

# The Other Side of Mersenne Primes

A THESIS SUBMITTED TO THE  
UNIVERSITY OF KENT IN THE SUBJECT  
OF NUMBER THEORY FOR THE DEGREE  
OF MASTER OF SCIENCE,  
BY  
AMY KLINTBERG

School of Mathematics, Statistics and Actuarial Science  
University of Kent

Friday 13<sup>th</sup> September, 2024

*Mathematics is the alphabet with which God has written the universe.*

Galileo Galilei



# *Abstract*

Mersenne numbers,  $2^n - 1$ , with  $n \in \mathbb{N}$ , are like pay dirt, containing dirt and apparent gold. They entice us to ask: which of these numbers are prime, which are not, and if not, why not — especially the shiny ones? We address the *why not?* of that question here, exploring the nature of all Mersenne composites, the other side of Mersenne primes. There are two main themes to this work: explorations into Mersenne numbers, and examples of community engagement with the concepts involved. Chapter 1 presents Mersenne numbers visually, using modular arithmetic clocks. Chapter 2 digs at the scope and cause of Mersenne composite construction. We take a Sieve of Eratosthenes approach, customized to Mersenne numbers. Here, we see how metaphorical fool's gold — Mersenne candidates that look prime but are composite — occur, through a behaviour we coin *telescoping*, and we examine the nature of telescoping. Chapter 3 presents the famed Lucas-Lehmer primality test, along with proofs. Chapter 4 presents a collection of enrichment modules, catered to highschoolers, maths enthusiasts, and crafters, that I have developed during my study. Chapter 5 closes with thoughts on further explorations, and the Appendices house Maple code and graphical data. In the spirit of community engagement, this thesis is written with the mathematically curious in mind, as an open invitation for research and play.

## *Acknowledgements*

Many thanks to the University of Kent, Canterbury, for welcoming me into this lifelong dream, to study these numbers and draw these pictures.

I am so grateful to my family and friends who have supported my study this past year, keeping me feeling loved and sane.

This work is dedicated to my nephew Raphael, whose attitude towards learning has been a constant inspiration.

Amy Klintberg, September 2024.

# Contents

<b>Abstract</b>	<b>ii</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>1 Cold open: Welcome to Mersenne Numberland</b>	<b>2</b>
<b>2 Explorations of Mersenne Numbers and Their Divisors</b>	<b>20</b>
2.1 Interpreting the Circle Diagrams . . . . .	21
2.2 Binary Notation and Proof that Composite $n$ Implies Composite $M_n$	28
2.3 A Binary Algorithm Companion to the Circle Diagrams . . . . .	31
2.4 Prime Divisors and Mersenne Candidate Divisibility . . . . .	35
2.5 Composite Divisors, Squarefree and Otherwise . . . . .	41
<b>3 The Lucas-Lehmer Primality Test</b>	<b>46</b>
<b>4 Presentation Projects of Mersenne Concepts</b>	<b>59</b>
4.1 Fermat's Little Theorem and Spirograph Maths . . . . .	61
4.2 Intro to Mersenne Primes and the Lucas-Lehmer Primality Test . .	61
4.3 A Postgraduate Research Poster . . . . .	82
4.4 Cardioid Yarn Art of Divisibility Graphs . . . . .	84
<b>5 Closing Thoughts</b>	<b>85</b>
<b>Appendices</b>	<b>86</b>
Appendix A: Maple Code for Circle Diagrams . . . . .	86
Appendix B: Maple Code for the Binary Algorithm . . . . .	90
Appendix C: Circle and Array Data, odd divisors 3-103 . . . . .	95
Appendix D: Circle Data, odd divisors 1897-2039 . . . . .	109
<b>Bibliography</b>	<b>120</b>

# Chapter 1

## Cold open: Welcome to Mersenne Numberland

The study of simple counting numbers can escalate quickly, yielding weird and unsettling results. “Elementary” number theory is given its name for the numbers, not the theory. Nevertheless, simple counting numbers are familiar friends to work with, feeling almost tactile, with an essence of wooden blocks and watermelons. They lend themselves well to visualization. On that note, let us start by picturing the integer number line, asking: what is  $1 + 2 + 4 + 8$ ?

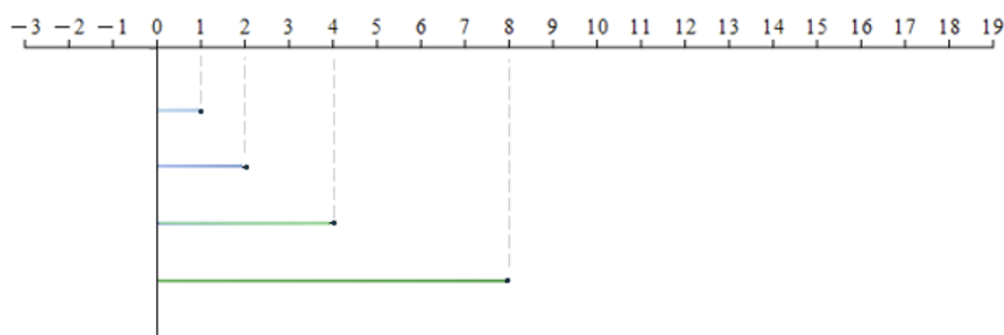


FIGURE 1.1: The integer number line and line segments of lengths 1, 2, 4, 8.

Using our number line as a ruler, we can draw the lengths 1, 2, 4, and 8 as line segments, each starting at 0 [Figure 1.1]. Observe their end points, aligned with the numbers identifying their lengths. Now, one by one, we can pivot each of them

180 degrees around their end points [Figure 1.2] , and we get a long connected line that starts at 1 and ends at 16 [Figure 1.3].

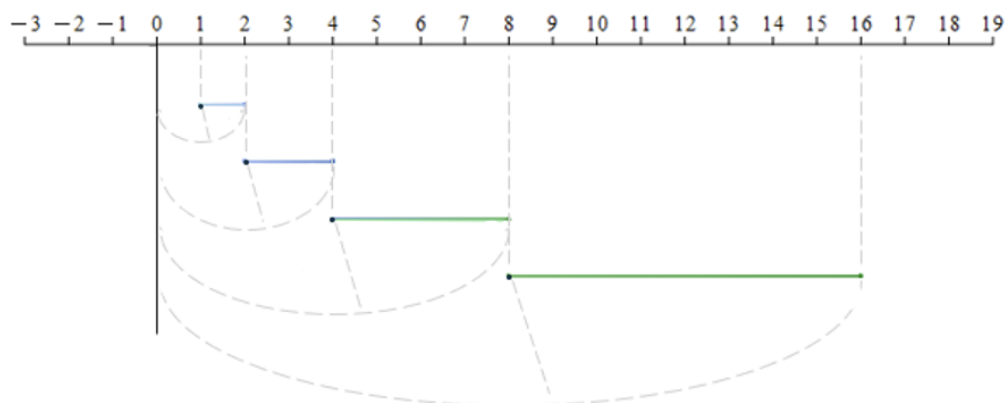


FIGURE 1.2: The line segments rotated, as described.

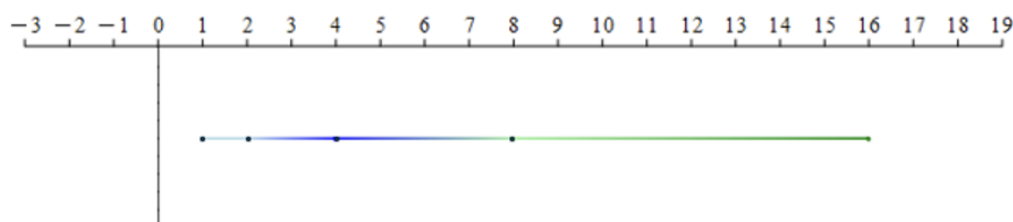


FIGURE 1.3: The total as a new line segment, fused together. Notice that this total line begins at 1, not 0.

This is a tidy visual for  $1 + 2 + 4 + 8 = 16 - 1$ . Revealingly,  $2^0 + 2^1 + 2^2 + 2^3 = 2^4 - 1$ .

Here we have an example of a **Mersenne number**, which is a number of the form  $2^n - 1$ , one less than a power of two, where  $n$  is a natural number.

Mersenne numbers are famous for their mischievous enormous primes, hiding sparsely where we can search and check, while remaining mysterious enough for us to wonder whether there are always more to find. Our goal will be to uncover some of the nature of all Mersenne numbers, both the celebrated Mersenne primes and the mild mannered Mersenne composites.

In our example case,  $n = 4$ . Notice that  $n$  equals the number of line segments — smaller whole powers of two — that we have added together. This pattern, explained in Section 2.2, happily holds true for every Mersenne number, so that we have  $2^n - 1 = 2^0 + 2^1 + 2^2 + 2^3 + \dots + 2^{n-1}$ .

Since  $n$  is a defining feature of each Mersenne number  $2^n - 1$ , we can use  $M_n$  as shorthand, with the natural number  $n \in \mathbb{N}$  as a naming index. This naming index mnemonic for  $n$  is particularly handy for us to remember the role  $n$  plays in our discussions later, since other natural numbers will be heavily involved. When seeing this line segment approach knit into application, nearly everyone mistakes  $n$  for a Mersenne number due to its star power, including career mathematicians. We will elaborate more on Mersenne numbers shortly; for now, we will continue to observe our example in motion.

We have drawn  $M_4 = 2^4 - 1$  on the number line by adding four consecutive powers of 2. Moreover, every step of the addition process landed on the next power of 2. This is powerful; creating a visual of  $2^4$  alone might encourage us to work in four spatial dimensions, but here we have built our target number  $2^4 - 1$  in one dimension, with an elegantly reliable routine.

Now, we can manipulate the integer number line itself, and observe the inner workings of the Mersenne number inscribed on it. Let us use the same technique as before, stringing together consecutive powers of 2, but with the number line wrapped around some size of circle. To pick the circle size, here is a relevant theorem that we will employ heavily throughout this thesis.

**Theorem 1.1** (Fermat's little theorem). *Given an odd prime  $p$  and  $a \in \mathbb{N}$ ,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

A basic theorem in number theory, Fermat's little theorem [16, 187], implies that any odd prime  $p$  divides Mersenne number  $M_{p-1} = 2^{p-1} - 1$ . We will discuss this theorem further in Chapters 2 and 4. For an intuitive proof of Fermat's little theorem featuring Spirograph maths, see the video link in Section 4.1.

Equipped with this clue about Mersenne number divisibility, we will look at a circle of circumference  $p = 5$  [Figure 1.4] with the entire number line coiled onto it, looking for more clues about how 5 divides our example  $2^{5-1} - 1$ .

We are using modular arithmetic, sometimes called clock arithmetic, where the equivalence of numbers that coincide is denoted  $\equiv$ , and reads, “(is) congruent to”.



FIGURE 1.4: To set up the drawing, we create a clock with 5 hours. Instead of  $12 \equiv 0$  at the top, we have  $5 \equiv 0$ .

Following the technique we used on the flat number line, we measure out each length from 0, use its endpoint number as our pivot, and then draw its length starting from the pivot and connecting to its double. There are four terms, so we draw four curved lines [Figures 1.5 and 1.6].

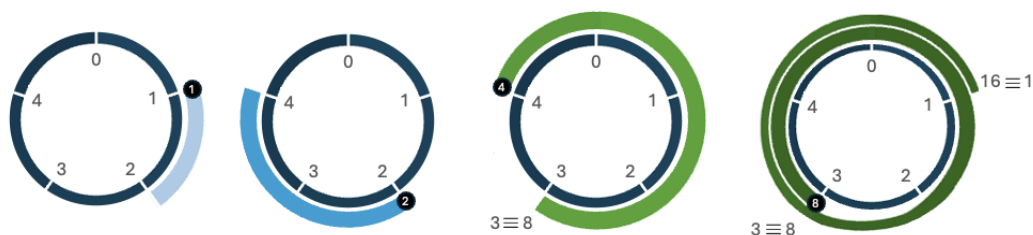


FIGURE 1.5: Lengths 1,2,4, and 8, wrapping clockwise around a circle of circumference 5, using the same strategy we saw at the beginning of the Chapter.

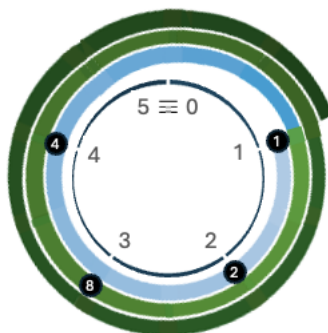


FIGURE 1.6: The fused length  $1+2+4+8$ , curled clockwise in a spiral around a circle of circumference 5. Notice that the spiral starts and ends at the same value, 1.

If we straighten the lines, connect-the-dots style, to show each line segment's beginning and end, we get a symmetrical path [Figures 1.7 and 1.8].



FIGURE 1.7: The stages of adding  $1+2+4+8$ , with each line segment launching from respective pivot points 1,2,4, and 8. Dotted lines show the distances that the pivot points are from 0.



FIGURE 1.8:  $1+2+4+8 \pmod{5}$

By building our Mersenne number  $M_4 = 1+2+4+8$ , we started at 1 and returned back to 1 at the end, completing a perfect loop of laps around the circle. Hence, our circle illustrates that the fused line segment  $M_4$  is a multiple of the circle circumference, 5. Indeed,  $M_4$  equals 15, so our results confirm that 15 is divisible by 5. We also see an interesting clue: that the path we have scribbled visits every numbered point around the circle except for the point  $0 \equiv 5$ , a satisfying visual for the 5-1 component of  $M_{5-1}$ , in the framing of Fermat's little theorem.

This is a great start, and we are excited to see what happens with other circles, for insight into Mersenne divisibility.

What circles shall we draw?

We can take any potential divisor  $d \in \mathbb{N}$  that could divide some Mersenne number, and set it as the circumference of a circle. We may as well ignore  $d = 1$ , since



everything is congruent in mod1. We can also ignore all the even numbers, since no Mersenne numbers are divisible by 2. So, we can take our potential divisor  $d$  to be any odd number greater than 1.

With a chosen circle of odd circumference  $d$ , we mentally wind the entire integer number line onto it, mark our integer positions as dots, and we are ready to scribble. In our circle, we want to draw the stepwise connect-the-dots pathway taken by ascending consecutive powers of  $2(\text{mod } d)$ , starting with  $2^0 = 1$ . By drawing our pathway, we are drawing a sum,  $2^0 + 2^1 + 2^2 + 2^3 + \dots(\text{mod } d)$ , that adds a term every time we add a line, and terminates when we stop adding lines.

As we have seen in our  $d = 5$  example, we can draw this pathway easily, by starting from the number 1 on the circle and then repeatedly multiplying by  $2(\text{mod } d)$ . This process bounces us around the circle as if pointing a laser light from 0 to our last location on the circle, and logging the ricochet. From a calculation perspective, the values counterclockwise from 0 are congruent to  $-1, -2, -3, \dots$ , so doubling them is just like doubling the values clockwise from 0, only mirrored. For example, doubling  $-1$  would take us to  $-2$  on the circle.

We get a pleasant consequence: if our path visits the value congruent to  $-1$ , the whole path will be symmetrical. As another pleasant consequence, we know that the path will never visit the value 0 itself, since no amount of doubling the number 1 will ever lead to 0.

Whenever our path returns to the starting position 1, made of say  $n$  lines, we get the same result as if we had wrapped an entire string length of  $n$  terms  $2^0 + 2^1 + 2^2 + \dots + 2^{n-1}$  around the circle, and returned to the start. Our path of  $n$  lines has drawn the representation of a Mersenne number  $2^0 + 2^1 + 2^2 + \dots + 2^{n-1} = 2^n - 1 = M_n$  that is divisible by the circle circumference  $d$ .

To interpret our drawing formulaically, remember that we started the path from the value 1; we did not start from 0. So, any time we stopped drawing lines, the answer to the sum  $2^0 + 2^1 + 2^2 + \dots 2^{\text{pause}}(\text{mod } d)$  was one less than the integer we stopped the path upon.

When our path of  $n$  lines ( $n$  terms) stops at the integer 1, we can see:

$$2^0 + 2^1 + 2^2 + \dots + 2^{n-1} \equiv 1 - 1(\text{mod } d),$$

$$2^n - 1 \equiv 0(\text{mod } d),$$

$$2^n \equiv 1(\text{mod } d).$$

Hello, Fermat's little theorem. As we touched on earlier, when  $d$  is an odd prime  $p$ , we know that  $n = p - 1$  will satisfy this congruence. Our diagrams speak the same mathematical language as our textbooks.

Let us see some circles. Now that we understand the drawing steps we want to make, we can write computer code for them, and we have. Odd divisors  $d$  are the input, and the drawings are the output. To start, we can take a look at odd divisors  $d = 3$ ,  $d = 5$ ,  $d = 7$ , and  $d = 9$  [Figures 1.9, 1.10, 1.11, and 1.12]. The Maple code for generating these circle diagrams can be found in Appendix A.

Circles with odd *prime* divisors  $d = p$  as their circumference are displayed in colour, sporting pathways of blue blended to green. A Mersenne number  $M_n$  represented by a blue-green pathway is divisible by the prime circumference  $p$ , so this Mersenne number  $M_n$  is only prime if the divisor  $p$  is itself that very Mersenne number,  $M_n$ . This is rare. Usually,  $M_n$  is composite.

Circles with odd *composite* divisors  $d$  as their circumference are displayed in grey. A Mersenne number  $M_n$  represented by a pathway in one of these circles is always composite.

On all of our example circles, the paths of consecutive powers of 2 always start at 1 and return to 1 eventually. Do we know that they will always return to 1? Happily, yes, as long as  $d$  is an odd number (namely, as long as  $\gcd(2, d) = 1$ ). We will discuss more secrets of the circles in Section 2.1.

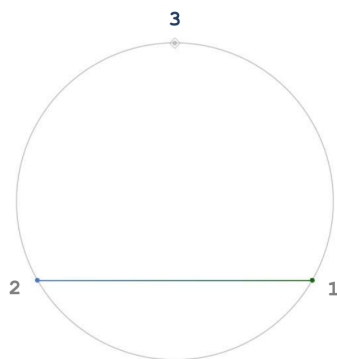


FIGURE 1.9: Prime 3 divides Mersenne prime  $M_2 = 3$ , as predicted by Fermat's little theorem. This path looks like one line segment, but the path visits two points on the circle. The path retraces itself back to the starting value, 1.

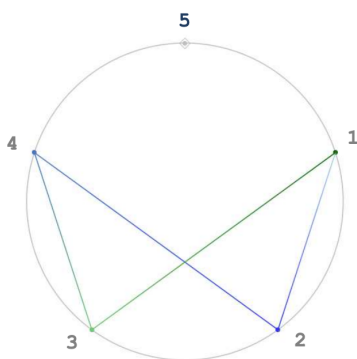


FIGURE 1.10: Prime 5 divides Mersenne composite  $M_4 = 15$ . This is our previous example, as predicted by Fermat's little theorem.

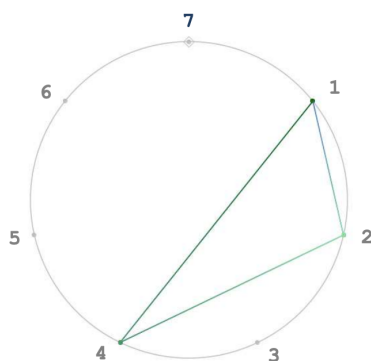


FIGURE 1.11: Prime 7 divides Mersenne prime  $M_3 = 7$ . This is a bit unexpected from Fermat's little theorem alone, but makes sense. 7 divides itself. Fermat's little theorem tells us that 7 divides  $M_6 = 63$ , which we can see on this circle as well. The six terms in  $1 + 2 + 4 + 8 + 16 + 32 \pmod{7}$  merely follow the looping path from 1 back to 1 twice.

