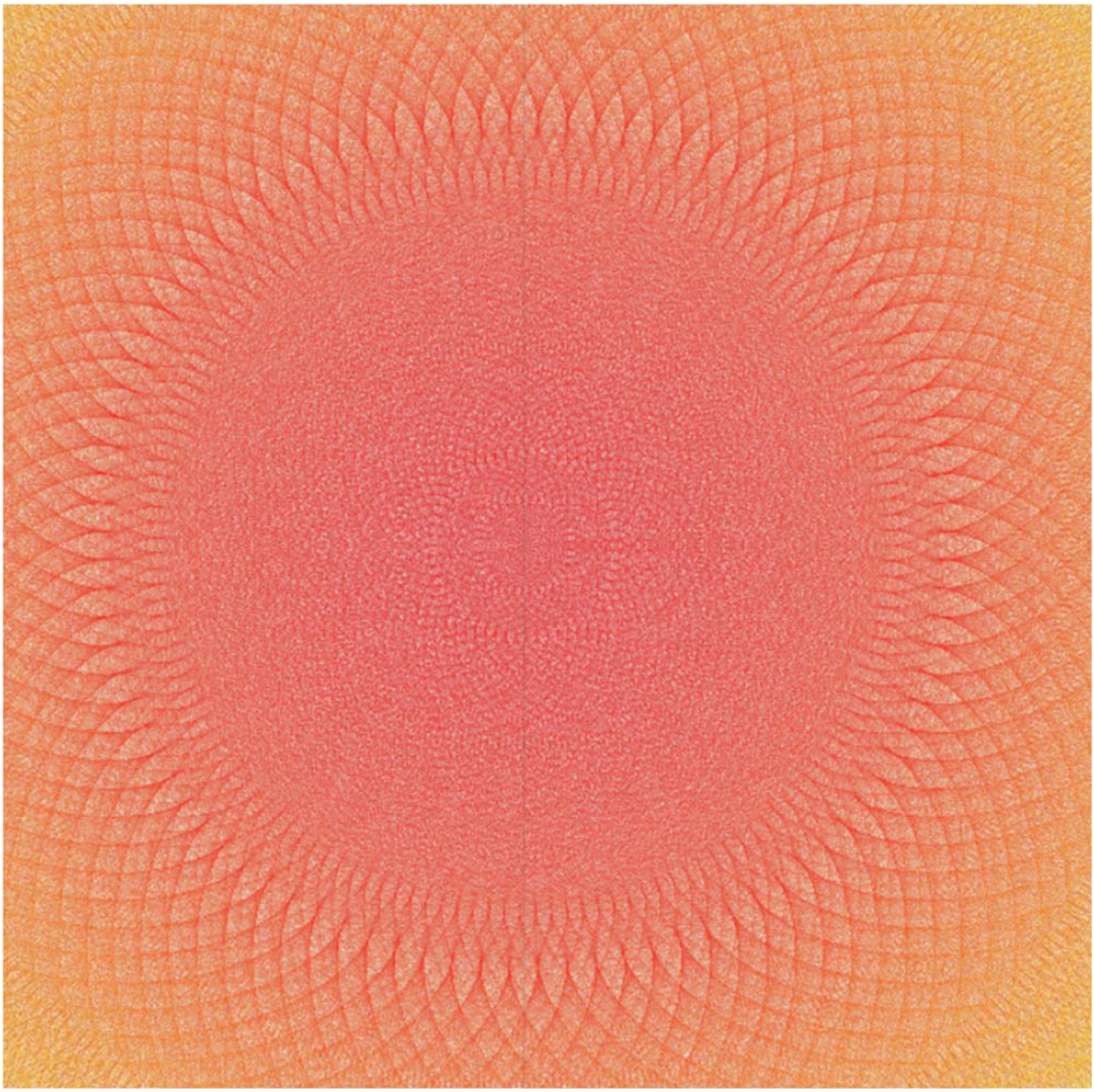


With the prime 32173 we have 55 spikes as calculated. The greater the prime number, the greater the number of sets of spikes.

