Residue Designs, String Art, and Number Theory

David Richeson

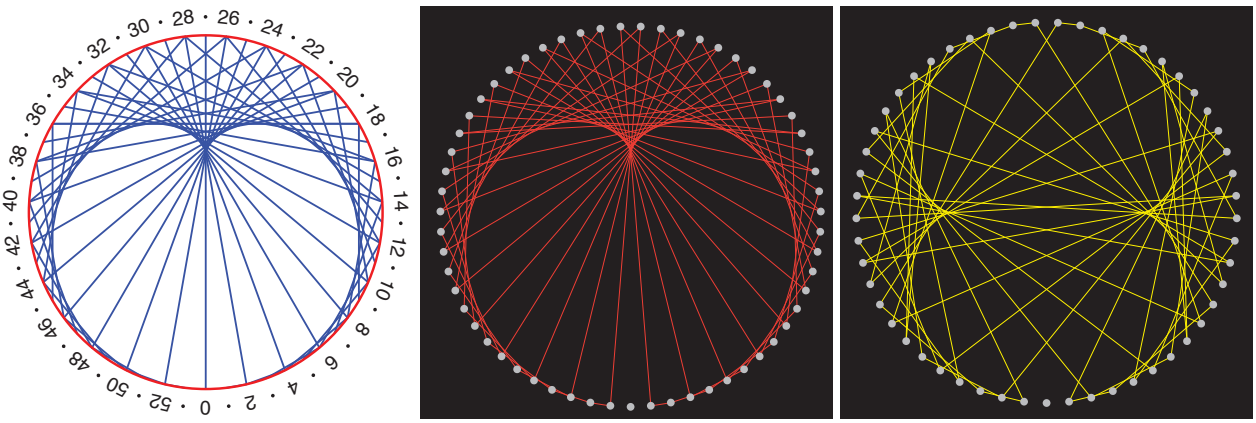
Dickinson College, Carlisle, Pennsylvania; richesod@dickinson.edu

Abstract

To make string-art cardioids and nephroids, we must divide a circle into n equal parts and connect all points k to ak (modulo n). In this article we show that the best choice of n is one for which n is prime and a is a primitive root of n.

The cardioid is a beloved mathematical object. This heart-shaped curve is an *epicycloid*; it is traced by a point on a circle rolling around the circumference of another circle of the same radius. It is the caustic in the bottom of a coffee cup when light shines in from the brim of the cup. The main bulb of the Mandelbrot set is a cardioid. Given a point P on a circle C, the envelope of circles with center on C passing through P is a cardioid. It can even be formed as the envelope of lines. It is the last of these that will be our focus.

Begin by placing n equally-spaced points on a circle. Number them 0 through $n-1$. Draw line segments between k and $2k$ for all k, doing arithmetic modulo n. The envelope of these lines is a cardioid. The larger the n, the more clearly we see the curve. Figure 1(a) shows a cardioid obtained with $n = 54$ divisions. This construction clearly lends itself to string art, as shown in Figure 1(b); in this case there are $n = 59$ equally-spaced nails with red string running between them.



(a) **(b)** **(c)**

Figure 1: *(a) A cardioid formed with $n = 54$, (b) a cardioid made from string and $n = 59$ nails, and (c) a nephroid made using $a = 3$ and $n = 53$.*

We can generalize this procedure by choosing an integer $a \geq 2$ and drawing line segments (or running string) between k and $ak \pmod{n}$ for all k. Figure 1(c) shows the case $a = 3$ and $n = 53$. The envelope of these lines is a *nephroid.* More generally, for a given a, the envelope is an epicycloid with $a-1$ cusps. In the literature, such figures are known as *residue designs* (see, e.g., [5], [3], [4], [2]).

To make one of these designs on paper, simply divide a circle into any number of equal parts and draw all required lines with a ruler and pencil. Making one out of string is more complicated—and more interesting.

Let's look at the process required to make the cardioid in Figure 1(b). After placing the 59 nails, start with the string tied to nail 1 and run it to 2, then to 4, then to 8, and so on (doing all arithmetic modulo 59).