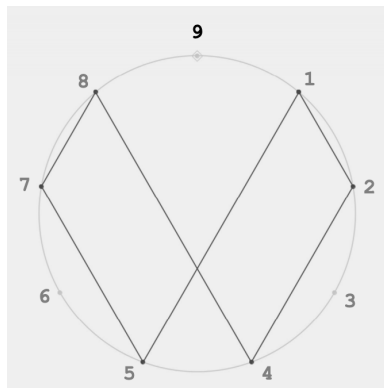


FIGURE 1.12: Composite 9 divides Mersenne composite  $M_6 = 63$ . This is not predicted by Fermat's little theorem because 9 is not prime. We will see composite divisors covered by a broader theorem, Euler's totient theorem, in Section 2.1.

When our path returns to its starting place 1 for the *first time*, the Mersenne number  $M_n$  that it represents is the *smallest* Mersenne number divisible by  $d$ . We could keep adding more lines to the path and return to 1 as many times as we like, and every time we stop at 1 we will have found another Mersenne number divisible by  $d$ . So, by finding the smallest Mersenne number  $M_n$  divisible by  $d$ , we can identify the entire collection of Mersenne numbers  $M_{\mu n}$  divisible by  $d$ , where  $\mu \in \mathbb{N}$  tells us how many times our path has completed a circuit of  $n$  steps.

We see on our example  $d = 7$  [Figure 1.11], which itself is a Mersenne number, that the smallest Mersenne number it divides,  $1 + 2 + 4 = M_3 = 7$ , is represented by a pathway that only visits three points on the circle. The pathway avoids the other three potential visitation points altogether. No matter how many times the pathway retraces its steps around the powers-of-two circuit, it will only visit those three points.

To identify the smallest such path for the smallest  $n$  giving us the smallest  $M_n$  divisible by  $d$ , we can count the number of points visited around the circle, instead of relying solely on the number of lines drawn. This was convenient for coding the circle diagrams on a computer; we did not need to tell the computer the smallest number of lines to draw, we only had to tell it how many lines would be plentiful enough to return to the integer 1 at least once.

Appendix C contains fifty-one drawings of circles with odd circumferences, and the Mersenne paths in them, for odd divisors 3-103. Let us see one more of those here, a fan favourite to view:  $d = 101$  [Figure 1.13].

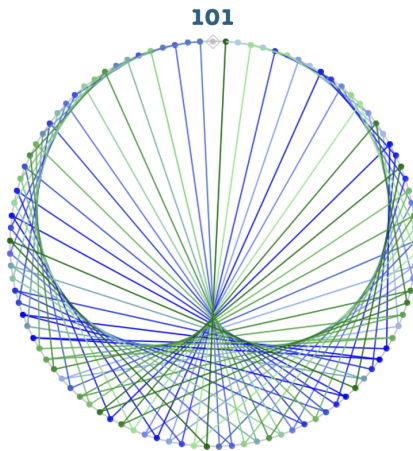


FIGURE 1.13: Prime 101 divides Mersenne composite  $M_{100} = 1, 267, 650, 600, 228, 229, 401, 496, 703, 205, 375$ , as predicted by Fermat's little theorem.

The geometric layouts of these paths are very pleasing. A common question at this stage is, “what shape are these upside-down hearts approaching?” In fact, the lines tracing multiplication by 2 are tangent to a cardioid, which is consistent with light from a single source bouncing off the rim of a coffee cup. [Figure 1.14].

Appendix D contains even more drawings of circles with odd circumferences, with more beautiful and varied Mersenne paths in them, for odd divisors 1897-2039. They are generated for possible personal connections to years in our lives, as fun images to peruse and diverse examples for our data set. A few people have expressed interest in crafting them, especially taken by the fact that the mathematical term “cardioid” means “heart-shaped”.

Although we do not explore it further in this thesis, the cardioid connection to Mersenne numbers may be worth revisiting in the future. Regardless, the geometry is magnetic.

Now, on our circles so far, we have touched on examples of Mersenne numbers that are prime:  $M_2 = 3$  and  $M_3 = 7$ , and examples of Mersenne numbers that are composite:  $M_4 = 15$ ,  $M_6 = 63$ , and  $M_{100} = 1, 267, 650, 600, 228, 229, 401, 496, 703, 205, 375$ .



FIGURE 1.14: A photo of the author's coffee cup with a cardioid light path inside. From top of frame, a tiny light source is shining down, about an arm's length away.

In each of those examples, we have read  $n$  directly from a diagram and then deduced  $M_n$ . Both  $n$  and  $M_n$  are valuable output data for us. Taking a moment to review our examples, we see there is a correlation between the primality of the index  $n$  and the primality of the Mersenne number  $M_n$ . Do we have causation as well, or coincidence?

The surprise up ahead is well known, but let us see it for ourselves. We list the first 20 Mersenne numbers [Figure 1.15] and see whether we can predict where the primes are.

We compare when  $n$  is prime and when the Mersenne number  $M_n = 2^n - 1$  is prime. In our chart, all of them match — except for one anomaly, where  $n = 11$  is prime and  $M_{11} = 2047$  is composite. The Mersenne number 2047 certainly looks prime, but, surprise, a calculator confirms it equals  $23 * 89$ . This is a bit irksome. With prime Mersenne numbers appearing so often in the first handful when  $n$  is prime, is there a primality pattern between  $n$  and  $M_n$  or not?

Marin Mersenne, the monk for whom Mersenne numbers are named, saw the intrigue in searching out their primality pattern. In Section 2.2, we will see proofs that when  $n$  is composite,  $M_n = 2^n - 1$  is always composite. On the other hand,

<u>n</u>	<u><math>2^n - 1</math></u>	<u>prime?</u>
1	1	× ×
2	3	✓ ✓
3	7	✓ ✓
4	15	× ×
5	31	✓ ✓
6	63	× ×
7	127	✓ ✓
8	255	× ×
9	511	× ×
10	1023	× ×
11	2047	<span style="color: green;">n</span> ✓ × <span style="color: red;"><math>M_n</math></span>
12	4095	× ×
13	8191	✓ ✓
14	16383	× ×
15	32767	× ×
16	65535	× ×
17	131071	✓ ✓
18	262143	× ×
19	524287	✓ ✓
20	1048575	× ×

FIGURE 1.15: Primality comparisons between  $n$  and  $M_n = 2^n - 1$ .

when  $n$  is prime, Marin Mersenne knew that  $M_n = 2^n - 1$  *might* be prime. He studied these numbers in the early 1600s, scrutinizing them up to  $2^{257} - 1$ , but did not find a formula that predicts Mersenne primes. He also investigated the mathematics of music frequencies, and was a frequent correspondent with Galileo, Fermat, and many other prominent scientists of the time [12]. We are following in some perseverant footsteps, and armed now with stronger computing power.

Here we introduce an important standardized term: when  $n$  is prime, the Mersenne number  $2^n - 1$  is called a **Mersenne candidate**, and its primality is a mystery until checked.

Mersenne candidates receive plenty of attention from organized enthusiasts globally. For the past several years, when a Mersenne candidate has been revealed as a newly discovered Mersenne prime, it has been the immediate world-champion

for its size. Of all the different kinds of prime numbers we know about, the largest currently known is a Mersenne prime,  $2^{136,279,841} - 1$ , with over 41 million digits. It was just found in October 2024 (during revisions for this thesis) through the Great Internet Mersenne Prime Search [5], which coordinates volunteer computing power around the world, testing enormous Mersenne candidates. (The previous champion was  $2^{82,589,933} - 1$ , discovered in December 2018.)

Even when a prime  $n$  is gigantic, the Mersenne candidate  $2^n - 1$  can be tested for primality using a procedure so simple that its instructions can fit on a sticky note. In Chapter 3, we will see the definition and proofs for the **Lucas-Lehmer primality test**, an elegant test applicable exclusively to Mersenne candidates. Part of what makes Mersenne numbers special is their accessibility to testing, and the strength of this primality test, which is not merely probabilistic as many primality tests are, but deterministic.

Although we know there are infinitely many primes, we still do not know whether there are infinitely many *Mersenne* primes. This adds to the allure of Mersenne candidates, enticing us to keep checking them for primes without knowing for sure whether there are more Mersenne primes to find.

In general, gigantic primes are valuable for data security via number-coded cryptography, since multiplying primes together is easy and the resulting product is difficult to factor [17, pg 156]. Finding primes suitable for use in cryptography can be tricky due to the unpredictable distribution of primes, especially among larger and larger numbers, and due to the time complexities of primality testing any numbers that are large enough. We would love to say that Mersenne numbers help to supply this market for encryption keys, but they do not. So far, only 52 Mersenne primes have been discovered, even after Mersenne candidates have been double-checked into the millions [5].

Rather than being used in encryption keys themselves, Mersenne primes are valuable to us as spokes-numbers for primes, generating excitement and cooperation for what we can discover. With many mysteries still unsolved regarding and surrounding Mersenne numbers, both the Mersenne primes and the composites challenge



us too, to find new ways to engage with mathematics and develop new methods of reasoning.

We do not discuss the strategies of cryptography much further in this thesis, nor the intricacies of other primality tests and their designs, but it is worth here noting a helpful type of prime used in cryptography, aptly called a “safe prime”.

A **safe prime**  $f$  is a prime of the form  $2g + 1$ , where  $g$  is also prime.

Relatedly, a **Sophie Germain prime**  $g$  is a prime such that  $f = 2g + 1$  is also prime.

We will see safe primes and Sophie Germain primes again in Chapter 2, Section 2.4. Mersenne primes are never safe primes nor Sophie Germain primes because, if we set  $2g + 1 = M_n$ , we calculate  $g = M_{n-1}$ . We know that  $M_n$  and  $M_{n-1}$  cannot both be prime at the same time because either  $n$  is even or  $n - 1$  is even, and a Mersenne number with an even, and thus composite, index is always composite. Nevertheless, we mention safe primes and Sophie Germain primes here because  $M_{11}$  is still on our minds. Notice that  $2(5) + 1 = 11$  with 5 being prime, and  $2(11) + 1 = 23$  with 23 being prime. 11 is both a safe prime and a Sophie Germain prime. We have found a new correlation for our Mersenne number investigations, and we explore this further in Section 2.4.

Our curiosity is piqued. What causes a Mersenne candidate to be composite instead of prime? To start, why is  $2^{11} - 1$  composite instead of prime? Its divisors, of course, are the cause, with  $2^{11} - 1 = 23 * 89$ . Well then, is there something special about 23 and 89?

Recalling Fermat’s little theorem, every odd prime  $p$  divides  $M_{p-1} = 2^{p-1} - 1$ , so, we know that 23 divides  $2^{22} - 1$ , and 89 divides  $2^{88} - 1$ .

Let us draw the circle diagrams for 23 and 89. The following drawings are taken from the author’s notebook when she was first exploring these ideas for diagrams [Figures 1.16 and 1.17].

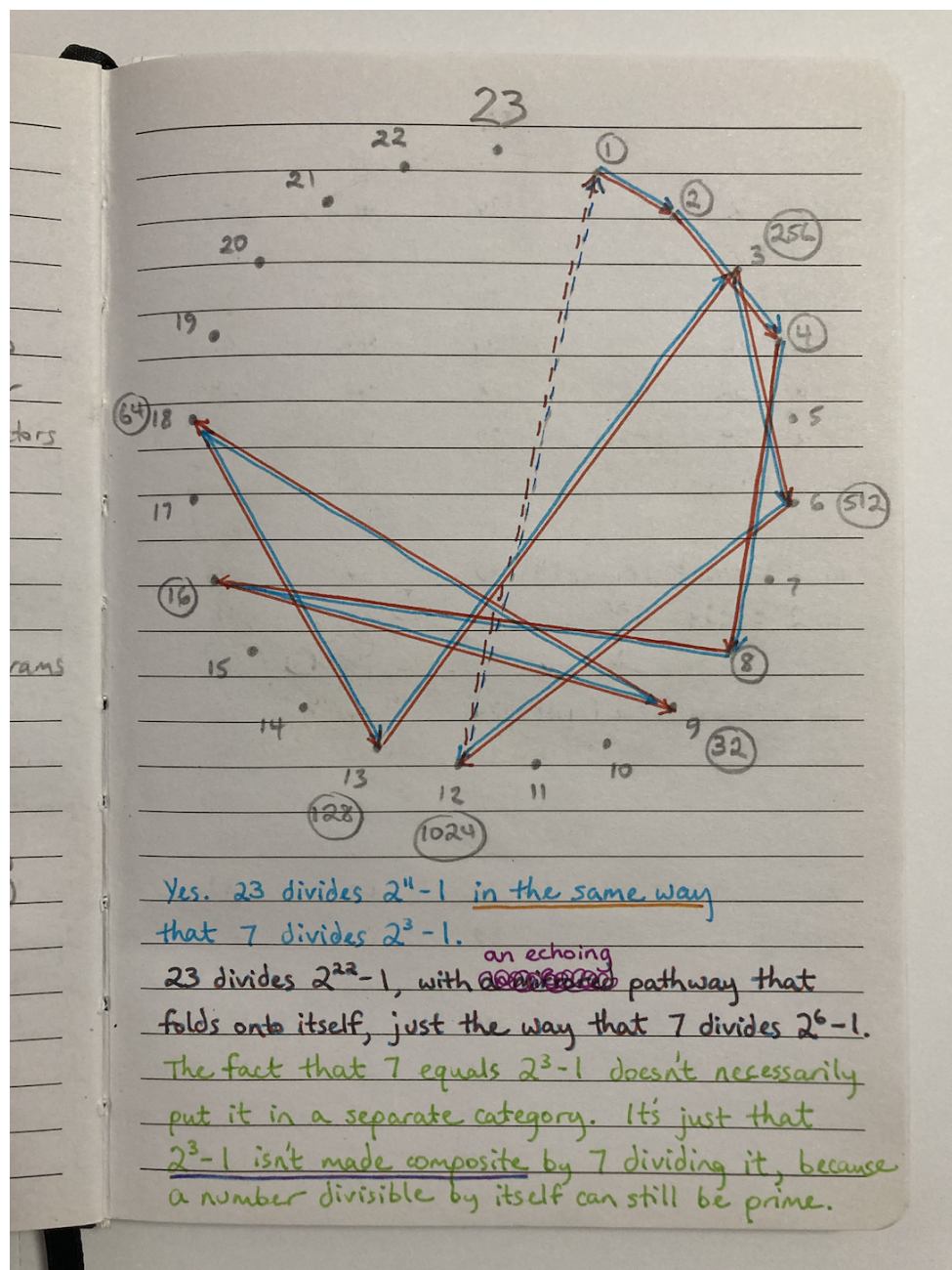


FIGURE 1.16: Here, we have added 22 terms:  $1+2+4+8+16+32+\dots$  because we know that this long line of 22 line segments will return to the start, 1. However, instead of fulfilling the symmetry potential to visit every nonzero clock hour, the pathway returns to the start after eleven terms, and then repeats the path again. It shows that, not only does 23 divide  $2^{22}-1$ , it divides a smaller Mersenne number,  $2^{11}-1$ , our star player.

The circles show us what is happening. Although Fermat's little theorem appeared to have nothing to do with Mersenne candidates — since the Mersenne index  $n = p - 1$  is never prime when  $p$  is odd — we see that it houses more intricate details about Mersenne divisibility.

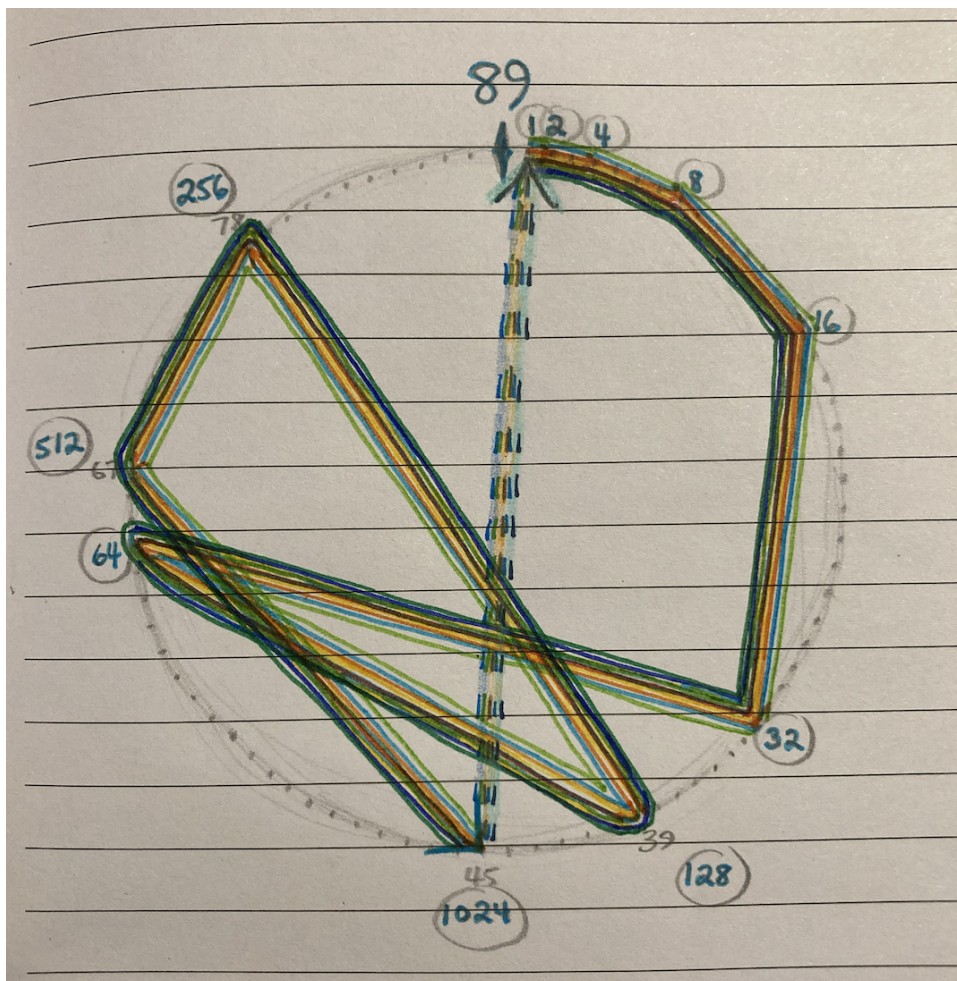


FIGURE 1.17: Likewise, here we have added 88 terms:  $1+2+4+8+16+32+\dots$  because we know this long line of 88 lines will return to the start, 1. But, as with the clock 23, this clock 89 has a pathway that returns to the start after eleven terms, and then repeats the path again and again, for a total of eight iterations. Hence, we see that 89 not only divides  $2^{88} - 1$ , it also divides the smaller  $2^{11} - 1$ .

In section 2.1, we will spell out that an odd prime  $p$  not only divides the Mersenne number with index  $n = p - 1$ , but, more specifically, with index  $n = \frac{p-1}{x}$ ,  $x \in \mathbb{N}$ . When  $x > 1$ , sometimes that index  $n$  is prime, bringing  $p$  to divide a Mersenne candidate.

We need terminology for this. Because of the retracing behaviour on the circle when  $x > 1$ , we coin the term “telescoping”. The word “echoing” was a close second choice. We continue to call the path that traces consecutive powers of 2 the “path” or “pathway”.

Under the concepts we have explored so far, we define that, given an odd prime divisor  $p$ , a path of consecutive powers of 2 **telescopes** when  $2^{(p-1)/x} \equiv 1 \pmod{p}$ , for some **telescoping factor**  $x > 1$ . We say that such a divisor  $p$  is a **telescoping divisor**, with respect to the path of powers of 2.

This is revelatory. This is why some Mersenne candidates —  $M_n$  with prime  $n$  — are themselves composite: because some odd prime divisor  $p = xn + 1$  that is sure to divide  $M_{xn}$  somehow telescopes the path of consecutive powers of 2, and consequently divides the smaller Mersenne number  $M_n$ .