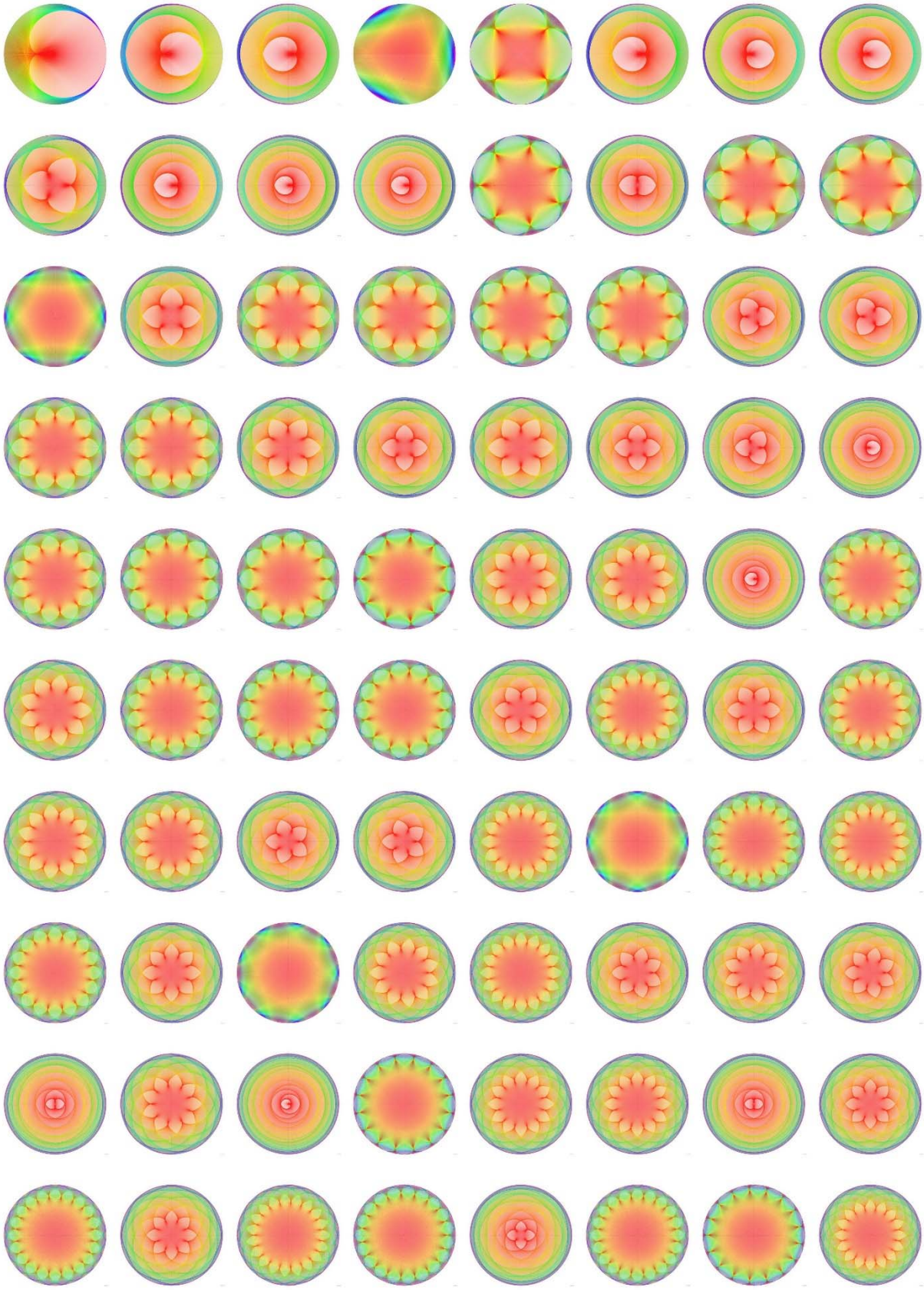
The final list is therefore: 3, 6, 17, 20, 23, 26, 37, 40, 43, 100, 106 by removing the multiples of the same number the purified list becomes: {3, 17, 20, 23, 26, 37, 40, 43, 106} The 2 numbers, 106 and 43 are therefore the generators of the groups of points which appear in the drawing. It should also be understood that there is a limit to the precision and the identification of a group of points, they are not necessarily very visible. For validate the hypothesis about and, we take a sample of primes and bases. To simplify the problem we will choose bases which are primitive roots of p.