The string will eventually return to the first nail. (The complete sequence is 1, 2, 4, 8, 16, 32, 5, 10, 20, 40, 21, 42, 25, 50, 41, 23, 46, 33, 7, 14, 28, 56, 53, 47, 35, 11, 22, 44, 29, 58, 57, 55, 51, 43, 27, 54, 49, 39, 19, 38, 17, 34, 9, 18, 36, 13, 26, 52, 45, 31, 3, 6, 12, 24, 48, 37, 15, 30, and 1.) Notice that the string does not reach nail 0, which is good since $2 \cdot 0 = 0$ is a dead-end.

What if we tried to recreate the design in Figure 1(a) with 54 nails and string? The sequence would start with 1, 2, 4, 8, 16, 32, 10, 20, 40, 26, 52, 50, 46, 38, 22, 44, 34, 14, 28, and 2, and then it would enter a cycle of length 18. Two-thirds of the nails would remain unvisited.

These examples prompt a question: which integers $1 < a < n$ will yield a string art design requiring one string? Restated mathematically, will $\{1, a, a^2, a^3 \ldots, a^{n-1}\} = \{1, 2, \ldots, n-1\}$ when computed modulo n? Our earlier examples show that for $a = 2$ and $n = 59$ the answer is yes, for $a = 3$ and $n = 53$ the answer is yes, and for $a = 2$ and $n = 54$ the answer is no. This question is not a geometric one but a number theoretic one. Really we can rephrase the question as: For what integers $1 < a < n$ is it the case that

1. $a^{n-1} \equiv 1 \bmod n$, but
2. $a^k \not\equiv 1 \bmod n$ for $k = 1, 2, \ldots, n-2$?

The set of integers modulo n, which we will write as $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$, is a group under addition—0 is the additive identity, every element has an additive inverse, and so on. We can also multiply elements in $\mathbb{Z}_n$. But $\mathbb{Z}_n$ is not a group under multiplication because not every element has a multiplicative inverse. For instance, 0 does not have a multiplicative inverse for any n; 2 does not have a multiplicative inverse for any even value of n; and so on. The elements of $\mathbb{Z}_n$ that have multiplicative inverses are precisely those that are relatively prime to n. This set, which we denote $\mathbb{Z}_n^\times$, is a group under multiplication. The number of elements between 1 and $n-1$ relatively prime to n, and hence the order of the group $\mathbb{Z}_n^\times$, is $\phi(n)$, where ϕ is *Euler's totient function*.

Returning to our question, then, we would like to find integers $1 < a < n$ so that

1. $\phi(n) = n - 1$, and
2. a is a generator of the group $\mathbb{Z}_n^\times$.

We know that property (1) is satisfied only when $n = p$ is prime. So, our string art must, at a minimum, have a prime number of nails. In this case, $\mathbb{Z}_p^\times$ is a cyclic group with $\phi(p-1)$ generators, and a generator a is called a *primitive root* of n. Thus, we can rephrase our central question yet again: For what integers $1 < a < p$, with p prime, is a a primitive root of p?

This question has a long an interesting history. Gauss introduced primitive roots in his 1801 *Disquisitiones Arithmeticae*. In 1927 Emil Artin conjectured that if a is an integer not equal to -1 and is not a perfect square, then it is the primitive root of infinitely many prime numbers. So assuming Artin's conjecture is true, if we want to obtain a cardioid ($a = 2$) we have infinitely many p to choose from so the circle of nails can be strung with one string. The same is true when a is 3, 5, 6, 7, and 8. But Artin's conjecture does not apply when a is a square like 4 and 9. This conjecture is still an open problem for all a. (Interestingly, in 1967 Christopher Hooley proved that Artin's conjecture would be true if the generalized Riemann hypothesis is true ([1]).) Finding primitive roots for prime numbers is central to some number-theoretic encryption schemes, although unlike for our string art, these situations are faced with extremely large prime numbers. In general, finding integers k for which $a^k \equiv b \bmod n$ is known as a *discrete logarithm* problem.

For small a and p, it is not too difficult to use a brute force approach to check whether a is a primitive root of p—with pencil and paper, using an Excel spreadsheet, using WolframAlpha, or with a little computer code. For larger p we can use tools from number theory to streamline the process, but we will not discuss those techniques here. It is also possible to look online. The On-Line Encyclopedia of Integer Sequences has entries for the primes with primitive roots 2 (sequence A001122), 3 (A019334), 5 (A019335), 6 (A019336),

7 (A0193377), 8 (A019338), 10 (A001913), and more. For instance, the primes less than 100 that have primitive root 2 are 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, and 83.