We will see in Chapter 2 how retracing the pathway is the only mechanism by which a prime divisor  $p$  divides a collection of Mersenne numbers. In that collection, the smallest index  $(p - 1)/x$  is the only one that has a chance of being prime. So, telescoping is the only chance that any prime  $p$  has of dividing a Mersenne number with a prime index. Every time a Mersenne candidate is eliminated from being prime, this telescoping behaviour is the cause.

In the bulk of this thesis, we explore the nature of telescoping, to shed light on the structures behind *all* composite Mersenne numbers  $2^n - 1$ , especially those with prime  $n$  — the intriguing Mersenne candidates. Instead of looking at what makes Mersenne numbers prime, this is the other side: what makes Mersenne numbers composite.

We will use several visual approaches to explore the nature of Mersenne composites, while bringing in supplemental tools when helpful, for rigorous mathematical proof.

The remaining content of the thesis is as follows. Each chapter has its own flavour.

In Chapter 2, we explore the divisors of Mersenne composites. 2.1 will focus on our circle diagrams and their illustrative application to group theory in general, and Mersenne composites in particular. 2.2 introduces the use of binary notation to represent Mersenne numbers, where we see proofs for a composite index  $n$  implying a composite  $M_n$ , showing the strengths of binary notation. 2.3 extends the binary notation summation method to form a binary algorithm, showing the



smallest Mersenne number a given odd number divides. 2.4 takes a closer look at prime divisors  $p$  of Mersenne numbers, looking at the forms  $p$  may take to produce different ways of telescoping. 2.5 takes a look at composite divisors  $d$  of Mersenne numbers, where we narrow down the possible Mersenne numbers divisible by  $d$  based on  $d$ 's prime factorization.

In Chapter 3, we formally present the Lucas-Lehmer primality test, complete with a proof of sufficiency and a proof of necessity. This chapter is the most advanced, and we recommend some corequisite research topics to the reader at the start. We merge the two proofs from different sources, outlining the connection between their approaches and providing background calculations for their development.

In Chapter 4, I relay the community engagement aspect of my work this year, changing tone to the first person singular to express my experience. 4.1 covers a video I created about Fermat's little theorem for a music composer, presenting circle diagrams as a metaphor for one's lot in life. 4.2 shows a slide presentation introducing Mersenne primes for a highschool enrichment outreach project. 4.3 shows my postgraduate research poster for the University of Kent postgraduate conference at the end of the year. Finally, 4.4 discusses a yarn-art activity of crafting the cardioid circle diagrams that fellow students, teachers, and friends have expressed interest in.

In Chapter 5, the closing thoughts, we close with commentary on Mersenne numbers as rich ground for further exploration in many forms.

## Chapter 2

# Explorations of Mersenne Numbers and Their Divisors

We can think poetically of Mersenne numbers  $2^n - 1, n \in \mathbb{N}$ , as a fantastical scoop of semi-sparkling paydirt. Some Mersenne numbers are composite, and some Mersenne numbers are prime, and the primes are highly sought after, mostly for the excitement of discovering one. They are the metaphorical gold particles in this metaphor, all with prime exponent  $n$ . Amid the sparkling Mersenne primes, there are other sparkling Mersenne numbers that are difficult to distinguish from the gold at first glance. These are Mersenne composites that also have a prime exponent  $n$ , like the Mersenne primes do. The prime  $n$  is what catches our attention. Such sparkling Mersenne numbers with prime  $n$  are titled Mersenne candidates.

The Mersenne numbers with composite  $n$  make up the rest, and are known to be composite themselves, as we will see. They can be quite beautiful themselves.

In order to narrow down to true gold, we could restrict our consideration to the sparkling ones — the Mersenne candidates  $2^n - 1$  with prime  $n$  — and filter those. This is how the Lucas-Lehmer primality test is used, which we will see in the next chapter.

In this chapter, we take a wider approach. Rather than targeting the gold ones, our approach is to actively exclude them. The bulk of our explorations filter out Mersenne primes with a sieve of Eratosthenes approach.

The sieve of Eratosthenes, a sieve for all primes, identifies all possible composites by selecting multiples of all possible divisors, leaving only primes behind. It is panning for gold, with numbers. In our customized sieve, we will be able to look at every possible divisor of any Mersenne number, consider the collection of Mersenne numbers that each one divides, and therefore involve all Mersenne composites in our discussion, including both those with prime  $n$  and those with composite  $n$ .

Our guiding principle for this chapter is to identify patterns for various types of divisors, taking steps toward understanding the nature of telescoping, that we saw in Chapter 1, painting a more comprehensive view of Mersenne composition.

## 2.1 Interpreting the Circle Diagrams

In Chapter 1, we have traced consecutive powers of 2 on some example “clocks” with circumference  $d$ , working in modulo  $d$ , employing the tools of modular arithmetic. In this Chapter, we are pleased to implement tools of group theory, which the reader is encouraged to reference outside of this thesis. Without going into full definitions, here are some contextual highlights.

In group theory, there are collections known as groups, rings, and fields, with qualifiers on each, for the types of objects they contain and the manners in which the objects interact. Every ring is a type of group, and every field is a type of ring and therefore also a type of group.

Working in modulo  $d$ , as we have been up until now, translates into working in a **residue ring**  $\mathbb{Z}/d\mathbb{Z} = \mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$ , with a total of  $d$  residues, also known as equivalence classes or elements. Notably, the term “residue” here is a synonym for “remainder”, in reference to modular arithmetic.

Working in modulo  $p$ , where  $p$  is prime, translates into working in a special kind of residue ring: a **finite field**  $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ , with a total of  $p$  residues, likewise also known as equivalence classes or elements.

We will see the term **multiplicative group** referenced as well, when we want to specify a group whose operation is a form of multiplication rather than addition. The residue rings  $\mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$  have both modular addition and modular multiplication defined on them, but when viewed as groups, they are groups under modular addition. When working with their elements, we will sometimes make multiplicative groups, to help us further understand the powers of 2 we are interested in.

The set of all invertible elements in a group  $G$  form a multiplicative subgroup, denoted  $G^*$ . For example, the set of invertible elements in  $\mathbb{F}_p$  include all of them except for the element 0. So,  $\mathbb{F}_p^* = \{1, 2, 3, \dots, p-1\}$ .

We will define the **generative path** of an element  $a$  in a group  $G$  as the list of elements that  $a$  visits when the group operation is applied to  $a$  repeatedly. We can denote such repeated operations as powers,  $a^n$ .

In a group  $G$ , the **order of an element**  $a \in G$ , denoted  $\text{ord}(a)$ , if the order exists, is the smallest number  $s$  that yields  $a^s = I$ , the identity element.

The **order of a group**  $G$ , denoted  $\text{ord}(G)$ , is the size of the group, telling how many elements are in it.

Narrowing in on our areas of interest, in the residue ring  $\mathbb{Z}_d$ , the generative multiplicative path of  $a$  shows all the powers of  $a$ . If this path returns to the identity element  $a^0 = 1$ , then the element  $a$  has generated a cyclic group  $\langle a \rangle$  made up of all the elements in the path. When this happens,  $a$  is the generative element of that cyclic group  $\langle a \rangle$ , and it has  $\text{ord}(a)$  elements in it.

It is now simple to apply these concepts to Mersenne numbers. The generative multiplicative path of  $2 \in \mathbb{Z}_d$  gives us the scribbled path of consecutive powers of 2 in a circle of circumference  $d$ . We have seen in Chapter 1 that when the path



returns to the value 1 on the circle, the path has drawn the representation of a Mersenne number  $M_n = 2^n - 1$ , and has visited a total of  $n$  points on the circle. In our group theory terminology, we see that if the generative multiplicative path of 2 revisits the element 1, then  $\langle 2 \rangle$  is the cyclic multiplicative group generated by the element 2, and it has  $\text{ord}(2) = n$  elements in it.

We will see more about all of this shortly.

Now, in addition to Fermat's little theorem, which we saw in Chapter 1, we will make frequent use of the following theorems in number theory.

**Theorem 2.1** (Euler's totient theorem). *Given  $d, a \in \mathbb{N}$  with  $\gcd(a, d) = 1$ ,*

$$a^{\varphi(d)} \equiv 1 \pmod{d},$$

*where the **totient** of  $d$ ,  $\varphi(d)$ , states how many integers in  $\mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$  are coprime to  $d$ .*

Euler's totient theorem, also known as Euler's theorem, is a more powerful version of Fermat's little theorem.

To obtain the totient of a given number, **Euler's totient function** [17, pg 9], also known as Euler's phi function, can be calculated as follows. Given the prime factorization of  $d = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_{\Omega}^{\varepsilon_{\Omega}}$ ,

$$\varphi(d) = (p_1 - 1)(p_1^{\varepsilon_1 - 1})(p_2 - 1)(p_2^{\varepsilon_2 - 1}) \dots (p_{\Omega} - 1)(p_{\Omega}^{\varepsilon_{\Omega} - 1}).$$

The totient  $\varphi(p)$  equals  $p - 1$  when  $p$  is prime, which gives us Fermat's little theorem.

For our purposes with Mersenne numbers, Euler's theorem tells us that the Mersenne number  $2^{\varphi(d)} - 1$  is divisible by  $d$  when  $\gcd(2, d) = 1$ , that is, when  $d$  is odd. This is great. Euler's theorem gives us a formula we can use for any of our odd divisors, no longer restricted to the odd prime ones.

**Theorem 2.2** (Lagrange's theorem). *Let  $G$  be a multiplicative group of order  $d$ , and  $a \in G$ . Then the order of the element  $a$  divides  $d$ .*

From Lagrange's theorem, we get that the order of an element  $a$  in a group  $G$  will divide the order of the multiplicative subgroup comprising its invertible elements,  $G^*$ . Notationally, we know that  $\text{ord}(a) \in G$  will divide  $\text{ord}(G^*)$ .

To find the order of the element  $2 \in \mathbb{Z}_d$  numerically, it is standard practice [7, pg 35] to use the same method we use for the circles: go through powers of 2 one at a time until we return to the element 1.

Lagrange's theorem [17, pg 164] provides us confirmation about telescoping:

In  $\mathbb{F}_p$  with prime  $p$ , the set of invertible elements  $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$  forms a multiplicative group of order  $p - 1$ . The set of powers of any given element  $a \in \mathbb{F}_p^*$  form a multiplicative subgroup  $\langle a \rangle$  of  $\mathbb{F}_p^*$ . The order of each such subgroup  $\langle a \rangle$  is the order of the element  $a \in \mathbb{F}_p$  that generates it, and  $\text{ord}(a)$  must divide  $p - 1$ . So, for every non-zero element  $a \in \mathbb{F}_p$ , we have  $\text{ord}(a) = \frac{p-1}{x}$ , for some telescoping factor  $x \in \mathbb{N}$  that depends on  $p$  and  $a$ .

Pertaining to our investigation of Mersenne numbers, given a prime  $p$ , the order of  $2 \in \mathbb{F}_p$  equals the index  $n$  of the smallest Mersenne number  $2^n - 1$  divisible by  $p$ . So, the smallest Mersenne number that a given prime  $p$  divides is  $2^{\text{ord}_p(2)} - 1 = 2^{p-1/x_p} - 1$  for some telescoping factor  $x_p$  specific to  $p$ .

The same principle can be said of residue rings  $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$  with  $d \in \mathbb{N}$ , whether prime or composite. If the pathway of an element  $a \in \mathbb{Z}_d$  returns to the element 1 before visiting all  $\varphi(d)$  elements possible, it does so by telescoping; that is, it does so in a fractional  $n = \varphi(d)/x$  number of steps, where  $x \in \mathbb{N}$  is the telescoping factor that depends on  $d$  and  $a$ .

Regarding Mersenne composites, given  $d$  such that  $\gcd(2, d) = 1$  (so for any odd number  $d$ ), the smallest Mersenne number that  $d$  divides is  $2^{\varphi(d)/x_d} - 1$ , for some telescoping factor  $x_d$ . Since  $\varphi(d)$  is dependent on the prime factorization of  $d$ , we expect the particular telescoping factor  $x_d$  will depend on the telescoping factors

$x_{p_1}, x_{p_2}, \dots$  of those primes in  $d$ 's factorization. We will look at this in section 2.5: Composite Divisors.

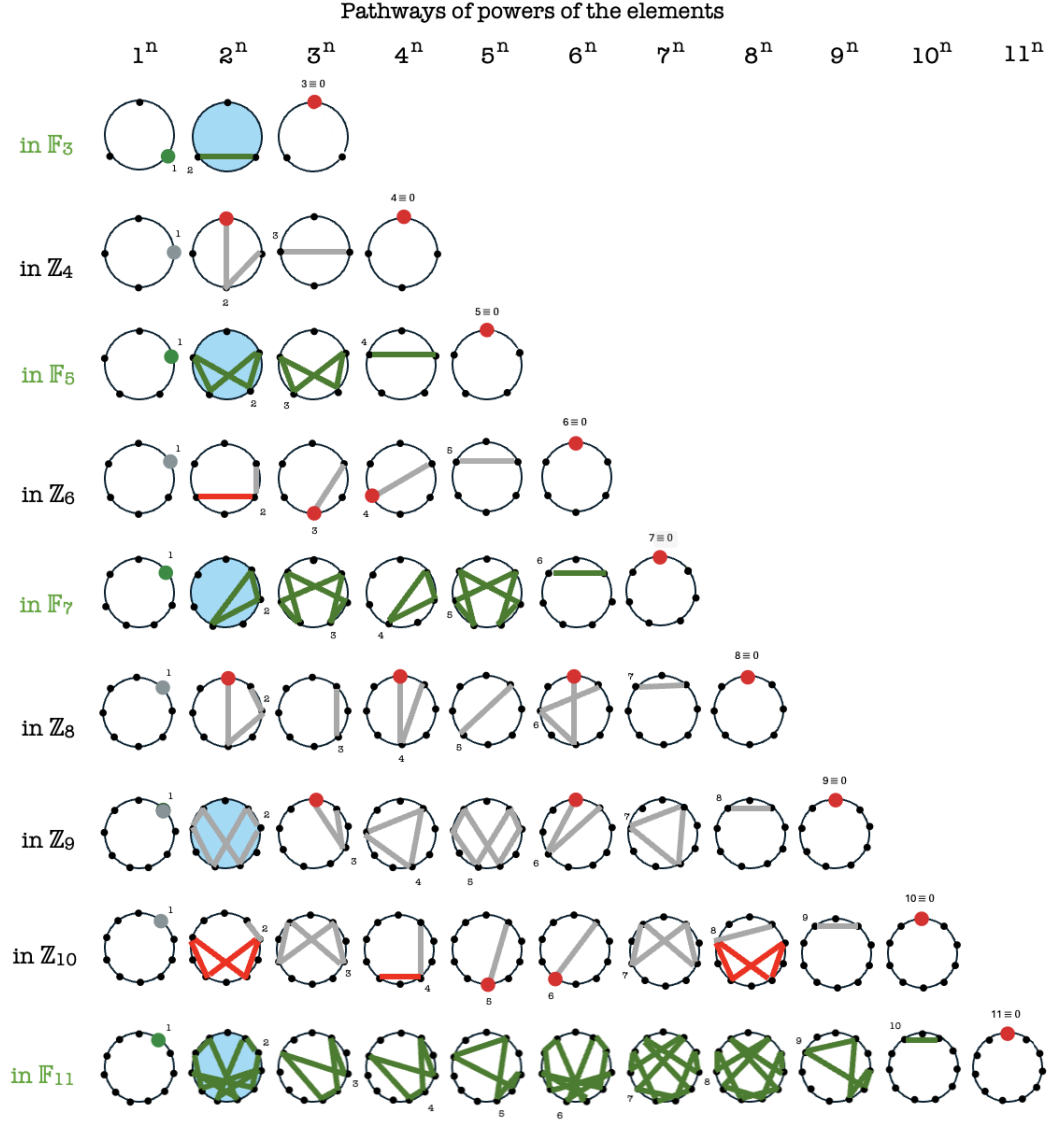


FIGURE 2.1: Some select residue rings (in rows) and their elements (in columns), showing the progression of powers of each element in each ring. We see some paths fail to return to the identity 1 and instead become trapped in a repeat loop elsewhere (in red). Rings with a prime number of elements are marked as finite fields (in green). Filled circles (in blue) show paths of the element 2 in rings of odd orders, where Mersenne numbers are relevant.

To see how our circle diagrams operate in a group theory context, we observe various residue rings and the pathways of powers of the elements they contain. [Figure 2.1]. We put the element  $0 \equiv d \in \mathbb{Z}_d$  at the end of each row for easy navigating at a glance. These circles for the powers of 0 could just as easily

go at the beginning of each row, to align with the standard residue list  $\mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$ . Note that when  $d$  is prime, we get a finite field, denoted on the diagram as  $\mathbb{F}_d$  instead of  $\mathbb{Z}_d$ .

These circle diagrams illustrate a few core properties of groups, rings, and fields:

1. The totient concept is visible. We see that when an element  $a$  of one of these residue rings shares a common factor with the total number of elements  $d$  in the ring, the generative path of  $a$  does not return to the element 1, and is instead marked red where it cycles elsewhere. Again, the totient of  $d$  is the number of integers in  $\mathbb{Z}_d$  that are coprime to  $d$ , so we can count them in each row by skipping the circles with red in them. When the total number of elements in the ring is a prime  $p$ , we see clearly that the totient of  $p$  is  $p-1$ .
2. The generative path of an element and the generative path of its multiplicative inverse trace identical pathways, merely in opposite directions. Travelling one way on a given path, we are multiplying by an element. Travelling the other way, we are multiplying by its inverse element.
3. Within each circle where the generating element  $a$  is coprime to the total number of elements  $d$ , the multiplicative inverse element  $a^{-1}$  is easy to spot. The elements  $a^{-1}$  and  $a$  are found one step to and from the element 1 respectively. Notice that, on a generative path for the element 2, the element  $\frac{1}{2}$  always takes the same spot on the circle: just past half-way around the circle.
4. Excluding the circle at the end of a given list, a pair of circles that show multiplicative inverses to each other (with the same pathways) have mirrored placement in the list to their negative counterparts, and that pair of counterparts are multiplicative inverses of each other. For example, in  $\mathbb{F}_{11}$ , if we exclude the circle at the end of the row showing the path of the element 11, we find the pathways of 3 and 4 match, and we compare them with  $8 \equiv -3$  and  $7 \equiv -4$  to find that their pathways also match.

5. More specifically, given an element  $a$  with a generative path that returns to the element 1 (for example,  $3 \in \mathbb{F}_{11}$ ), the circle showing the generative path of its multiplicative inverse  $a^{-1}$  (for example, 4) has mirrored placement with the circle showing the multiplicative inverse of its negative:  $(-a)^{-1}$  (for example, 7). We see some of the nature of  $a$  and  $-a$ . This becomes even more visually apparent when we strategically hide duplicate circles, leaving only one of each kind uncovered (for example, in the row for  $\mathbb{F}_{11}$ , hide the circles for elements 4, 5, 6, and 7).
6. Euler's theorem is visible ( $a^{\varphi(d)} \equiv 1 \pmod{d}$  where  $\gcd(a, d) = 1$ ), and therefore Fermat's little theorem as well, with the added nuance of visible telescoping.
7. Lagrange's theorem is visible (the order of an element in a group divides the order of the group.) Displayed here, the number of lines in  $\langle a \rangle$ 's generative path equals the order of that subgroup  $\langle a \rangle$ . As observed a moment ago, we see the number of lines in the path of an element  $a \in \mathbb{F}_p$  divides  $(p - 1)$ . Likewise, the number of lines in the path of an element  $a \in \mathbb{Z}_d$  divides  $\varphi(d)$ .
8. Primitive roots are easy to spot. A pathway that reaches every node but 0 shows the generative path of a primitive root  $r$  where  $\langle r \rangle = \mathbb{F}_p^*$ .

When we look at circles with generative paths of the element 2 — the diagrams of Mersenne number divisibility — here are some properties to keep in mind, some of which we have already seen.