With $240^n \ mod\ 14009$, we obtain $P_0 = 92$ and $P_1 = 239$ the center of the huge 1 billion pixels gives 18 and 19 spikes.



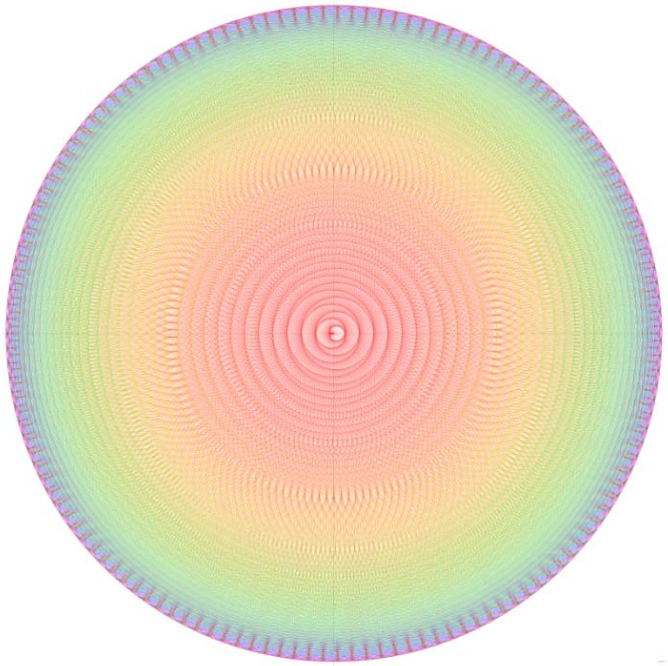
With the prime 45263 and base 240



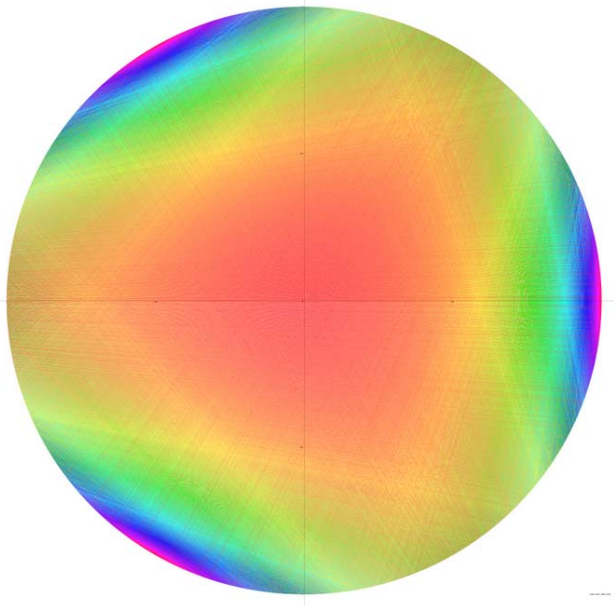
The first 80 images of mod 10037
All the other images are here: http: //plouffe.fr/10037

If

1- If $P_1 = 1$, the number of turns or layers will be proportional to p/P_0, for example with 140 mod 10009, we have 10009/139 will have 72 layers.