What if we want to make a nephroid ($a = 3$) using a circle of 67 nails? A quick check shows that 3 is not a primitive root of 67. Indeed, 3 generates the proper subgroup

$$H = \{1, 3, 5, 8, 9, 14, 15, 22, 24, 25, 27, 40, 42, 43, 45, 52, 53, 58, 59, 62, 64, 66\}$$

of $\mathbb{Z}_{67}^{\times}$. For our string art, that means we could use one piece of string to connect these 22 values. This string is shown in blue in Figure 2.

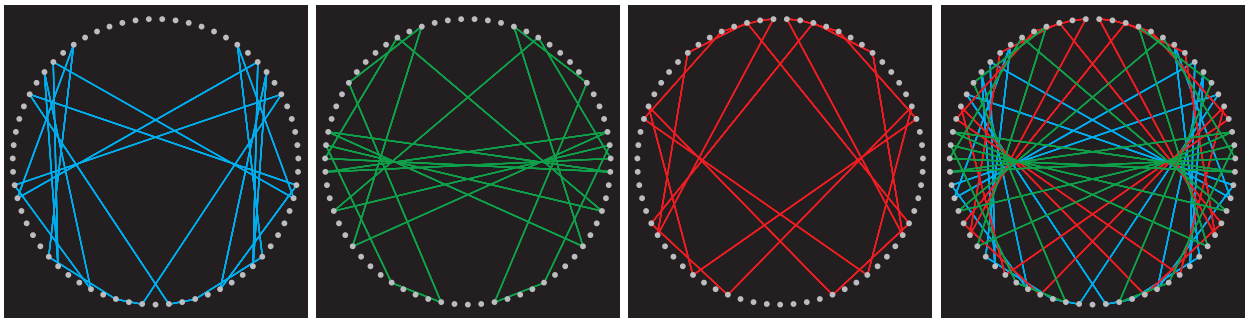


Figure 2: *The case of $n = 67$ and $a = 3$ requires three strings*

This leaves 45 nails unvisited. Fortunately, because H is a subgroup of $\mathbb{Z}_{67}^{\times}$, we can partition the group $\mathbb{Z}_{67}^{\times}$ into $[G : H] = |G|/|H| = 3$ disjoint cosets. (In [4], Moore also used ideas from group theory, including cosets, to describe the mathematics of residue designs.) In particular, take any value not in H, 2, say, and multiply every element of H by this value. This produces the coset

$$2H = \{2, 6, 10, 13, 16, 17, 18, 19, 23, 28, 30, 37, 39, 44, 48, 49, 50, 51, 54, 57, 61, 65\}.$$

An equivalent way of obtaining this coset, and one more useful to us, is to start with 2 and repeatedly multiply by 3, obtaining $2H = \{2, 2 \cdot 3, 2 \cdot 3^2, \ldots, 2 \cdot 3^{n-1}\}$, which we then reduce modulo 67. This means that after tying off our first string, we can start a second string at a value that doesn't already have string, 2 in this case, and repeatedly multiply by 3 to connect all the values in the coset. This string pattern is shown in green in Figure 2. Finally, take any element not in either H or $2H$, 4, say, and multiply every element of H by this value to obtain

$$4H = \{4, 7, 11, 12, 20, 21, 26, 29, 31, 32, 33, 34, 35, 36, 38, 41, 46, 47, 55, 56, 60, 63\}.$$

The corresponding string pattern is shown in red in Figure 2.