1. The order of 2:  $\text{ord}(2) \in \mathbb{Z}_d$ , is the number of elements visited by the path from 1 back to 1. The order always exists when  $d$  is odd, because then  $\gcd(2, d) = 1$ . This number  $\text{ord}(2) \in \mathbb{Z}_d$  is the index  $n$  of the smallest Mersenne number  $2^n - 1$  divisible by  $d$ .
2. Symmetry. When the generative path of the element 2 reaches the element -1, the pathway proceeds to mirror every move it made from the element 1,

creating a symmetrical pathway made of an even number of lines. In this case, the index  $n$  of the smallest Mersenne number divisible by  $d$  is even, so, with a composite index  $n$ , this Mersenne number  $2^n - 1$  was not a Mersenne candidate.

3. Telescoping. At the end of Chapter 1, we claimed that every Mersenne candidate has a prime index due to telescoping. This is because, without telescoping, the index  $n$  of the smallest Mersenne number divisible by odd divisor  $d$  is  $\varphi(d)$ , the totient of  $d$ . From Euler's totient formula, we know that  $\varphi(d)$  has at least one factor  $(p_1 - 1)$ , where  $p_1$  is one of the odd prime factors of  $d$ , and we know such a  $(p_1 - 1)$  factor must be even, making the index  $n$  even. The resulting Mersenne number  $2^n - 1$  cannot have been a Mersenne candidate. Any larger Mersenne number divisible by  $d$  must have an index  $\mu n$  that is a multiple of that smallest index  $n$  (where the path repeats itself some number of times on the circle). This index is also even. So, without telescoping, we do not find a Mersenne candidate.

## 2.2 Binary Notation and Proof that Composite $n$ Implies Composite $M_n$

In binary notation, a power of two,  $2^n$ , is written as a 1 followed by  $n$  0s. So, a Mersenne number  $M_n = 2^n - 1$  in binary is a string of  $n$ -many 1s. This is another way for us to see that a Mersenne number  $M_n$  is always a sum of consecutive powers of 2, starting with  $2^0$ .

$$\begin{array}{ccc}
 \begin{array}{c} \text{binary} \\ \text{notation} \end{array} & & \begin{array}{c} \text{binary} \\ \text{notation} \end{array} \\
 2^5 = 100000 & & 2^5 - 1 = 11111 \\
 \text{5-many 0s} & & \text{5-many 1s} \\
 \text{Mersenne} & & \\
 \text{number} & & 
 \end{array}$$

FIGURE 2.2: Example of binary notation with  $n = 5$

With such a convenient structure, we can use binary arithmetic to explore Mersenne numbers in more depth. Incidentally, writing Mersenne numbers in binary gives us an instant proof for why Mersenne numbers  $M_n$  with composite index  $n$  are themselves composite.

Let  $n \in \mathbb{N}$  be composite, so that  $n = uv$  for some proper factors  $u, v \in \mathbb{N}$ . We take  $12 = (6)(2)$  as an example [Figure 2.3].

	<b>n</b>	=	<b>( u )( v )</b>
<b>Illustrative example</b>	<b>12</b>	=	<b>( 6 )( 2 )</b>

FIGURE 2.3: A clear outline of which variable is which, for our example

Then the Mersenne number  $M_n$ , when written in binary, is a string of  $n$  1s. Notice those  $n$  1s are  $u$  groups of  $v$  1s each. In our example, we have 6 groups of 2 1s each [Figure 2.4]. The proof would now be obvious if we were used to looking at binary regularly.

	binary notation	
<b>M<sub>12</sub></b>	=	<b>11, 11, 11, 11, 11, 11</b>
Twelve 1s		6 groups of 2 each

FIGURE 2.4: This is analogous to looking at the number 333333 in base ten and knowing it is divisible by 3.

	11	=	$M_2 \times 2^0$
	11 00	=	$M_2 \times 2^2$
	11 00 00	=	$M_2 \times 2^4$
	11 00 00 00	=	$M_2 \times 2^6$
	11 00 00 00 00	=	$M_2 \times 2^8$
+	11 00 00 00 00 00	=	$+ M_2 \times 2^{10}$
<hr/>		<hr/>	
	11,11,11,11,11,11	=	$M_2 \times (2^{10} + 2^8 + 2^6 + 2^4 + 2^2 + 2^0)$

FIGURE 2.5: A breakdown of the binary arithmetic involved in our example, using traditional column addition.

Without loss of generality, using our example as a guide [Figure 2.5], we re-write  $M_n$  as a sum:

$$\begin{aligned} M_n &= \sum_{j=1}^u (M_v)(2^{v(u-j)}) \\ &= (M_v) \sum_{j=1}^u (2^{v(u-j)}). \end{aligned}$$

So,  $M_n$  is divisible by  $M_v$ , and is therefore composite. ■.

The fact that  $M_n$  is composite when  $n$  is composite can also be shown using the **difference of powers formula**:

$$A^n - B^n = (A - B) \sum_{j=1}^n A^{n-j} B^{j-1}.$$

In our use of the formula,  $u$  takes on the role of the power. So:

$$\begin{aligned} M_n &= 2^n - 1 \\ &= (2^v)^u - 1^u \\ &= (2^v - 1) \sum_{j=1}^u (2^v)^{u-j} \\ &= (M_v) \sum_{j=1}^u (2^{v(u-j)}). \end{aligned}$$

Just as before, we see that  $M_n$  is divisible by  $M_v$ , and is therefore composite. ■.

Although the difference of powers formula is notationally concise, the mechanism of binary arithmetic gives us a visual advantage, showing us how these particular divisors  $M_v$  of  $M_n$  operate, and what their **buddy divisors**  $b$  are, such that  $M_v b = M_n$  [Figure 2.6].



$$\begin{array}{rcccc}
& & 11 & & \\
& & 11\ 00 & & \\
& & 11\ 00\ 00 & & \\
& & 11\ 00\ 00\ 00 & & \\
& & 11\ 00\ 00\ 00\ 00 & & \\
+ & 11\ 00\ 00\ 00\ 00\ 00 & & & \\
\hline
11,11,11,11,11,11 & & & & \\
\end{array}
\quad
\begin{array}{rcccc}
& & 111 & & \\
& & 111\ 000 & & \\
& & 111\ 000\ 000 & & \\
+ & 111\ 000\ 000\ 000 & & & \\
\hline
111,111,111,111 & & & & \\
\end{array}
\quad
\begin{array}{rcccc}
& & & 1111 & \\
& & & 1111\ 0000 & \\
& & & 1111\ 0000\ 0000 & \\
+ & 1111\ 0000\ 0000\ 0000 & & & \\
\hline
1111,1111\ 1111 & & & & \\
\end{array}
\quad
\begin{array}{rcccc}
& & & & 111111 \\
& & & & 111111\ 000000 \\
+ & 111111\ 000000 & & & \\
\hline
111111,111111 & & & & 
\end{array}$$

FIGURE 2.6: At a glance, based on grouping twelve 1s,  $M_{12}$  has binary notation factorizations  $(11)(010101010101)$ ,  $(111)(001001001001)$ ,  $(1111)(000100010001)$ , and  $(111111)(000001000001)$ . In decimal notation, this says that 4095 has factorizations  $(3)(1365)$ ,  $(7)(585)$ ,  $(15)(273)$ , and  $(63)(65)$ . Note that these are not the only factorizations of  $M_{12}$ , but they are the only ones that feature other Mersenne numbers. Admittedly, the numbers are easier to name in decimal, but the numbers' power-of-two structures are easier to see in binary.

## 2.3 A Binary Algorithm Companion to the Circle Diagrams

We have warmed up to binary arithmetic, seeing that  $M_n$  is composite when  $n$  is composite. Our proofs give us partial insight into the divisors involved, but do not touch the question of what happens to  $M_n$  when  $n$  is prime. Let us consider the other direction; instead of looking at the Mersenne numbers  $M_n$  first, asking what numbers divide them, we will again look at divisors  $d$ , asking which Mersenne numbers they divide. This is the sieve of Eratosthanes approach. Let us look at every possible divisor of a generic Mersenne number, and extend our binary arithmetic mechanism to process it.

First, we know that any divisor of a Mersenne number must be odd, because every Mersenne number is odd. In binary, every divisor will end in 1.

Now, given any odd number  $d$ , our strategy is simple: write  $d$  in binary, and then keep adding copies of  $d$  in binary, column addition style, until we reach a binary sum made of a string of 1s. This strategy ensures that we will find, not just any Mersenne number that  $d$  divides, but the smallest Mersenne number that  $d$  divides.

To establish our process, let us see an example with  $d = 23$  [Figure 2.7].

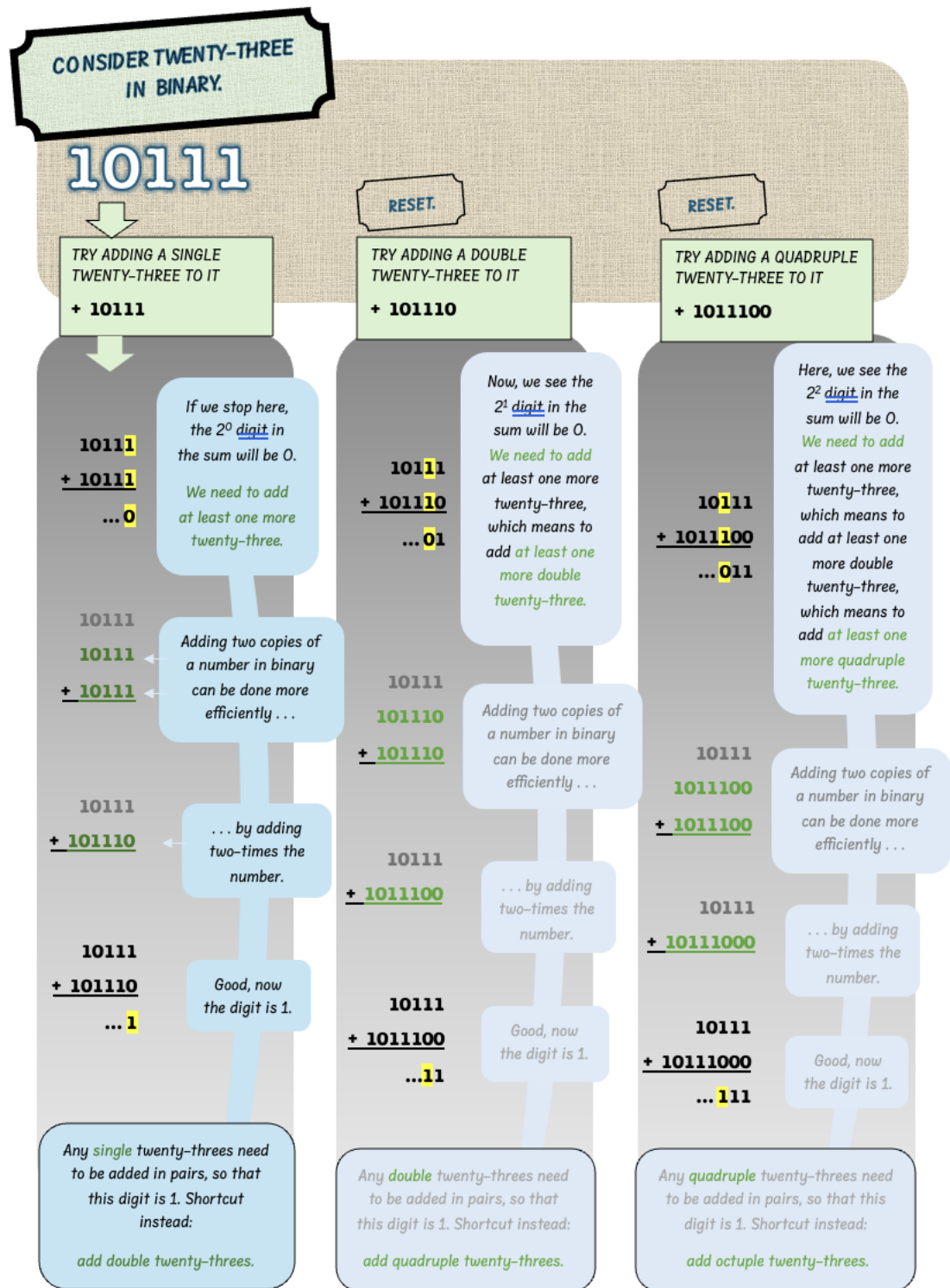


FIGURE 2.7: The rationale of our binary algorithm, using  $d=23$  as an example.

We know that we will eventually reach a final string-of-1s sum with this approach,

and our algorithm will terminate. When  $d$  is prime, ( $d = p$ ), we know by Fermat's little theorem that  $p$  divides  $2^{p-1} - 1$ . More broadly, whether  $d$  is prime or composite, we know by Euler's Theorem that  $d$  divides  $2^{\varphi(d)} - 1$ . The quantity of digits in our string-of-1s sum will be  $\varphi(d)$  at most.

All we need to do is recursively evaluate the digits of the prospective sum, smallest value column to largest, and at the first sight of a 0 in the sum, add a copy of  $d$ , shifted so that its last digit, a 1, corrects the 0.

So, every new addition is equal to  $d$ , multiplied by a unique power of 2.

The smaller value 1s in the sum (starting from right to left) will be unaffected by each new addition. At each step, we know there is no smaller multiple of  $d$  we could have added without disrupting those smaller value 1s. Once a 1 is established in the sum, that column need not be touched again.

Our algorithm terminates when the sum is a string of 1s.

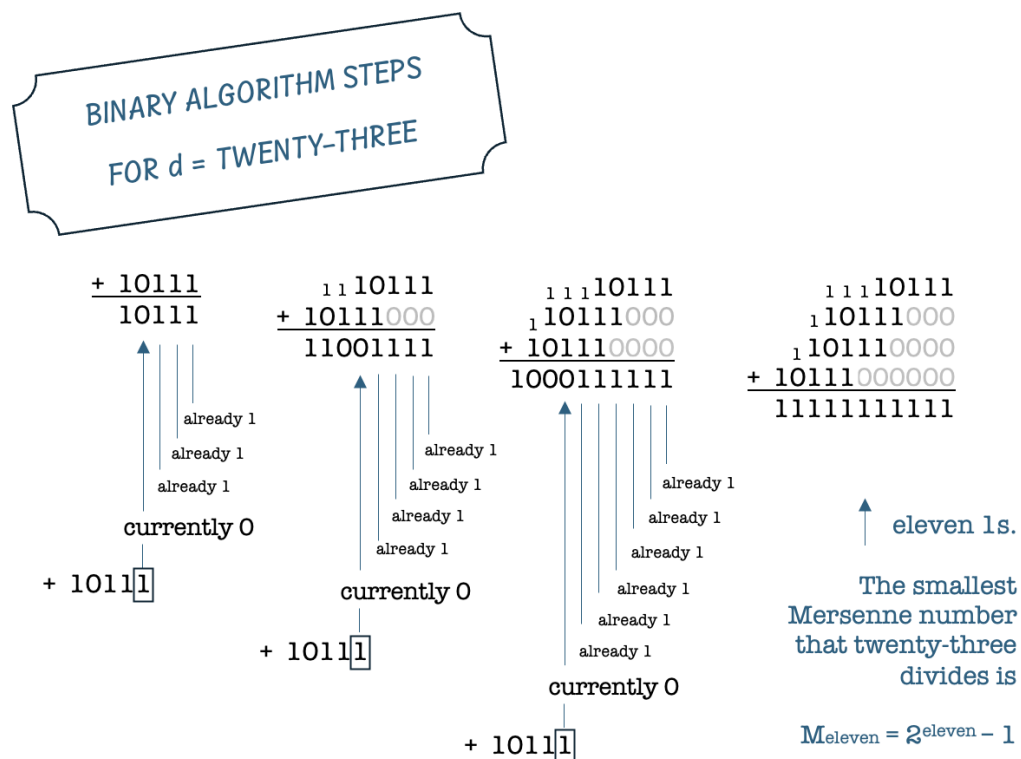


FIGURE 2.8: The binary algorithm in full, for  $d = 23$ .

To round out our binary algorithm development, consider what happens if we try to find the next Mersenne number divisible by divisor  $d$ . We would leave all the existing 1s in the sum alone, and start fresh, building another iteration of the binary algorithm array we just completed. Hence, the binary algorithm gives us the form of *every* Mersenne number that a given  $d$  divides. The naming index of any Mersenne number divisible by  $d$  needs to be a multiple  $\mu$  of the index for the smallest Mersenne number divisible by  $d$ .

Maple code for this Binary Algorithm can be found in Appendix B.

We saw that 23 divides  $M_{11}$  earlier, using the circles. The circles and the binary algorithm arrays work hand-in-hand, providing the same conclusion in different ways [Figure 2.9].

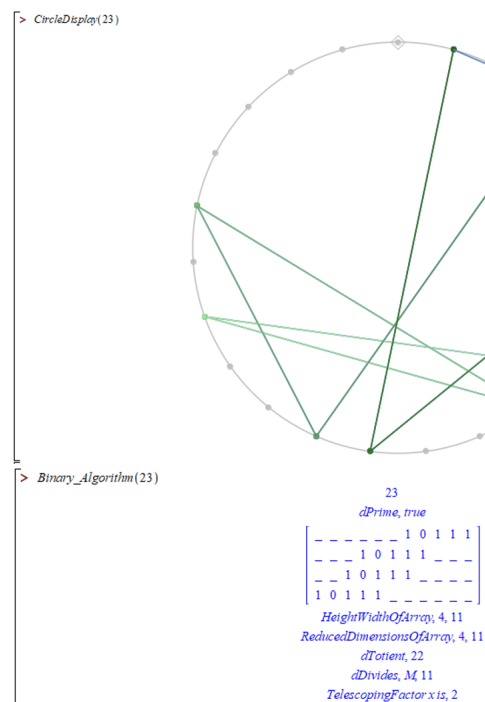


FIGURE 2.9: The circle for 23 and the binary algorithm array for 23. On the circle, eleven line segments in the path tell us the index of the smallest Mersenne number divisible by 23. On the array, its width, eleven, tells us the same. In both cases, we are looking at the sum of consecutive powers of 2 and identifying the number of terms in the sum.

Note that the circle diagrams comprise a serviceable Eratosthanes-style sieve on their own. Given an odd divisor  $d$ , we progress through the powers of 2 in  $\text{mod}(d)$ , starting with  $2^0 = 1$ , and we stop at the first moment a power of 2 arrives back

at  $1 \bmod(d)$ . The number of steps we took to get there equals the index  $n$  of the smallest Mersenne number  $M_n$  that is divisible by  $d$ .  $d$  divides all Mersenne numbers with an index that is a multiple  $\mu$  of that  $n$ . By looking at all possible divisors, one  $d$  at a time, we can sift out all Mersenne composites.

The binary algorithm sieve gives us a new perspective, with a bit of x-ray vision into the structure of Mersenne composite divisibility.

By using both visualization methods in tandem, we can uncover some other interesting patterns, which we will explore in section 2.5.

## 2.4 Prime Divisors and Mersenne Candidate Divisibility

### Quadratic Residues and Euler's Criterion

Quadratic residues are a popular topic of discussion in modular arithmetic, and consequently in group theory. We will see them employed in Chapter 3, where we prove the Lucas-Lehmer primality test. A **quadratic residue** is an element  $a$  of the residue ring  $\mathbb{Z}_d = \{0, 1, 2, \dots, d-1\}$  coprime to  $d$  such that there exists some element in  $\mathbb{Z}_d$  that squares to  $a$ . In a residue ring with prime  $d = p$ , we get our familiar finite field  $\mathbb{F}_p$ . In that case, after disqualifying  $0 \equiv p$  for not being coprime to itself, half of the remaining elements of the field  $\mathbb{F}_p$  are quadratic residues, and the other half are quadratic non-residues.

Now, in our explorations of Mersenne composites, we are not necessarily interested in whether an element of a residue ring is a square, however, there is an equation linked to quadratic residues that proves very useful to our investigation on telescoping the generative path of element 2. That equation is found in **Euler's criterion**.