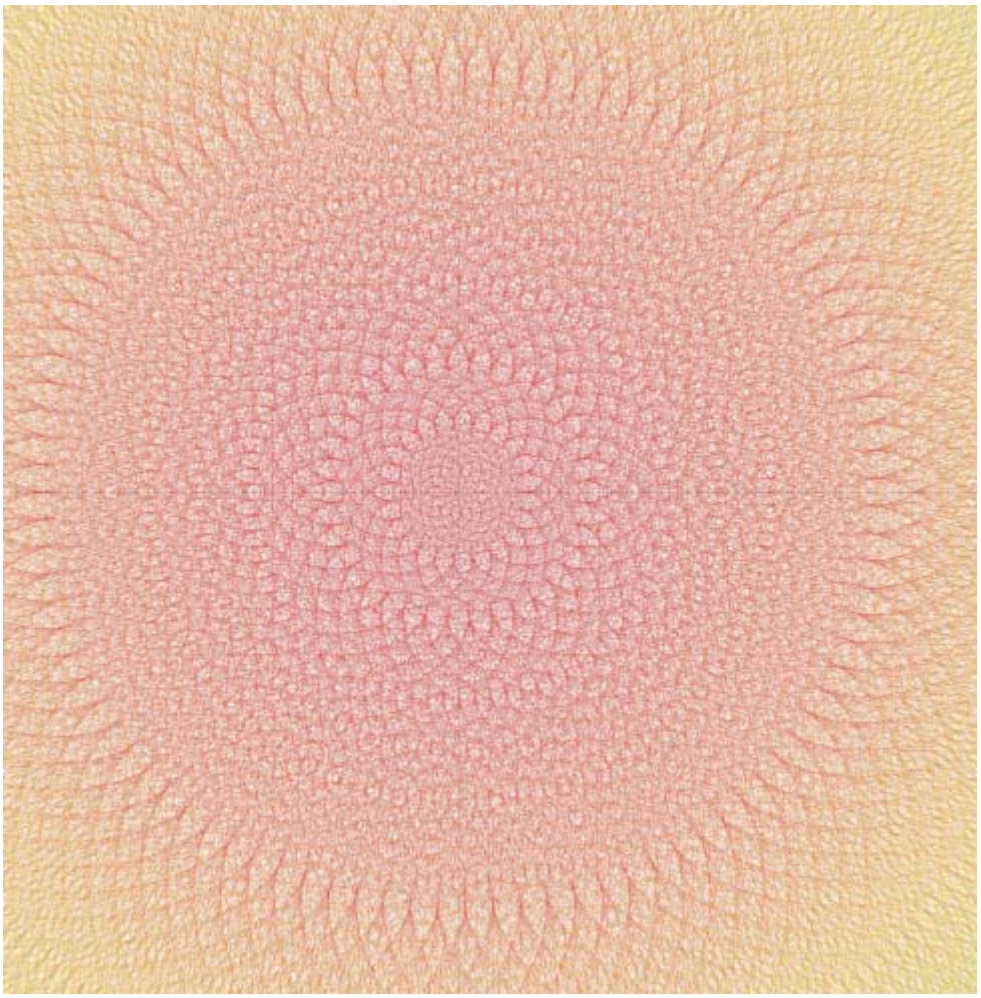


2- If $P_1 \approx P_0$ the tips will only be visible as a shadow on the outside and the number of outer tips will be$|P_1 - P_0|$, as here with $5018^n \bmod 10037$ gives us 5017 and 5014, we have 3 diffuse peaks P_0=5017 et P_1=5014.



3- The larger the base, the richer the design will be in harmonics. By taking the base 2 we always get a cardioid and if p increases the richness of the drawing is the same but more precise, there are no complex harmonics. If the base is 60 for example, already in the

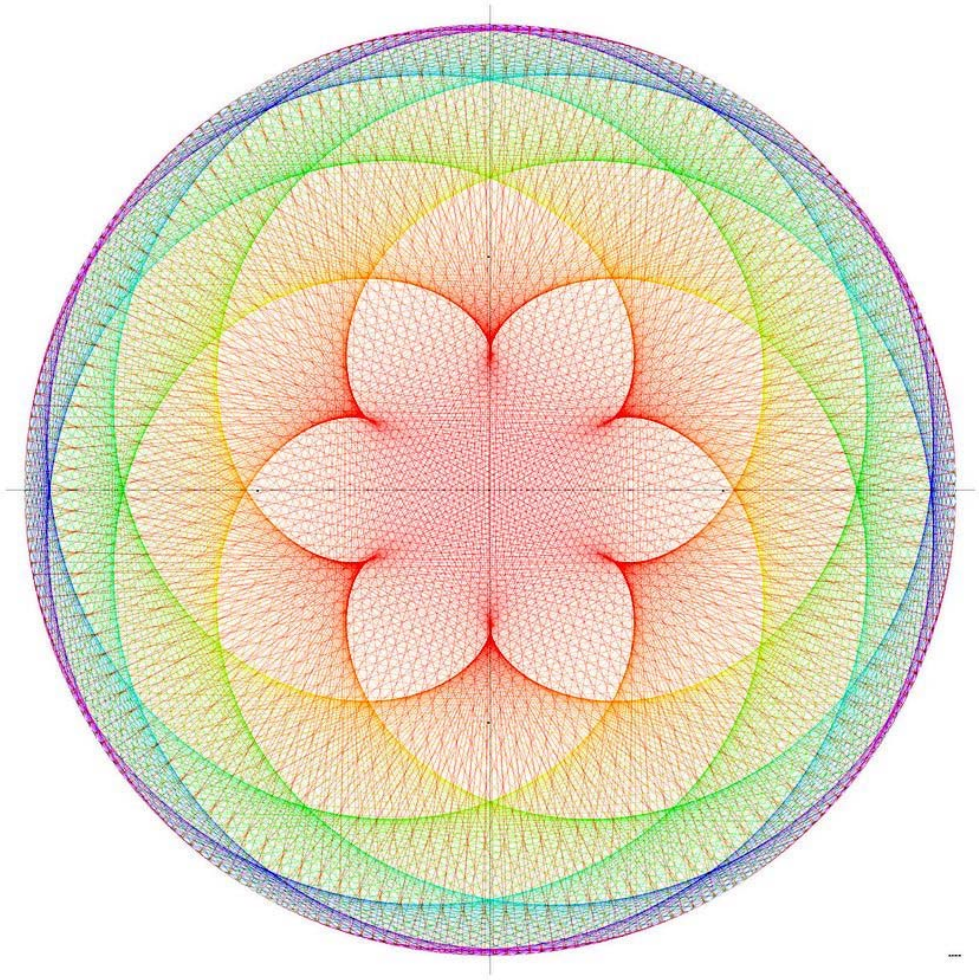
center we see lots of harmonics, in some designs there are up to 10 different groups of points.