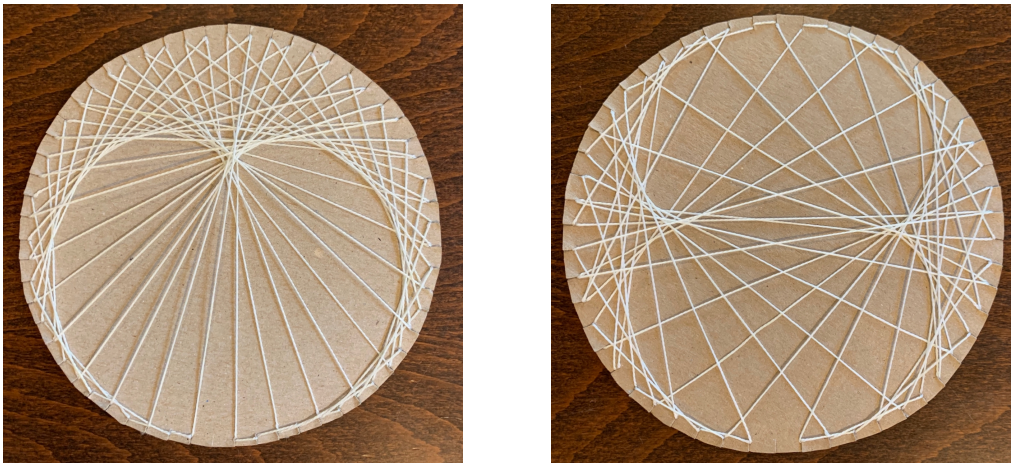
Table 1 lists all the primes p less than 100 along the top. Each row corresponds to an a-value. Then each entry in the table is the index of the subgroup generated by a in the group $\mathbb{Z}_p^{\times}$. Equivalently, it gives the number of strings required to make the corresponding piece of string art. The cells colored green are those that can be strung with one piece of string. That is, they correspond to the primitive roots a of the prime p.

Readers are encouraged to make their own string art. Using a board, nails, and string is one method. A more accessible approach is to use string and cardboard with slits cut along the rim, as shown in Figure 3. One thing to be aware of with this approach is that when we complete the first circuit with the string, the design shows only half the lines because half run along the back side. So we need to follow the circuit a second time with the string sitting on the opposite side of the cardboard. In the case of the cardioid in Figure 3(a), for instance, because $n - 1 = 58$ is even, the string running from 30 to 1 would be behind the cardboard, and the following segment would be above the cardboard—just like the first segment. We want the sides switched,

Table 1: *The number of strings required for a disk with p nails (columns) using the multiplicative factor a (rows). The green cells indicate the a-values that are primitive roots of p.*

	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
2	1	1	2	1	1	2	1	2	1	6	1	2	3	2	1	1	1	1	2	8	2	1	8	2
3		1	1	2	4	1	1	2	1	1	2	5	1	2	1	2	6	3	2	6	1	2	1	2
4		2	2	2	2	4	2	2	2	6	2	4	6	2	2	2	2	2	2	8	2	2	8	4
5			1	2	3	1	2	1	2	10	1	2	1	1	1	2	2	3	14	1	2	1	2	1
6			3	1	1	1	2	2	2	5	9	1	14	2	2	1	1	2	2	2	1	1	1	8
7				1	1	1	6	1	4	2	4	1	7	2	2	2	1	1	1	3	1	2	1	1
8				1	3	2	3	2	1	6	3	2	3	2	1	1	3	3	2	24	6	1	8	6
9				2	4	2	2	2	2	2	4	10	2	2	2	2	12	6	2	12	2	2	2	4
10				5	2	1	1	1	1	2	12	8	2	1	4	1	1	2	2	9	6	2	2	1

so instead, run the string from 30 to 2, and then continue 2, 4, 8, and so on. When we reach 1 again, the cardioid is finished. According to Table 1, the p-values 53, 59, and 83 would be good choices for a variety of a-values, but the reader is encouraged to use the methods in this article to help choose their optimal value.



(a) **(b)**

Figure 3: *(a) A cardioid made from string and cardboard using $n = 59$ and (b) a nephroid using $n = 53$.*

Acknowledgements

Thank you to Jennifer Schaefer for the helpful conversations on this topic and to Michael McConnell and Michael Gilbert for sharing some references and for informing me that these are known as “residue designs.”

References

[1] C. Hooley. “On Artin’s conjecture.” *J. Reine Angew. Math.*, vol. 225, 1967, pp. 209–220.

[2] I. D. Johnson. “Paving the Way to Algebraic Thought Using Residue Designs.” *Math. Teacher*, vol. 91, no. 4, April 1998, pp. 326–332.

[3] P. Locke. “Residue Designs.” *Math. Teacher*, vol. 65, no. 3, March 1972, pp. 260–263.

[4] T. E. Moore. “Aspects of Group Theory in Residue Designs.” *Two-Year College Mathematics Readings*. W. Page, Ed. Washington, DC: Mathematical Association of America, 1981. pp. 254–257.

[5] A. J. Picard. “Graphing in Modular Systems.” *Math. Teacher*, vol. 64, no. 5, May 1971, pp. 459–466.