**Theorem 2.3** (Euler's criterion). *Let  $p$  be an odd prime. Then*

$$a^{(p-1)/2} = \begin{cases} 0 & \text{iff } a \equiv 0 \pmod{p}, \\ 1 & \text{iff } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{iff } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Euler's criterion [17, pg 174] gives us insight into the path of 2 on our circle diagrams in  $\mathbb{F}_p$ .

To aid us further, the primes  $p$  for which 2 is a quadratic residue in  $\mathbb{F}_p$  are known [16, pg 337]. If  $p$  is an odd prime, then

$$2^{(p-1)/2} = \begin{cases} 1 & \text{if } p = 8k \pm 1, k \in \mathbb{N}, \\ -1 & \text{if } p = 8k \pm 3, k \in \mathbb{N}. \end{cases}$$

So, if  $p = 8k \pm 1$  and therefore  $2^{(p-1)/2} = 1$ , this means the pathway of powers of 2 in  $\mathbb{F}_p$  has returned to the element 1 after only half the predicted  $p - 1$  steps. So, if 2 is a quadratic residue mod  $p$ , then the path of 2 is guaranteed to telescope in  $\mathbb{F}_p$ . The smallest Mersenne number divisible by  $p$  may not be a Mersenne candidate, but it is a good place to look.

On the other hand, if  $p = 8k \pm 3$  and therefore  $2^{(p-1)/2} = -1$ , this means the pathway reaches the element -1, and so the generative path of 2 is symmetrical in  $\mathbb{F}_p$ . So, if 2 is a quadratic non-residue mod  $p$ , then the smallest Mersenne number divisible by  $p$  has an even index, and is not a Mersenne candidate.

In Appendix C of this thesis, we show the circle diagram and binary algorithm array data for all odd divisors 3-103. There are four divisors displayed on every page, one in each quadrant, so that the layout consistently shows numbers of the form  $8k + 1$ ,  $8k + 3$ ,  $8k + 5$ , and  $8k + 7$  — the last two of this list being another way of saying  $8k - 3$  and  $8k - 1$  for some  $k \in \mathbb{N}$ . The primes are in colour, and the composites in gray, for the reader to easily peruse the primes of the different forms.

**We explore primes of the form  $8k \pm 1$ .** As stated above, these are guaranteed telescoping primes. The telescoping factor  $x_p$  of such a prime  $p$  is *always even*, since the generative pathway of element  $2 \in \mathbb{F}_p$  folds in half at  $2^{(p-1)/2}$ .

Note that *sometimes* the pathways in these circles are still symmetrical because the pathway can reach -1 without contradicting that  $2^{\frac{p-1}{2}} = +1$ . For example, -1 could be at the quarter point  $2^{\frac{p-1}{4}}$ , as is the case with  $p = 17$ . When the path is symmetrical like this, the number of lines  $n$  in the path is even, and the Mersenne number  $2^n - 1$  that we see represented is not a Mersenne candidate.

Nevertheless, knowing whether a telescoping factor  $x_p$  is even or odd is useful for seeking out Mersenne candidates, as we will see from the following theorem.

**Theorem 2.4** (Divisors of Mersenne candidates). *If  $n$  is an odd prime, then any divisor of the Mersenne number  $M_n = 2^n - 1$  is of the form  $2kn + 1, k \in \mathbb{N}$ .*

A proof can be found in Rosen's textbook Elementary Number Theory and its Applications [16, pg 225].

Applying this theorem to prime divisors of any kind, we get that every prime divisor  $p$  of a Mersenne candidate  $M_n = 2^n - 1$  is  $p = 2kn + 1, k \in \mathbb{N}$ . In  $\mathbb{F}_p$ , remember that the index  $n$  of the smallest Mersenne number divisible by  $p$  is  $n = \text{ord}(2) = \frac{(p-1)}{x_p}$ . So, we get  $p = \frac{2k(p-1)}{x_p} + 1$ , yielding  $x_p = 2k$ . The theorem reveals: any prime divisor of a Mersenne candidate has an even telescoping factor.

Therefore, primes of the form  $8k \pm 1$ , which are the primes with even telescoping factors, are the only primes that divide Mersenne candidates. Not all of them do, but we see again that they are the only ones with that potential.

These prime divisors  $8k \pm 1$  overlap with some safe primes and Sophie Germain primes. A **safe prime**  $f = 2g + 1$  is a prime such that  $g$  is also prime. A **Sophie Germain prime** is a prime  $g$  such that  $2g + 1$  is also prime [3].

To organize our thoughts, we observe that, in each associated pair of primes  $g = (f - 1)/2$  and  $f = 2g + 1$ , the Sophie Germain prime is the smaller one and the safe prime is the larger. Sometimes, we can find chains of primes, where

the primes in the middle of the chains qualify as both Sophie Germain and safe primes. For example, 2, 5, 11, 23, and 47 are all primes. 2 is a Sophie Germain prime. 47 is a safe prime. 5, 11, and 23 are both Sophie Germain and safe primes.

These primes are interesting to us because of the theorem we just saw about the divisors of Mersenne candidates. To reiterate, a divisor of a Mersenne candidate  $M_n$  must be of the form  $2kn + 1, k \in \mathbb{N}$ , where  $n$  is an odd prime.

Say that  $g$  is an odd Sophie Germain prime. Then the associated safe prime  $f = 2g + 1$  is of the correct form, and might divide the Mersenne candidate  $M_g$ . What condition would guarantee that such a prime  $f$  divides  $M_g$ ? Note that  $g = (f - 1)/2$ . Well, we have just seen that every prime  $p$  of the form  $8k \pm 1, k \in \mathbb{N}$  is guaranteed to telescope with an even telescoping factor, so that such a prime will divide a Mersenne number with index  $n = (p - 1)/2$ . This is wildly promising. Can  $f$  be of the form  $8k + 1$  or  $8k - 1$ ? A quick check [Figure 2.10] shows that  $8k + 1$  is out of the question, but  $8k - 1$  can be a safe prime  $f$ .

We are on the brink of a revelation. If  $n$  is an odd Sophie Germain prime and the associated safe prime  $p$  is of the form  $8k - 1, k \in \mathbb{N}$ , then the prime divisor  $p$  divides the Mersenne candidate  $M_n = 2^{(p-1)/2} - 1$ . Amazing! We still need to check one last primality condition before we can declare this Mersenne candidate to be composite. For this Mersenne candidate to be prime instead, it would have to be the case that  $p = M_n$ . Setting  $p = M_n = 2^{(p-1)/2} - 1$  with  $p = 8k - 1$ , we derive an equation with only one solution in  $\mathbb{N}$ , namely that  $p = 7$  [Figure 2.10]. Our Mersenne candidate  $M_n = 2^{(p-1)/2} - 1$ , as long as it is not  $M_3 = 7$ , must therefore be composite! We state this as a tidy corollary:

**Corollary 2.5.** *If  $n > 3$  is an odd Sophie Germain prime and the associated safe prime  $p$  is of the form  $8k - 1, k \in \mathbb{N}$ , then the prime divisor  $p$  divides the Mersenne candidate  $M_n = 2^{(p-1)/2} - 1$ , and  $M_n$  is composite.*

Let us see a few examples from the chain of Sophie Germain and safe primes we listed earlier, to see which ones fit the template.



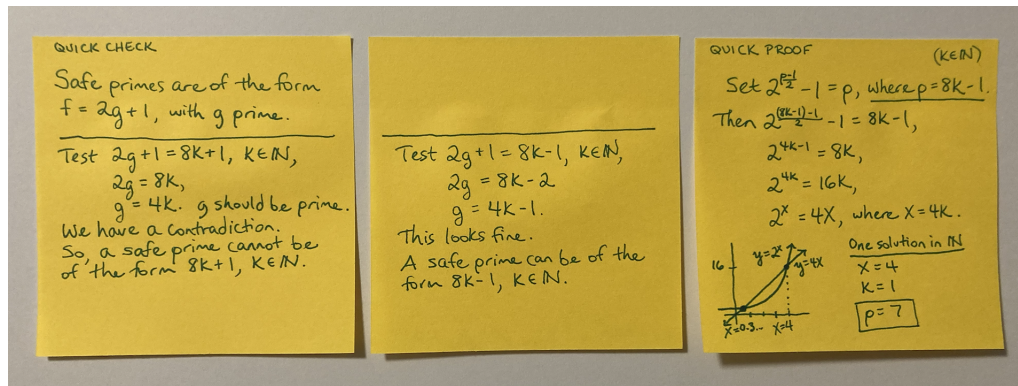


FIGURE 2.10: Some quick background calculations to help formulate Corollary 2.5.

2 is even.

$$5 = 8(1) - 3.$$

$$11 = 8(1) + 3.$$

$23 = 8(3) - 1$  is of the form  $8k - 1$ ,  $k \in \mathbb{N}$ , and is the associated safe prime to odd Sophie Germain prime 11, with  $11 > 3$ . So, we know that 23 divides Mersenne candidate  $M_{11}$ , and that  $M_{11}$  is composite.

$47 = 8(6) - 1$  is of the form  $8k - 1$ ,  $k \in \mathbb{N}$ , and is the associated safe prime to odd Sophie Germain prime 23, with  $23 > 3$ . So, we know that 47 divides Mersenne candidate  $M_{23}$ , and that  $M_{23}$  is composite.

Our classic Mersenne candidate example  $M_{11}$  is featured here, as is  $M_{23}$ . When working with Mersenne numbers for the first time, enthusiasts may notice that the first two composite Mersenne candidates are these two,  $M_{11}$  and  $M_{23}$ , and may wonder at the coincidence that the prime divisor 23 divides  $M_{11}$ . Seeing here the reason why is very satisfying.

Before we move on to discuss prime divisors of the form  $8k \pm 3$ , we must point out that our Corollary 2.5 does not describe the only conditions for a prime divisor to divide a composite Mersenne candidate. For example, we have already seen that 89 divides  $M_{11}$ , and 89 is of the form  $8k + 1$ . There is still plenty to explore and discover about composite Mersenne candidates and the primes  $8k \pm 1$  that might divide them.

**We explore primes of the form  $8k \pm 3$ .** As stated above, the power-of-two paths for all of these primes are symmetrical, since the path reaches -1 and mirrors everything that comes after 1. We would expect that none of these primes are telescoping, since the path needs to perfectly fold onto itself, and the halfway mark is already committed to landing at -1, not 1. However, there is a way.

In Appendix C, looking at the circle for  $p = 43$ , we see that it has a telescoping factor of 3. In  $\mathbb{F}_{43}$  the path visits -1 at the halfway mark of a full  $(p - 1)$  cycle, so how is it possible that  $p = 43$  is a telescoping prime? We have:

$$\begin{array}{ccccc}
 2^0 & & 2^{(p-1)/2} & & 2^{(p-1)} \\
 1 & \searrow & -1 & \nearrow & 1 \\
 \text{fixed} & & \text{fixed} & & \text{fixed.}
 \end{array}$$

So, for the path to telescope, it needs to visit -1 at least once more in the cycle, and we know the cycle must strictly repeat with no variations. So, here is what 43 does:

$$\begin{array}{ccccccc}
 2^0 & 2^{\frac{1}{6}(p-1)} & 2^{\frac{2}{6}(p-1)} & 2^{\frac{3}{6}(p-1)} & 2^{\frac{4}{6}(p-1)} & 2^{\frac{5}{6}(p-1)} & 2^{(p-1)} \\
 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
 \text{fixed} & & & \text{fixed} & & & \text{fixed.}
 \end{array}$$

Primes of the form  $p = 8k \pm 3, k \in \mathbb{N}$  cannot have even telescoping factors, but we are intrigued to see that odd telescoping factors  $x_p$  other than  $x_p = 1$  are possible. In this example, the smallest Mersenne number that 43 divides is  $M_{14}$ , and  $x_{43} = 3$ .

With some experimentation on variations of the binary notation for 43, we can find other telescoping divisors of the form  $8k \pm 3$ , and some of them are prime. In binary, 43 is 101011. It happens that the binary numbers  $10101011 = 171$ ,  $1010101011 = 683$ , and  $101010101011 = 2731$  are all telescoping divisors of the path of 2, with sizeable telescoping factors. In particular, 2731 is prime, with telescoping factor  $x_{2731} = 105$ . Looking up this pattern in the Online Encyclopedia for Integer

Sequences [2], we find that these primes overlap with Wagstaff primes [4]. This warrants further investigation in the future.

## 2.5 Composite Divisors, Squarefree and Otherwise

In this section, we explore whether we can determine the smallest Mersenne number divisible by a composite divisor  $d$ , given its prime factorization.

To start, we consider Carmichael numbers [1]. We are interested in them merely to give us a starting example.

**Carmichael numbers** are composite numbers  $d$  that satisfy Fermat's little theorem,  $a^{d-1} \equiv 1 \pmod{d}$  for every  $a$  such that  $\gcd(a, d) = 1$ . Interestingly, they are **squarefree**, meaning their prime factorization only includes each prime factor once.

Because of their connection to Fermat's little theorem, a few professors and maths enthusiasts have asked about the smallest Mersenne number that a Carmichael number divides. Let us see the binary algorithm data for input  $d = 561$ , the smallest Carmichael number [Figure 2.11].

We see that the smallest Mersenne number that Carmichael number 561 divides is  $M_{40}$ .

$561 = (3)(11)(17)$ . The smallest Mersenne numbers that each of 561's prime factors divide are  $M_2, M_{10}$ , and  $M_8$ , respectively. The Mersenne number  $M_{40}$  appears to be related to the others, and we have found a clue for how composite divisors work. 40 is the lowest common multiple of 2, 10, and 8.

In this early stage of exploration, we have a sense that our lowest common multiple clue about Carmichael number 561 could apply to all composite numbers, but for now, we see that this insight at least gives us a handle on squarefree composite divisors.

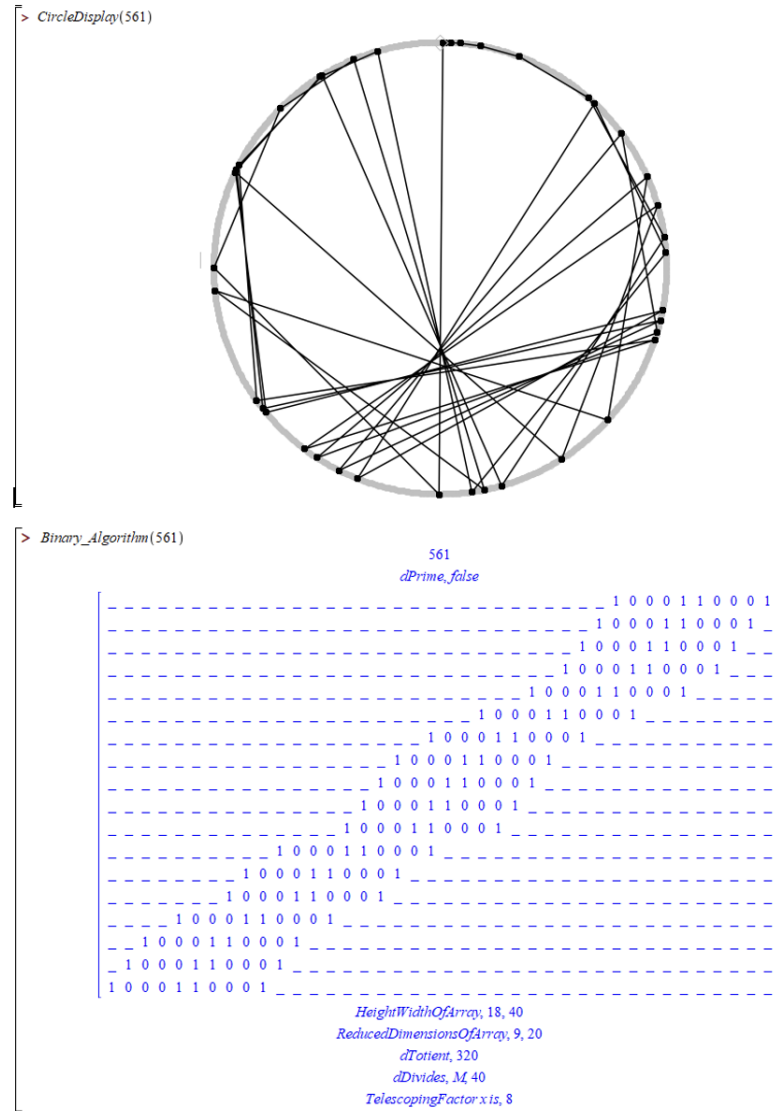


FIGURE 2.11: The circle for 561 and the binary algorithm array for 561.

Let squarefree odd divisor  $d = p_1 p_2 p_3 \dots p_\Omega$ .

Then every Mersenne number that  $d$  divides must also be divisible by each of its prime factors. This includes the smallest Mersenne number divisible by  $d$ . Take a prime factor  $p_i$  of  $d$ . That prime is odd because  $d$  is odd, and therefore divides Mersenne numbers, with indices of the form  $\mu n_{p_i}$ , with  $n_{p_i}$  being the index of the smallest Mersenne number it divides. This is the case for every prime factor of  $d$ : each one of them divides only those Mersenne numbers with indices that are multiples of the indices  $n_{p_i}$  for the smallest Mersenne number each one divides. So, the smallest Mersenne number divisible by  $d$  must have an index that is a

multiple of all of those smallest indices. Take the lowest common multiple, and we have the index for the smallest Mersenne number divisible by the squarefree odd divisor  $d$ .

Now, clearly, not all odd divisors are squarefree. We know that the smallest Mersenne number divisible by any given odd divisor  $d$  must be connected to the primes in its factorization, because all of the components involved are multiples and factors. We have seen what we can deduce from single prime factors of  $d$ . What can we deduce from its factors if they are powers of primes?

Specifically, looking at the simplest case, when  $d = p^\varepsilon$ , a power of an odd prime  $p$ , what is the smallest Mersenne number that  $p^\varepsilon$  divides, if we already know the smallest Mersenne number that  $p$  divides?

By Fermat's little theorem and Lagrange's theorem, we know that the smallest Mersenne number divisible by  $p$  is  $M_{(p-1)/x_p}$ , with  $x_p \in \mathbb{N}$  unique to  $p$ .

By Euler's theorem, we know that the prime power  $p^\varepsilon$  divides Mersenne number  $M_{\varphi(p^\varepsilon)} = M_{(p-1)(p^{\varepsilon-1})}$ , but we do not yet know whether this is the *smallest* Mersenne number that  $p^\varepsilon$  divides. Fortunately, we can see at least how  $p$ 's telescoping factor  $x_p$  incorporates into a particular Mersenne number that  $p^\varepsilon$  divides.

**Proposition 2.6:** *Let  $p$  be an odd prime such that the smallest Mersenne number divisible by  $p$  is  $M_{\frac{p-1}{x_p}}$ , with  $x_p \in \mathbb{N}$  unique to  $p$ . Then, for all  $\varepsilon \in \mathbb{N}$ ,  $p^\varepsilon$  divides  $M_{\frac{\varphi(p^\varepsilon)}{x_p}} = M_{\frac{(p-1)(p^{\varepsilon-1})}{x_p}}$ .*

Proof is by induction on  $\varepsilon$ .

For our base case, when  $\varepsilon = 1$ ,  $p$  divides  $M_{\frac{p-1}{x_p}}$ , which is already of the form proposed.

For our induction case, we want to show that if the proposition is true for some  $p^\varepsilon, \varepsilon \in \mathbb{N}$ , then it is true for  $p^{\varepsilon+1}$ .

Given that odd prime  $p$  divides Mersenne number  $M_{\frac{p-1}{x_p}}$ , with  $x_p \in \mathbb{N}$  unique to  $p$ , and given that it is the smallest Mersenne number  $p$  divides, suppose that  $\varepsilon = e$  for some  $e \in \mathbb{N}$  such that  $M_{\frac{(p-1)(p^{e-1})}{x_p}} = p^e b$ , with  $b \in \mathbb{N}$ .