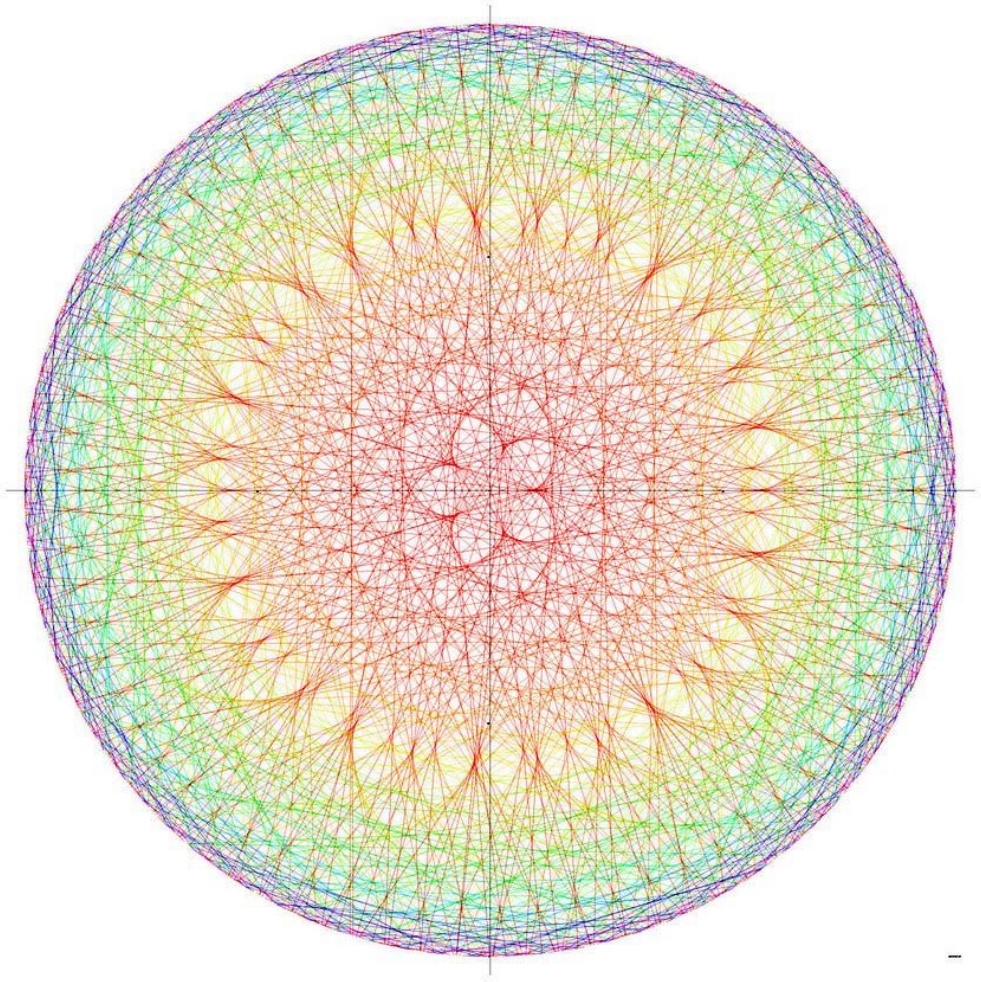
Here with $60^n \bmod 10007$

4- The tip or spike groups are not sub-groups of the cyclic group for a good reason. The tips are grouped together on the same perimeter in roughly equal sets. If we spoke of a group and a sub-group, we would have a precise number of elements, it is not the case. For example, 63 mod 10037 has in its center 7 distinct spikes which contain approximately 