Then, by repeated use of the difference of powers formula,

$$\begin{aligned}
 M_{\frac{(p-1)(p^e)}{x_p}} &= 2^{\frac{(p-1)(p^e)}{x_p}} - 1 \\
 &= \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} \right)^p - (1)^p \\
 &= \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} - 1 \right) \left( \sum_{j=1}^p \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} \right)^{p-j} \right) \\
 &\quad \text{There are } p \text{ terms in the } \sum \text{ sum. We can leverage this.} \\
 &= \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} - 1 \right) \left( \sum_{j=1}^p \left[ \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} \right)^{p-j} - (1)^{p-j} + 1 \right] \right) \\
 &\quad \text{Factor the nested difference of powers. Substitute in } p^e b. \\
 &= (p^e b) \left( \sum_{j=1}^p \left[ (p^e b) \sum_{i=1}^{p-j} \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} \right)^{p-j-i} \right] + p \right) \\
 &= (p^{e+1} b) \left( (p^{e-1} b) \sum_{j=1}^p \left[ \sum_{i=1}^{p-j} \left( 2^{\frac{(p-1)(p^{e-1})}{x_p}} \right)^{p-j-i} \right] + 1 \right).
 \end{aligned}$$

So, if some  $p^e$  divides  $M_{\frac{(p-1)(p^{e-1})}{x_p}}$ , then  $p^{e+1}$  divides  $M_{\frac{(p-1)(p^e)}{x_p}}$ .

We conclude that Proposition 2.6 is true for every  $\varepsilon \in \mathbb{N}$ . ■

We would have liked to also have proven that this Mersenne number,  $M_{\frac{(p-1)(p^{\varepsilon-1})}{x_p}}$  is the smallest one divisible by  $p^\varepsilon$ . This would have led to a definitive formula for the smallest Mersenne number divisible by any composite divisor  $d$ , provided we knew all the telescoping factors of the primes in  $d$ 's prime factorization. It would also have meant that no incrementally larger prime power  $p^{\varepsilon+1}$  could divide the smallest Mersenne number divisible by prime power  $p^\varepsilon$ . Unfortunately, or perhaps fortunately for surprise's sake, there is at least one counterexample,  $p^2 = 1093^2$ , which divides Mersenne number  $M_{364}$ , the smallest Mersenne number divisible by prime  $p = 1093$  itself.

A consequence of  $p^{\varepsilon+1}$  never dividing the smallest Mersenne number that  $p^\varepsilon$  divides would have been that every Mersenne candidate is squarefree. To see why, say that

a Mersenne candidate,  $M_n$  with prime  $n$ , is divisible by prime  $p$ . Then, because  $n$  is prime and cannot telescope any smaller,  $M_n$  is the smallest Mersenne number divisible by  $p$ . Now, if it were true that no prime power  $p^{\varepsilon+1}$  could divide the smallest Mersenne number that  $p^\varepsilon$  divides, then it would be the case that no power of  $p$  higher than  $p^1$  could be a factor of  $M_n$ , and  $M_n$  would be guaranteed squarefree.

Although it is likely the case, the question of whether all Mersenne candidates are squarefree is still an open problem [14]. It would have been so exciting to prove this way, but it is also character-building to find this way blocked.

Composite divisors have proven to be rich subject matter. We would still love to know the full answer to the question, “What is the smallest Mersenne number divisible by a composite divisor  $d$ , based on its prime factorization?” The question has unearthed some fascinating complexity, and we have found some interesting connections already. In Appendix C, where the circle and array data are housed for divisors 3-103, the composite divisors list their prime factorizations, for the reader to use at their leisure during further pattern hunting.

Overall, Mersenne numbers continue to be increasingly intriguing, and we have only begun to explore them. Divisors of Mersenne numbers come in many forms, and they all have interesting patterns and clues to them, as do the different forms of Mersenne numbers themselves. The reader is encouraged to look through the Appendices for patterns. We have harnessed binary notation as a numerical visual tool, using it to see the structure of Mersenne divisibility. We have seen prime divisors with unexpected telescoping potential, and composite divisors that challenge our expectations. A quick look at the array data in Appendix C shows that the arrays are often of dimension 1:2, which hints at the interplay between input divisors  $d$  and passive buddy divisors  $b$ . We have plenty of open fields of possibility to explore, and explore some more.

## Chapter 3

# The Lucas-Lehmer Primality Test

This chapter is written for number theory students at an undergraduate university level. It was first written for advanced high school students in a mathematics enrichment club about huge primes. In conjunction with reading this chapter, readers are encouraged to review and research material on: linear recursive sequences and characteristic roots, particularly Lucas sequences; quadratic residues and the Legendre-Jacobi symbol; and finite fields and field extensions.

The Lucas-Lehmer primality test [16, pg 226] is a cornerstone of Mersenne primality handling. It answers with certainty whether a given Mersenne candidate is prime or not. We present it here, complete with proofs of sufficiency and necessity.

**Theorem 3.1** (The Lucas-Lehmer Primality Test). *Let  $M_n = 2^n - 1$  be a Mersenne number with odd prime index  $n$ . We employ the Lucas-Lehmer sequence, defined recursively as:*

$$S_j = (S_{j-1})^2 - 2, \quad \text{with } S_1 = 4. \quad (3.1)$$

*Then  $M_n$  is prime iff  $M_n$  divides  $S_{n-1}$ .*

To run the test, given odd prime  $n$ , we would set up a routine to recursively calculate terms of the  $\{S_j\}$  sequence until attaining  $S_{n-1}$ , reducing the terms mod  $M_n$  at every step to keep their sizes manageable. If  $S_{n-1} \equiv 0 \pmod{M_n}$ , then we know  $M_n$  is prime.



After establishing some preliminaries, we will restate the sufficiency and necessity directions of the Lucas-Lehmer test as their own theorems, proving them in different but related styles.

**Outline of the sufficiency direction:** We will follow J.W.Bruce's proof [6] for the sufficiency direction. On YouTube, Fred Farrand [9] talks through Bruce's proof of sufficiency. In his video, he also shows some examples of running the test on a computer in Sage, showing the test's remarkable efficiency and capacity to test huge Mersenne candidates. Our retelling of Bruce's proof uses similar notation and framing that Bruce and Farrand use, and elaborates on the intermediate steps. Some notation is adjusted to carry smoothly into the necessity proof, but it is a retelling that follows the same content and reasoning.

Using  $\mathbb{Z}[\sqrt{3}]$  much like a parent set, we will form a related finite set,  $X$ ,

1. that involves  $M_n$  being composite, and
2. from which we can extract a multiplicative group  $X^*$  containing an element  $\omega = 2 + \sqrt{3}$ , introduced in the preliminaries section below.

From there, we will use properties of groups to produce a proof-by-contradiction, arriving at the logically-equivalent contrapositive:

If  $M_n$  is not prime, then  $M_n$  does not divide  $S_{n-1}$ .

**Outline and background of the necessity direction:** For the necessity direction, we will show a version of Rödseth's more general proof [15] of primality testing for  $N = h \cdot 2^n - 1$ , adapted to the notation established in Bruce's sufficiency half.

Rödseth handles the (non-linear) Lucas-Lehmer recursive relation (3.1) by introducing the linear recursive relation

$$V_{\ell+2} - PV_{\ell+1} + V_{\ell} = 0, \text{ with } V_0 = 2, V_1 = P,$$

such that  $\{S_j\}$  is a subsequence of the sequence  $\{V_\ell\}$ . Indeed, it is the case that

$$V_{2\ell} = V_\ell^2 - 2,$$

which strongly resembles the equation in the Lucas-Lehmer test.

The advantage of working with a linear recursive sequence is that we can work with its characteristic polynomial and characteristic roots, and find an explicit formula for it that no longer relies on recursion. This particular sequence  $\{V_\ell\}$  is a type of Lucas sequence, which is a linear recursive sequence often written in the form  $u_{n+2} = Pu_{n+1} + Qu_n$ , where  $P$  and  $Q$  are integers. From the linear recursive sequence  $\{V_\ell\}$ , we can derive the equation  $V_{2\ell} = V_\ell^2 - 2$  as follows.

We can find the explicit formula for a given linear recursive sequence by using the roots of its characteristic polynomial, in this case  $x^2 - Px + 1$ . The Berkeley Math Circle covers the method in a paper for high school student enrichment [13]. Taking  $\{V_\ell\}$ , its characteristic roots  $\lambda_1$  and  $\lambda_2$  happen to be inverses of each other, and the coefficients in its explicit formula are both 1. The explicit formula that we get for  $\{V_\ell\}$  is a very clean cut explicit formula:  $V_\ell = \lambda_1^\ell + \lambda_1^{-\ell}$ . With Euler's formula in mind:  $e^{i\theta} = \cos \theta + i \sin \theta$ , we can parametrize  $\lambda_1$  to be  $e^{i\theta}$ , to obtain  $V_\ell = e^{i\ell\theta} + e^{-i\ell\theta} = 2 \cos(\ell\theta)$ . Then, using the trig identity  $\cos(2X) = 2 \cos^2 X - 1$ , we get:

$$\begin{aligned} V_{2\ell} &= 2 \cos(2\ell\theta) \\ &= 2(2 \cos^2(\ell\theta) - 1) \\ &= 4 \cos^2(\ell\theta) - 2 \\ &= (2 \cos(\ell\theta))^2 - 2 \\ &= V_\ell^2 - 2. \end{aligned}$$

We have attained the formula that Rødseth claimed. Now, by setting  $S_1 = V_1$ , we

can experience the connection between the two sequences  $\{S_j\}$  and  $\{V_\ell\}$  term-by-term:

$$\begin{aligned} S_1 &= P = V_1. \\ S_2 &= V_1^2 - 2 = V_2. \\ S_3 &= V_2^2 - 2 = V_4. \\ S_4 &= V_4^2 - 2 = V_8. \end{aligned}$$

We see indeed that  $\{S_j\}$  is a subsequence of  $\{V_\ell\}$  with  $S_j = V_{2^{j-1}}$ , resulting in their explicit formulae being related.

Now, as we have mentioned, an explicit formula for the  $\{V_\ell\}$  sequence is found by using its characteristic roots. The characteristic roots of the linear relation for  $\{V_\ell\}$  are  $\lambda_1 = \frac{P+\sqrt{P^2-4}}{2}$  and  $\lambda_2 = \frac{P-\sqrt{P^2-4}}{2}$ , so Rödseth's proof makes heavy use of the factors of the discriminant  $D = (P+2)(P-2)$ . Additionally, the characteristic roots  $\lambda_1$  and  $\lambda_2$  equate to Rödseth's  $\alpha = \frac{(P+2+\sigma)^2}{4(P+2)}$  and  $\alpha^{-1} = \frac{(P+2-\sigma)^2}{4(P+2)}$ , with  $\sigma^2 = D$ . The Lucas-Lehmer primality test emerges when  $P = 4$ .

With this background established, we leave  $\{V_\ell\}$  behind and carry forward the salient points for our proofs. Note that, when  $P = 4$ , then  $D = 12$ , which we will jump to at the start of the necessity proof without preamble. When  $P = 4$ ,  $\lambda_1$  and  $\lambda_2$  match the upcoming numbers  $\omega$  and  $\bar{\omega}$ , helping us understand the explicit formula for  $\{S_j\}$  given in upcoming Lemma 3.2.

Similar to Bruce's approach, Rödseth specifies that we are not only working in a group, but in a field extension  $\mathbb{F}_{p^2}$ , and uses properties of quadratic residues to achieve a final calculation for  $S_{n-1} = 0$  in  $\mathbb{F}_{p^2}$ , with  $p = M_n$ .

**Preliminaries:** The proof for both directions features the following two conjugate numbers, which we denote  $\omega$  and  $\bar{\omega}$  as follows:

$$\omega = 2 + \sqrt{3}, \quad \bar{\omega} = 2 - \sqrt{3}.$$

These numbers  $\omega$  and  $\bar{\omega}$  are useful for their connection with the Lucas-Lehmer sequence  $\{S_j\}$ , as seen in Lemma 3.2 directly below. They also have a tidy format,

being elements of the set  $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ . Furthermore, notice that  $\omega\bar{\omega} = (2 + \sqrt{3})(2 - \sqrt{3}) = 4 - 3 = 1$ , so  $\omega^{-1} = \bar{\omega}$ .

**Lemma 3.2.**

$$S_j = \omega^{2^{j-1}} + \bar{\omega}^{2^{j-1}}.$$

*Proof.* Proof of Lemma 3.2 is by Induction on  $j$ .

For the initial condition, when  $j = 1$ , we get:

$$\begin{aligned} S_1 &= (2 + \sqrt{3})^{2^{(0)}} + (2 - \sqrt{3})^{2^{(0)}} \\ &= (2 + \sqrt{3}) + (2 - \sqrt{3}) \\ &= 4. \end{aligned}$$

$S_1$  is indeed set to 4, so Lemma 3.2 holds true for the initial condition.

For the induction condition, when  $S_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$  for some  $m \in \mathbb{N}$  we get:

$$\begin{aligned} S_{m+1} &= (S_m)^2 - 2 \\ &= \left(\omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}\right)^2 - 2 \\ &= \omega^{2^m} + 2(\omega\bar{\omega})^{2^{m-1}} + \bar{\omega}^{2^m} - 2 \\ &= \omega^{2^m} + 2(1) + \bar{\omega}^{2^m} - 2 \\ &= \omega^{2^m} + \bar{\omega}^{2^m}. \end{aligned}$$

So, if Lemma 3.2 is true for some  $j = m \in \mathbb{N}$ , it is also true for  $j = m + 1$ . □

To arrive at our intended group for the sufficiency proof, we will call on the following two lemmas from group theory.

**Lemma 3.3.** *Let  $X$  be a set with binary operation  $\odot$  which satisfies closure and associativity, and contains an identity element. Then the set  $X^*$  of invertible elements in  $X$  forms a group under the same operation  $\odot$ .*

*Proof.* Checking the criteria for a group in reverse of traditional order:

4. By definition,  $X^*$  only contains invertible elements under the binary operation, so there is an inverse element for every element.
3.  $X^*$  inherits the identity element from  $X$ , since the identity element is always invertible. (This also confirms for us that  $X^*$  is non-empty.)
2. The binary operation is still the same, operating on the same type of elements, so  $X^*$  inherits associativity.
1. Closure: Let  $x, y \in X^*$ . Then  $x^{-1}, y^{-1} \in X^*$  by definition. Now, consider  $x \odot y$ .  $(x \odot y) \odot (y^{-1} \odot x^{-1}) = 1$  by the rules of associativity, so, for any  $x, y \in X^*$ ,  $(x \odot y)$  is an invertible element. Therefore,  $X^*$  is closed under the binary operation  $\odot$ .

□

**Lemma 3.4.** *If  $G$  is a finite group with an element  $x \in G$ , then  $\text{ord}(x) = s$  is at most the number of elements in the group.*

*Furthermore, if  $x \in G$  and  $x^r = 1$ , then  $r$  is a multiple of  $s = \text{ord}(x)$ .*

*Proof.* Let  $G$  be a non-empty finite group. Since  $G$  is closed, every time an element  $x \in G$  has the operation  $\odot$  applied to itself, the result equals an element of  $G$ . When we start with the identity element  $I$  and repeatedly apply the operation  $\odot x$ , the number of times applied cannot exceed the total number of finite elements in the group before the result is  $I$  again. By the pigeonhole principle, we eventually run out of elements. Say we operate  $\odot x$  for a total of  $n$  times and the product is the same as an earlier result. Then  $x^n = x^{n-m}$ , where  $m < n$ . Every element of  $G$  is invertible, so we can operate both sides by  $[x^{(-1)}]^{(n-m)}$ , and we get  $x^m = I$ . Hence, to arrive at the same element of  $G$  that we already arrived at, when starting at  $I$  and repeatedly applying  $\odot x$ , we already passed the number of applications it took to arrive back at  $I$ .

Furthermore, if  $x^r = 1$ , and  $s$  is the smallest quantity such that  $x^s = 1$ , then  $x^r = 1 = 1^t = (x^s)^t = x^{st}$ . So  $r$  is a multiple of  $s$ , the order of  $x$ . □

We are ready for the meat of the sufficiency proof.

**Theorem 3.5** (Lucas-Lehmer sufficiency). *If  $M_n$  divides  $S_{n-1}$ , then  $M_n = 2^n - 1$  is prime.*

*Proof.* We will prove that if  $M_n = 2^n - 1$  is composite, then  $M_n$  does not divide  $S_{n-1}$ . This is logically equivalent to Theorem 3.5.

Let  $M_n = 2^n - 1$  be composite. Choose a prime proper factor  $q$  of  $M_n$  such that  $1 < q \leq \sqrt{M_n}$ ; that is,  $q^2 \leq M_n$ . Note that  $q$  cannot equal 2, since all numbers of the form  $M_n = 2^n - 1$  are odd. Good; the coefficients of  $\omega$  (2 and 1) will not be bothered when working in  $\text{mod } q$ .

Define a set  $X$  such that:

$$X = \{a + b\sqrt{3} : a, b \in \mathbb{Z}_q\},$$

where  $\mathbb{Z}_q$  denotes the finite field  $\mathbb{Z} \text{ mod } q$ , so  $a$  and  $b$  are any of  $\{0, 1, 2, \dots, (q-1)\}$ .

Define the multiplication of two elements of  $X$  by taking the ordinary product we outlined for  $\mathbb{Z}[\sqrt{3}]$ , and then reduce the resulting coefficients  $\text{mod } q$ . The product is in  $X$ . We see that  $X$ , under this multiplication, satisfies closure and associativity, and has an identity element. Then, by Lemma 3.3, construct a group  $X^*$  consisting of all the invertible elements of  $X$ , under the same multiplication.

Now,  $X$  was a finite set, so  $X^*$  is a finite group. By Lemma 3.4, we know that all elements of  $X^*$  have an order no greater than the total number of elements in  $X$ . Note that the total number of elements in  $X$  was  $q^2$  due to the two-term nature of every element. Note also that the element  $0 \in X$  is not invertible, and did not make it into  $X^*$ . So the total number of elements in  $X^*$  is  $q^2 - 1$  at most, and we get

$$\text{ord}(x^*) \leq (q^2 - 1), \text{ for all } x^* \in X^*.$$

Let us reprise our friend  $\omega$ , which we know is in  $X$ . Is it an element of  $X^*$ ? Yes! It is an invertible element, with familiar inverse  $\bar{\omega} = (2) + (q-1)\sqrt{3} \in X^*$ , as we can check. We want to see  $\omega\bar{\omega} = 1$ . To find the product, we remember to first multiply representatives from  $\mathbb{Z}\sqrt{3}$  whose elements are in  $\mathbb{R}$ , and then reduce the coefficients mod  $q$  at the end.

Working in  $\mathbb{Z}\sqrt{3}$ , we get:

$$\begin{aligned}\omega\bar{\omega} &= \left((2) + (1)\sqrt{3}\right) \left((2) + (q-1)\sqrt{3}\right) \\ &= [(2)(2) + 3(1)(q-1)] + [(2)(q-1) + (1)(2)]\sqrt{3} \\ &= [1 + 3q] + [2q]\sqrt{3}.\end{aligned}$$

So, working in  $X$ , we get:

$$\begin{aligned}\omega\bar{\omega} &= [1] + [0]\sqrt{3} \\ &= 1.\end{aligned}$$

Having confirmed that  $\omega$  and  $\bar{\omega}$  are elements of  $X^*$ , we return to working in  $\mathbb{R}$  for the next few calculations, leading to the payoff when we consider the result in  $X^*$ .

Now, assume, by way of contradiction, that  $M_n$  divides  $S_{n-1}$ . Then, by applying Lemma 3.2, this condition becomes:

$$M_p \text{ divides } \omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}}.$$

Algebraically:

$$\omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}} = RM_n, \quad R \in \mathbb{N}.$$

Multiplying this equation by  $\omega^{2^{n-2}}$ , we get:

$$\begin{aligned} \left(\omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}}\right) \left(\omega^{2^{n-2}}\right) &= (RM_n) \left(\omega^{2^{n-2}}\right), \\ \left(\omega^{2^{n-2}}\right)^2 + (\omega\bar{\omega})^{2^{n-2}} &= RM_n \omega^{2^{n-2}}, \\ \omega^{2^{n-1}} + 1 &= RM_n \omega^{2^{n-2}}, \end{aligned}$$

$$\omega^{2^{n-1}} = RM_n \omega^{2^{n-2}} - 1. \quad (3.2)$$

Now, by squaring, we get:

$$\omega^{2^n} = \left(RM_n \omega^{2^{n-2}} - 1\right)^2. \quad (3.3)$$

Since we have stipulated that  $q$  is a factor of  $M_n$ , we know  $M_n \equiv 0 \pmod{q}$ . Consider the middle terms in the two numbered formulae (3.2) and (3.3) above. Working in the group  $X^*$ , where we still define multiplication by multiplying and then reducing the coefficients mod  $q$ , those middle terms become  $0 + 0\sqrt{3}$  and we get:

$$\omega^{2^{n-1}} = -1, \quad (3.4)$$

and

$$\omega^{2^n} = (-1)^2 = 1. \quad (3.5)$$

From these results, we can find the order of the element  $\omega \in X^*$ . By Lemma 3.4 and formula (3.5), we know  $\text{ord}(\omega)$  divides  $2^n$ . So, our only option is for  $\text{ord}(\omega)$  to be a power of 2 (since the prime factorization of  $2^n$  is all 2s). But, by formula (3.4), when we divide  $2^{(n)}$  by a single 2, then  $\omega$  to that power is -1. To be clear, we have squared  $\omega$  a total of  $(n-1)$  times for a result of -1, and we want to know whether we could have squared  $\omega$  fewer times to achieve 1. This is impossible; if we had achieved 1 earlier and then squared at all, we would only get 1 again, never -1. We are left with the only option being  $\text{ord}(\omega) = 2^n$ .

So, from everything we have gathered:



1.  $M_n = 2^n - 1$ ,
2. We have chosen  $q^2$  to be less than or equal to  $M_n$ ,
3. The number of elements in the set  $X$  is  $q^2$ ,
4. The number of elements of the group  $X^*$  is at most the number of elements in the set  $X$ , minus the element 0, so at most it is  $q^2 - 1$ ,
5. The order of  $\omega$  is at most the number of elements of the group  $X^*$ ,
6. The order of  $\omega \in X^*$  is  $2^n$ .

In ascending quantities,

$$\text{ord}(\omega) = 2^n \leq q^2 - 1 < q^2 \leq M_n = 2^n - 1.$$

$$2^n < 2^n - 1.$$

A contradiction! Therefore, our last assumption, that  $M_n$  divides  $S_{n-1}$ , must be false. We conclude that, if  $M_n$  is not prime, then  $M_n$  does not divide  $S_{n-1}$ .

Equivalently, we have proven that if  $M_n$  divides  $S_{n-1}$ , then  $M_n$  is prime.  $\square$

Next, in the proof for the necessity direction, we consider quadratic residues mod  $p$ , employing the Legendre-Jacobi symbol  $(-)$ .

**Lemma 3.6.** *If  $p$  is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k \pm 1, k \in \mathbb{N}, \\ -1 & \text{if } p = 8k \pm 3, k \in \mathbb{N}. \end{cases}$$

A proof can be found in Rosen's textbook *Elementary Number Theory and its Applications* [16, pg 337].

**Lemma 3.7.** *If  $p$  is an odd prime, then*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p = 12k \pm 1, k \in \mathbb{N}, \\ -1 & \text{if } p = 12k \pm 3 \text{ or } p = 12k \pm 5, k \in \mathbb{N}. \end{cases}$$

This can be proven using standard properties of quadratic residues, and appears on occasion as an exercise in a University course that teaches about them. A course at Northeastern University covers a proof in the lecture notes. [8].

We are ready for the meat of the necessity proof.

**Theorem 3.8** (Lucas-Lehmer necessity). *If  $M_n = 2^n - 1$  is prime, then  $M_n$  divides  $S_{n-1}$ .*

*Proof.* Let  $p = M_n = 2^n - 1$  be prime.  $p$  is of the form  $8(2^m) - 1, m \in \mathbb{N}$ , so it is always of the form  $8k - 1$  and never of the form  $12k \pm 1$ .

Let  $\sigma = 0 + 2\sqrt{3}$ . Notice that  $\sigma^2 = 12$ .

By the multiplicity of the Legendre-Jacobi symbol, and Lemmas 3.6 and 3.7, we find:

$$\left(\frac{12}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{2}{p}\right) \left(\frac{3}{p}\right) = (1)(1)(-1) = -1.$$

Now, although 12 is a quadratic non-residue in the field  $\mathbb{F}_p$ , nevertheless we can guarantee it to be a quadratic residue in the field  $\mathbb{F}_{p^2}$ , by representing  $\mathbb{F}_{p^2}$  as:

$$\mathbb{F}_{p^2} = \{a + b\sqrt{3} : a, b \in \mathbb{F}_p\},$$

with  $\sigma$  as a member.

Now, with  $\omega = 2 + \sqrt{3}$  and  $\bar{\omega} = 2 - \sqrt{3} = \omega^{-1}$  as covered before in the sufficiency proof, and both  $\omega$  and  $\bar{\omega} \in \mathbb{F}_{p^2}$ , we reprise Lemma 3.2:

$$S_j = \omega^{(2^j-1)} + \omega^{-(2^j-1)}.$$

Observe that  $\frac{1}{2} \in \mathbb{F}_p$  because  $\gcd(2, p) = 1$ , so 2 is invertible mod  $p$ .  $\frac{1}{2}$  is acceptable and useful notation for the inverse of 2 in modular arithmetic, when the inverse exists [7]. Therefore,  $\omega = \frac{1}{2}(4) + \frac{1}{2}(2)\sqrt{3} \in \mathbb{F}_{p^2}$ . Using this, we rewrite  $\omega$  to have a square numerator:

$$\begin{aligned}
 \omega &= \frac{4}{2} + \frac{2}{2}\sqrt{3} \in \mathbb{F}_{p^2} \\
 &= \frac{4 + \sigma}{2} \\
 &= \frac{4 + \sigma}{2} \cdot \frac{2}{2} + \frac{2}{4} - \frac{2}{4} \\
 &= \frac{(6) + 2\sigma + (2)}{4} \cdot \frac{6}{6} \\
 &= \frac{(6)^2 + 2\sigma(6) + \sigma^2}{24}.
 \end{aligned}$$

So we have:

$$\omega = \frac{(6 + \sigma)^2}{24}.$$

We will observe that a power  $\frac{p+1}{2} = 1 + \frac{p-1}{2}$  of  $\omega$  equals  $\left(\frac{6}{p}\right)$ , as follows.

Consider  $(6 + \sigma)^p$  in  $\mathbb{F}_{p^2}$ . Using the binomial theorem, every term but the first and last in the summation expansion will have an uncanceled factor  $p = 0 + 0\sqrt{3} \in \mathbb{F}_p^2$ , turning all of those terms to 0. Next, we can use Fermat's little theorem with  $6 \in \mathbb{F}_p$ , and Euler's criterion with  $-1 = \left(\frac{12}{p}\right) = \left(\frac{\sigma^2}{p}\right) = (\sigma^2)^{(p-1)/2} = \sigma^{p-1} = \frac{\sigma^p}{\sigma}$  giving us  $-\sigma = \sigma^p$ , so that altogether we have:

$$\begin{aligned}
 (6 + \sigma)^p &= \sum_{j=0}^p \binom{p}{j} (6)^{p-j} \sigma^j \\
 &= 6^p + 0 + \sigma^p \\
 &= 6 + \sigma^p \\
 &= 6 - \sigma.
 \end{aligned}$$

So, in  $\mathbb{F}_{p^2}$ , we have

$$(6 + \sigma)^p = 6 - \sigma.$$

Now, by Euler's Criterion again, and by the fact that 4 is always a quadratic residue mod  $p$ , and that taking the inverse of 1 or -1 leaves the value unchanged:

$$\begin{aligned}
 \omega^{(p+1)/2} &= \left( \frac{(6 + \sigma)^2}{4 \cdot 6} \right)^{(p+1)/2} \\
 &= \frac{(6 + \sigma)^p (6 + \sigma)}{(4 \cdot 6)^{1+(p-1)/2}} \\
 &= \frac{(6 - \sigma)(6 + \sigma)}{4 \cdot 6 \cdot 4^{(p-1)/2} \cdot 6^{(p-1)/2}} \\
 &= \frac{[36 - 12]}{[24] \left( \frac{4}{p} \right) \left( \frac{6}{p} \right)} \\
 &= \left( \frac{6}{p} \right).
 \end{aligned}$$

By Lemmas 3.6 and 3.7, we have:

$$\omega^{(p+1)/2} = -1. \quad (3.6)$$

So, in  $\mathbb{F}_{p^2}$ , using Lemma 3.2 and equation (3.6):

$$\begin{aligned}
 S_{n-1} &= \omega^{2^{n-2}} + \omega^{-(2^{n-2})} \\
 &= \omega^{(2^n)/4} + \omega^{-(2^n)/4} \\
 &= \omega^{(p+1)/4} + \omega^{-(p+1)/4} \\
 &= \left( \omega^{-(p+1)/4} \right) \left( \omega^{(p+1)/2} + 1 \right) \\
 &= 0.
 \end{aligned}$$

Thus, if  $p = M_n = 2^n - 1$  is prime, then  $S_{n-1} \equiv 0 \pmod{M_n}$ .  $\square$

We have proven both the sufficiency and necessity directions of Theorem 3.1 (The Lucas-Lehmer Primality Test). This completes the proof.  $\blacksquare$ .

## Chapter 4

# Presentation Projects of Mersenne Concepts

In this chapter, I share my personal experience of presenting and discussing Mersenne composite explorations over my past year of study. Every audience has been a relatively small group of 1 to 100 individuals ranging on a spectrum of comfort levels with maths — from those who are already open and eager to dig into calculations, to those who reflexively shudder at maths, but spring to life when looking at the diagrams. This community engagement aspect of my Mersenne explorations is front-and-centre; I have chosen to work with Mersenne numbers exactly for their immediate accessibility with audiences. To my delight, audiences have responded with increasing positivity.

I have been fortunate this year to participate in several scientific communication training and outreach events, both by receiving training and by contributing myself.

Training opportunities included some full day workshops: Using the Media to Publicize your Research, and the London Mathematical Society Science Communication Seminars. Presentation opportunities included some lecture and discussion delivery: post-graduate talks to fellow post-grads, and extracurricular highschool

enrichment, including a pilot project in Canterbury secondary schools on Huge Primes [11], and Ri Royal Institute Masterclasses for Year 9 students.

Some valuable knowledge that I am now putting into practice includes:

1. \* to define your audience as specifically as possible when planning a module,
2. \* to use common language, ie, “to speak fluent human”,
3. \* to use illustrative examples,
4. \* to encourage questions and discussion,
5. \* and not to be too number-centric, but rather prioritize clarity.

The following are a series of my engagement projects that I have developed over the last year, expanding on aspects of Mersenne composites. They are designed to fuel curiosity, or to be a tool for the reader’s own investigation. I have ordered them according to topic progression.

To lead into the modules, here is a word on presenting the Chapter 1 cold open of this thesis.

**Summary:** Chapter 1 of this paper is a pointed investigation into the divisors of Mersenne composites. In the process, I introduce circle diagrams as visual tools.

**Audience:** A broad audience of the mathematically curious, generally of high-school age and above.

This past year, I have presented Mersenne explorations in three talks to fellow maths postgraduates, and in several presentations with interested friends of scientific background. The first few presentations fell flat. I could see well-meaning postgraduate listeners shifting uncomfortably in their chairs as I rattled off number theory. From their questions, I realized indirectly that number theory was a hazy memory, and they were alienated by the never-before-seen diagrams which only complicated the many variables involved.

In a fresh presentation with a friend, I led with the cold-open of Chapter 1: building a circle diagram from scratch, letting it show organically what it meant. Magic. His eyes lit up, and he continually wanted to know more. It became my essential introduction for subsequent Mersenne presentations, and one friend even asked if she could forward it to a colleague.

I am learning not to let pride get in the way of sitting with the basics for awhile, even in academic communities assessing my level of study. Everyone has a more enjoyable and often more fruitful experience when there is less pressure to be impressive.

## 4.1 Fermat's Little Theorem and Spirograph Maths

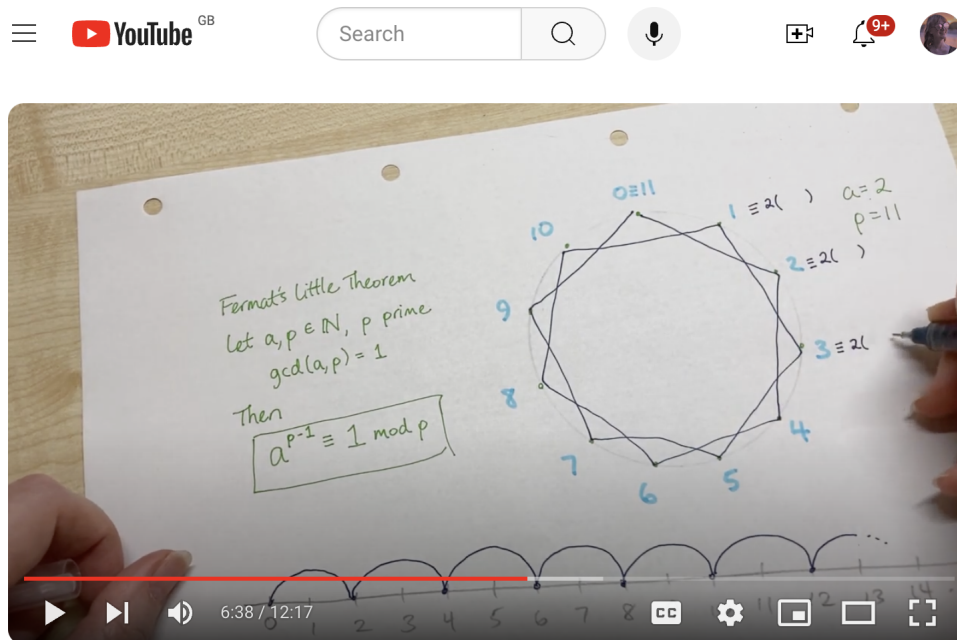
**Summary:** In support of a prominent music composer I am in contact with, I created a video [Figures [4.1](#) and [4.2](#)] to him specifically, that features a proof of Fermat's little theorem in visual terms.

**Audience:** An adult music composer, mathematically inclined, eager for knowledge

The visual nature of the proof invites play with Spirograph experiments, encouraging predictions about how many points of a star will be created by skip-counting around a circle.

## 4.2 Intro to Mersenne Primes and the Lucas-Lehmer Primality Test

**Summary:** The following powerpoint slides are designed for a 10 minute talk as part of the University of Kent Huge Primes pilot project in schools [[11](#)], headed by my supervisor, Professor Andrew Hone. I ended up giving the talk again



**Mathematical pathways: some numbers are born to +1, some to -1, all to +1 in the end**

Unlisted



Amethyst ...  
305...

Analytics

Edit video

0

Share

...

23 views 5 months ago

William Blake's poem "Auguries of Innocence" inspires a new choral work by Eric Whitacre, set to premiere at the end of 2024. In a Q&A session about composition, Eric mentioned a line of the poem that he's working through

FIGURE 4.1: <https://www.youtube.com/watch?v=emIhQUYzZJ0> My video to a music composer, employing maths as a metaphor connected to the text he was setting to music, explaining Fermat's little theorem in the process.



@EricWhitacre 1 year ago

This is amazing! Thank you for sharing it with me.



Reply

FIGURE 4.2: The composer enjoyed the video.

in a lecture hall, when the University of Kent hosted a few schools for maths enrichment. The slides proved suitable for both scenarios.

**Audience:** an extracurricular class of interested highschool students, attending voluntarily.

My goal for content in this introduction to Mersenne primes was to include a healthy number of topics already established for the Huge Primes project syllabus.



In addition to Mersenne primes, I chose Fermat's little theorem, the Lucas-Lehmer primality test, and a bit of modular arithmetic.

There are a large number of slides so that a concept can develop on a static slide and unfold a little at a time, as I talk about it. Charts are visible slide to slide, for ongoing comparison as new information is revealed. Talking points are on the screen, so that viewing and listening complement, and so that content is preserved for future delivery, or for viewing after the fact.

The first time I gave the talk, we handed out paper worksheets at the start that included copies of reference slides, along with exercises to fill the remainder of the hour with hands-on participation and teamwork. Along with some extension project options to work on later, exercises included:

1. using the binomial theorem to expand  $(a + 1)^p$  to prove Fermat's little theorem by induction on  $a$ ,
2. experimenting with Euler's totient function,
3. using the Lucas-Lehmer test to check the primality of Mersenne candidates, and
4. proving that if  $M_n = 2^n - 1$  is prime, then  $n$  is prime.

Note that the slides regarding the Lucas-Lehmer sequence do not give away the trick of reducing  $\text{mod}(M_7)$  at every step; that was left for student discovery.

The students engaged with full attention, nodding along slightly as I talked. They dug into the material and the exercises. Most were there as math superstars, but at least one student was there to support a friend, and ended up telling me, "I don't usually like maths, but I really liked this".

It was an uplifting experience, and I would only make one adjustment if doing again: I would make sure the class was comfortable with modular arithmetic first.

There was one recurring question that came from at least one student at the end of every talk: “how does the Lucas-Lehmer sequence work?” The question spurred my intent to create a clear explanation document on proofs for the Lucas-Lehmer test, which has culminated in Chapter 3 of this thesis.



Introduction to

# MERSENNE PRIMES

Amy Klintberg  
Post-Grad Mathematics Student  
University of Kent, Canterbury



## IN THIS TALK

### MERSENNE NUMBERS $M_n = 2^n - 1$

One less than a power of two.

$(2 \times 2 \times 2 \dots \times 2) - 1$ .

### MERSENNE COMPOSITES

Some Mersenne Numbers are composite. Their factors have a pattern! →

### MERSENNE PRIMES

Mersenne Numbers are an excellent place to look for huge primes. The largest prime found so far is a Mersenne Prime!

How can we find them? →

### FERMAT'S LITTLE THEOREM

$$a^{(p-1)} \equiv 1 \pmod{p}$$

### LUCAS-LEHMER PRIMALITY TEST

Choose a prime  $p$ . Calculate a certain sequence of numbers. If the  $(p-1)$ th term in the sequence is  $\equiv 0 \pmod{2^p-1}$ , then  $2^p-1$  is prime.



## PATTERN WARMUP

What is the next term  
in this sequence?

$2^2, 2^3, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}, ??$

3



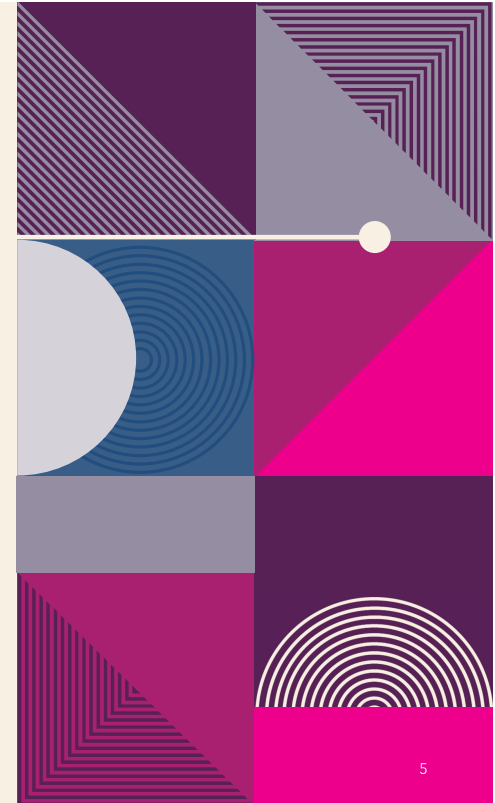
What is the next term  
in this sequence?