1433 lines each, since $10036 \; 4 \cdot 13 \cdot 193$ most of the time this will necessarily be the case. The harmonics in this case are: 7, 8, 13, 14, 15, 20, 21, 22, 27, 28….

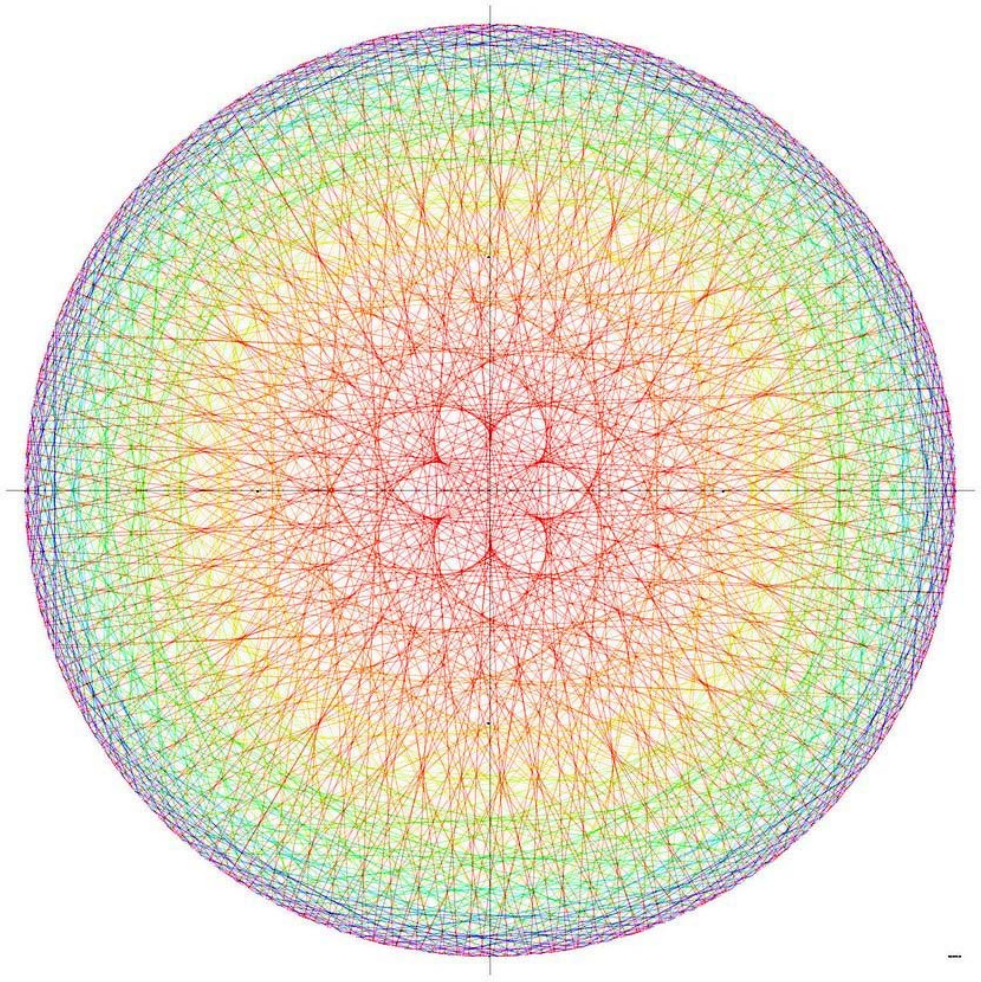
So I chose the base 240 to have a maximum of effects and with a size of graphics up to 32768 32768, which is over 1 billion pixels. Here are the few cases made with the base 240 for certain prime numbers.



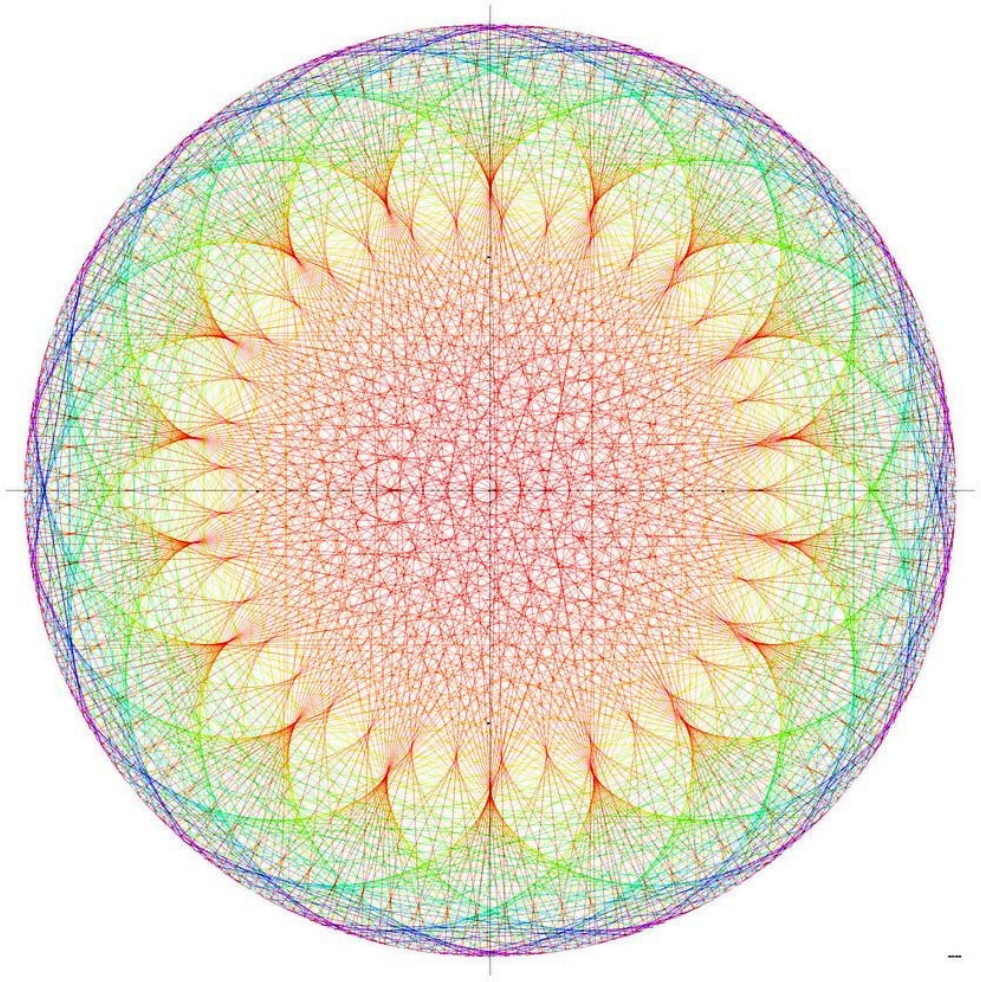
Simon Plouffe 2020: base = 240 , prime = 1667, P1 = 6, harmonics = 6, 95



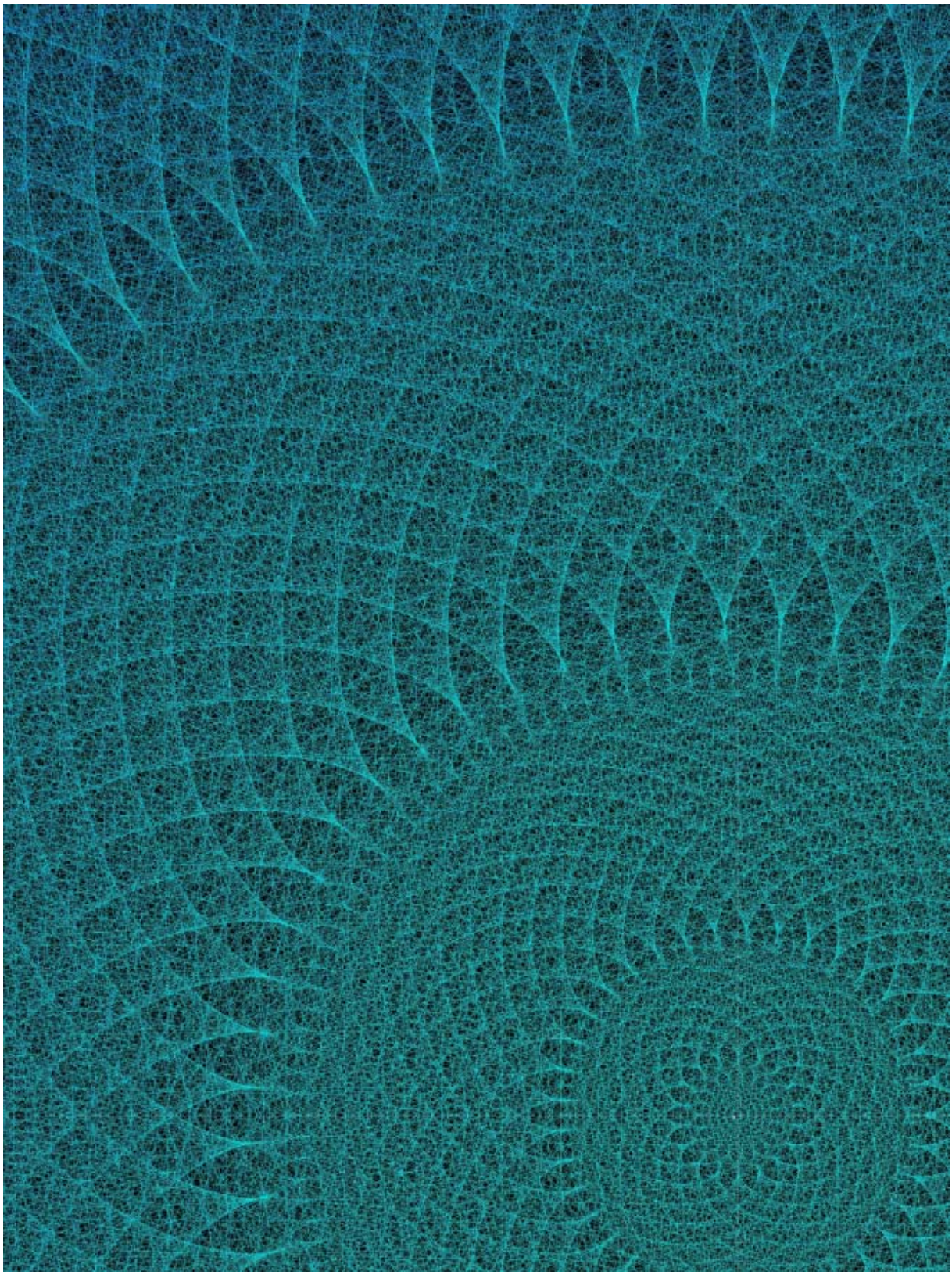
Simon Plouffe 2020: base = 240 , prime = 887, P1 = 69, harmonics = 5, 10, 15, 17, 22, 27, 32, 37, 42,



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,



Near the center of 240^n mod 26437 in inverted color for more visibility
$P_0 = 239, P_1 = 92$
The number of spikes are within the sequence of harmonics : 1, 17, 18, 19, 20, 35, 37, 54, 55, 56, 57, 72, 73, 74, 75, 91, 92

Bibliography:

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

[2] Animation with a variable base
https://www.youtube.com/watch?v=13be44CqrrI

[3] Multiplication Tables

https://www.youtube.com/watch?v=qhbuKbxJsk8

[4] Plouffe, Simon, Films of congruences around a circle :
https://www.youtube.com/results?search_query=plouffe314

[5] Plouffe, Simon, Shapes generated by 1229.

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

[6] Plouffe, Simon, Large scale experiment with base 240.
http://plouffe.fr/premiers%20base%20240C/

[7] Plouffe, Simon, Experiments with the prime 10037, all the 4606 primitive roots of 10037 are presented.

http://plouffe.fr/10037/