$2^2, 2^3, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}, 2^{19}$

4

# MERSENNE NUMBERS

n	$2^n - 1$	=	$M_n$
1	$2^1 - 1$	=	1
2	$2^2 - 1$	=	3
3	$2^3 - 1$	=	7
4	$2^4 - 1$	=	15
5	$2^5 - 1$	=	31
6	$2^6 - 1$	=	63
7	$2^7 - 1$	=	127
8	$2^8 - 1$	=	255
9	$2^9 - 1$	=	511
10	$2^{10} - 1$	=	1023
11	$2^{11} - 1$	=	2047
12	$2^{12} - 1$	=	4095
13	$2^{13} - 1$	=	8191

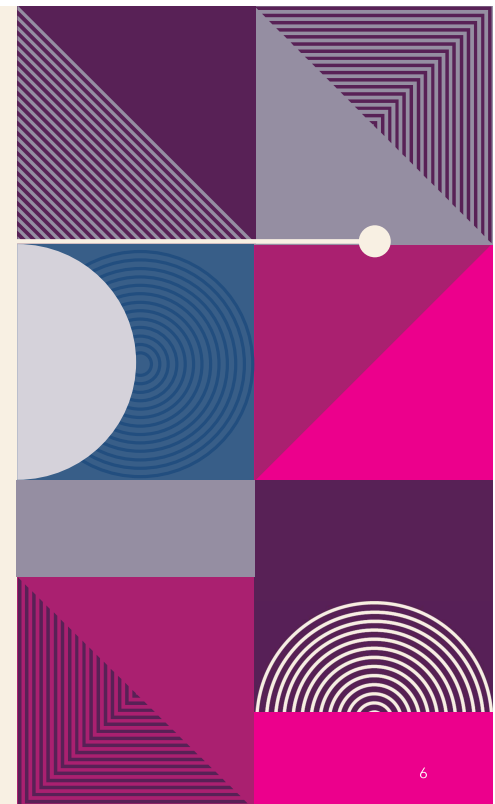


5

# MERSENNE NUMBERS

Let's see where the **primes** are.

n	$2^n - 1$	=	$M_n$
1	$2^1 - 1$	=	1
2	$2^2 - 1$	=	3
3	$2^3 - 1$	=	7
4	$2^4 - 1$	=	15
5	$2^5 - 1$	=	31
6	$2^6 - 1$	=	63
7	$2^7 - 1$	=	127
8	$2^8 - 1$	=	255
9	$2^9 - 1$	=	511
10	$2^{10} - 1$	=	1023
11	$2^{11} - 1$	=	2047
12	$2^{12} - 1$	=	4095
13	$2^{13} - 1$	=	8191

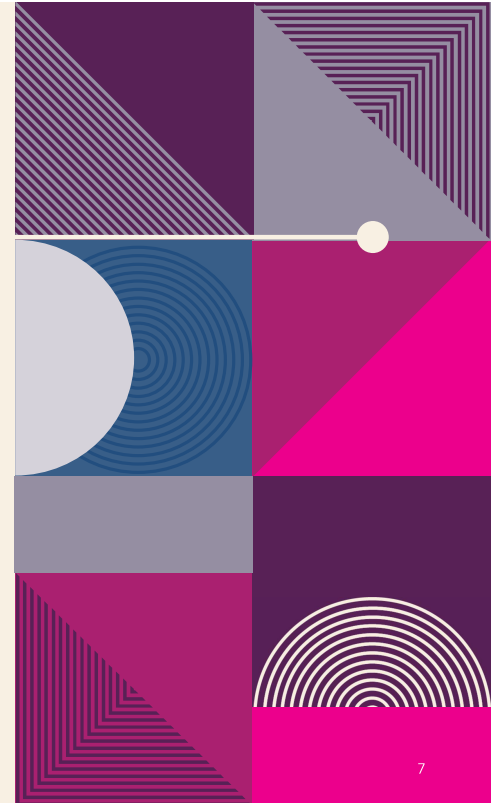


6

# MERSENNE NUMBERS

Let's see where the **primes** are.

n	$2^n - 1$	=	$M_n$
1	$2^1 - 1$	=	1
2	$2^2 - 1$	=	3
3	$2^3 - 1$	=	7
4	$2^4 - 1$	=	15
5	$2^5 - 1$	=	31
6	$2^6 - 1$	=	63
7	$2^7 - 1$	=	127
8	$2^8 - 1$	=	255
9	$2^9 - 1$	=	511
10	$2^{10} - 1$	=	1023
11	$2^{11} - 1$	=	2047
12	$2^{12} - 1$	=	4095
13	$2^{13} - 1$	=	8191

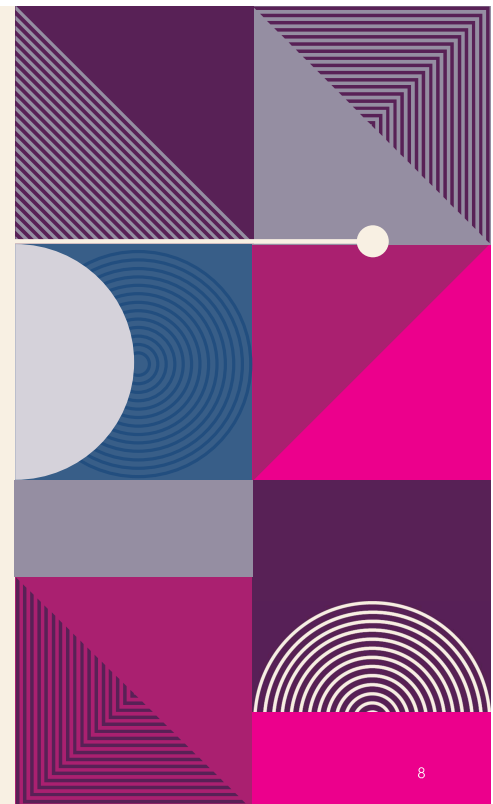


7

# MERSENNE NUMBERS

What is going on with  $M_{11}$ ? Can we predict 23 & 89?

n	$2^n - 1$	=	$M_n$	
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	
9	$2^9 - 1$	=	511	
10	$2^{10} - 1$	=	1023	
11	$2^{11} - 1$	=	2047	23 × 89
12	$2^{12} - 1$	=	4095	
13	$2^{13} - 1$	=	8191	

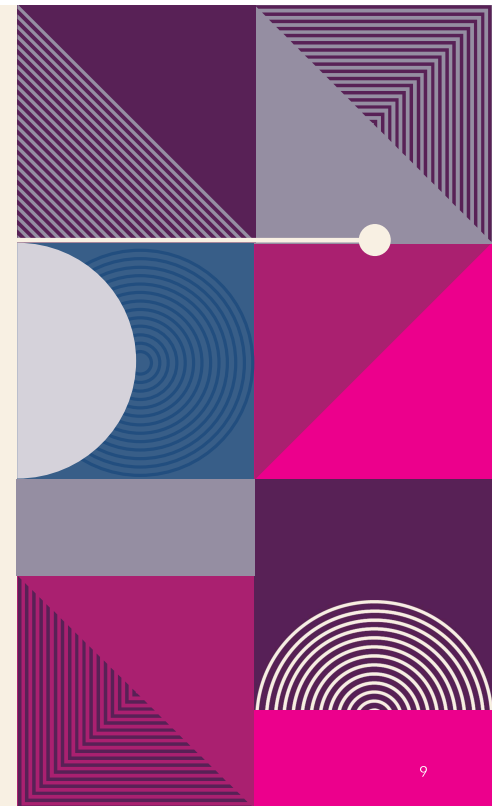


8

# MERSENNE NUMBERS

Let's look at some **prime factorizations**. Any pattern?

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	



# MERSENNE NUMBERS

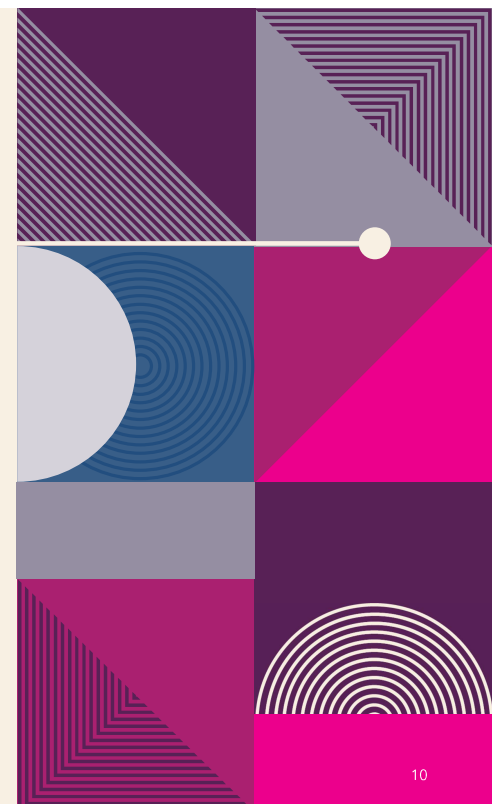
Let's look at some **prime factorizations**. Any pattern?

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	

Side note:

← I'm including the prime factor 3 here in the  $M_2$  line, to emphasize a pattern reveal.

$M_2$  is the smallest Mersenne number that 3 divides, so it gets to be part of this, even though  $M_2$  is highlighted green. This is only because I already know there is a pattern.



# MERSENNE NUMBERS

When does each prime factor **first appear**? 2,3,5,7,11...

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	

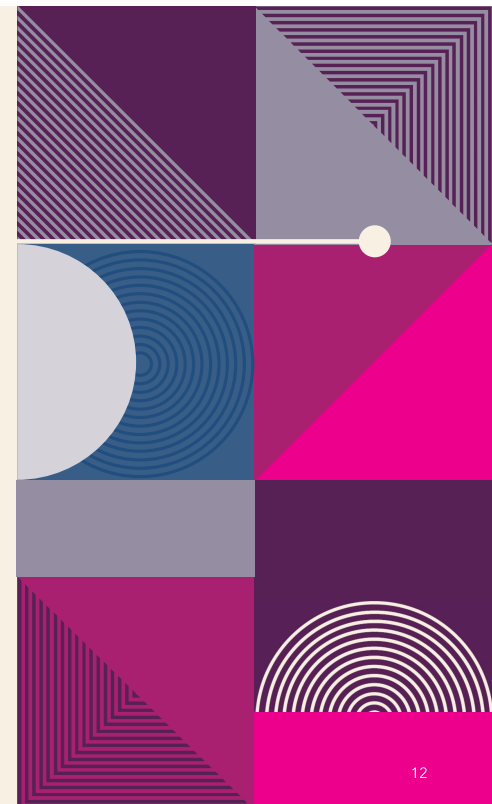


11

# MERSENNE NUMBERS

Each first appearance is **one more than a multiple of n**.

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	



12



We have this observation:

3 divides  $2^2 - 1$

5 divides  $2^4 - 1$

7 divides  $2^6 - 1$

11 divides  $2^{10} - 1$  ...

In general, it appears that:

**p divides the Mersenne number  $2^{(p-1)} - 1$ .**

Happily, this is already a theorem!

MERSENNE NUMBERS

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	

13

## FERMAT'S LITTLE THEOREM

Let p be prime, and a be an integer, coprime to p. Then

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Alternatively,

$$a^{(p-1)} - 1 \equiv 0 \pmod{p}. \quad \rightarrow$$

We have this observation in the Mersenne Number chart:

Prime p divides the Mersenne number  $2^{(p-1)} - 1$ .

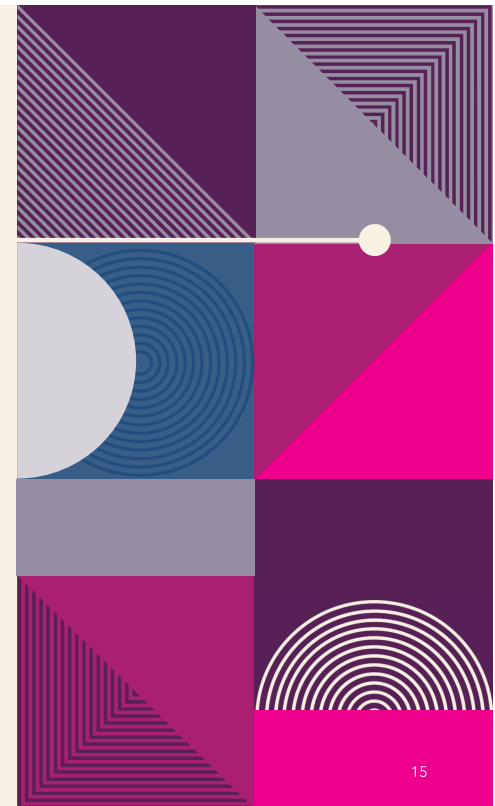
14

# FERMAT'S LITTLE THEOREM

Let  $p$  be prime, and  $a$  be an integer, coprime to  $p$ . Then

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

This is a grounding formula in number theory! When in mod  $p$ , we can multiply a natural number by itself many times, and know when we will return to 1, the multiplicative identity.



15

## FERMAT'S LITTLE THEOREM

$p$  is prime,  $a \in \mathbb{Z}$ ,  $\gcd(a, p) = 1$ .  
 $a^{(p-1)} \equiv 1 \pmod{p}.$

Let's see this in action, mod 5.

$x \pmod{5}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

16

## FERMAT'S LITTLE THEOREM

**p is prime,  $a \in \mathbb{Z}$ ,  $\gcd(a,p)=1$ .**  
 **$a^{(p-1)} \equiv 1 \pmod{p}$ .**

Let's see this in action, mod 5.

$x \pmod{5}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

If a is 2, we see

17

## FERMAT'S LITTLE THEOREM

**p is prime,  $a \in \mathbb{Z}$ ,  $\gcd(a,p)=1$ .**  
 **$a^{(p-1)} \equiv 1 \pmod{p}$ .**

Let's see this in action, mod 5.

$x \pmod{5}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

If a is 2, we see

$$2^2 \equiv 2(2) \equiv 4 \pmod{5}$$

18

## FERMAT'S LITTLE THEOREM

**p is prime,  $a \in \mathbb{Z}$ ,  $\gcd(a,p)=1$ .**  
 $a^{(p-1)} \equiv 1 \pmod{p}$ .

Let's see this in action, mod 5.

$x \pmod{5}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

If a is 2, we see

$$2^2 \equiv 2(2) \equiv 4 \pmod{5}$$

$$2^3 \equiv 4(2) \equiv 3 \pmod{5}$$

17

## FERMAT'S LITTLE THEOREM

**p is prime,  $a \in \mathbb{Z}$ ,  $\gcd(a,p)=1$ .**  
 $a^{(p-1)} \equiv 1 \pmod{p}$ .

Let's see this in action, mod 5.

$x \pmod{5}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

If a is 2, we see

$$2^2 \equiv 2(2) \equiv 4 \pmod{5}$$

$$2^3 \equiv 4(2) \equiv 3 \pmod{5}$$

$$2^4 \equiv 3(2) \equiv 1 \pmod{5}$$

20

## FERMAT'S LITTLE THEOREM

**p** is prime,  $a \in \mathbb{Z}$ ,  $\gcd(a,p)=1$ .  
 $a^{(p-1)} \equiv 1 \pmod{p}$ .

Let's see this in action, mod 5.

x (mod5)	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

If a is 2, we see

$$2^2 \equiv 2(2) \equiv 4 \pmod{5}$$

$$2^3 \equiv 4(2) \equiv 3 \pmod{5}$$

$$2^4 \equiv 3(2) \equiv 1 \pmod{5}$$

$$2^{5-1} \equiv 1 \pmod{5}$$

21

## MERSENNE NUMBERS

Back to  $M_{11}$  and finding Mersenne Primes

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	

22

# MERSENNE NUMBERS

Consider the factors of  $M_{11}$

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	

By Fermat's Little Theorem, we know

$2^{22} - 1 \equiv 0 \pmod{23}$ ,  
so 23 is a factor of  $M_{22}$

Also,  
 $2^{88} - 1 \equiv 0 \pmod{89}$ ,  
so 89 is a factor of  $M_{88}$

However, we have no predictive mechanism to tell us that 23 and 89 telescope down to be factors of  $M_{11}$  as well, and disqualify it from being prime.

This kind of telescoping happens frequently...

# MERSENNE NUMBERS

Back to  $M_{11}$  and now  $M_3$

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	(1)
2	$2^2 - 1$	=	3	3
3	$2^3 - 1$	=	7	7
4	$2^4 - 1$	=	15	$3 \times 5$
5	$2^5 - 1$	=	31	31
6	$2^6 - 1$	=	63	$3 \times 3 \times 7$
7	$2^7 - 1$	=	127	127
8	$2^8 - 1$	=	255	$3 \times 5 \times 17$
9	$2^9 - 1$	=	511	$7 \times 73$
10	$2^{10} - 1$	=	1023	$3 \times 11 \times 31$
11	$2^{11} - 1$	=	2047	$23 \times 89$
12	$2^{12} - 1$	=	4095	$3^2 \times 5 \times 7 \times 13$
13	$2^{13} - 1$	=	8191	8191

... In fact, when we complete the prime factorization table, we see the first Mersenne number that 7 divides is  $M_3$ , not  $M_6$ .

By Fermat's Little Theorem, we know

$2^6 - 1 \equiv 0 \pmod{7}$ ,  
so 7 is a factor of  $M_6$

But, how were we to know that 7 would divide  $M_3$  as well?

As a factor, 7 would disqualify  $M_3$  from being prime, if not for the fact that 7 is  $M_3$  itself.

Every Mersenne prime is its own factor in this way. 31 divides  $M_{30}$ , but also  $M_5$ , etc.

# MERSENNE NUMBERS

Primes are highlighted in green

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	
9	$2^9 - 1$	=	511	
10	$2^{10} - 1$	=	1023	
11	$2^{11} - 1$	=	2047	23×89
12	$2^{12} - 1$	=	4095	
13	$2^{13} - 1$	=	8191	

So now, how do we find Mersenne Primes?

# MERSENNE NUMBERS

Primes are highlighted in green

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	
9	$2^9 - 1$	=	511	
10	$2^{10} - 1$	=	1023	
11	$2^{11} - 1$	=	2047	23×89
12	$2^{12} - 1$	=	4095	
13	$2^{13} - 1$	=	8191	

Firstly, it is true that

composite n  
 $\Rightarrow$   
 composite  $M_n$

# MERSENNE NUMBERS

Primes are highlighted in green

n	$2^n - 1$	=	$M_n$	Prime factorization
1	$2^1 - 1$	=	1	
2	$2^2 - 1$	=	3	
3	$2^3 - 1$	=	7	
4	$2^4 - 1$	=	15	
5	$2^5 - 1$	=	31	
6	$2^6 - 1$	=	63	
7	$2^7 - 1$	=	127	
8	$2^8 - 1$	=	255	
9	$2^9 - 1$	=	511	
10	$2^{10} - 1$	=	1023	
11	$2^{11} - 1$	=	2047	23×89
12	$2^{12} - 1$	=	4095	
13	$2^{13} - 1$	=	8191	

When  $n$  is prime, we \*might\* have a Mersenne Prime.

We check, using the Lucas-Lehmer primality test.

## LUCAS-LEHMER PRIMALITY TEST

For testing Mersenne Candidates  $M_p = 2^p - 1$

Define a sequence  $S_n$ ,  $n \in \mathbb{N}$ , such that

$$S_1 = 4$$

$$S_{n+1} = (S_n)^2 - 2$$

Then  $M_p$  is prime iff  $M_p$  divides  $S_{p-1}$ .

ie, iff  $S_{p-1} \equiv 0 \pmod{M_p}$ .



# THE LUCAS-LEHMER SEQUENCE

$$\begin{aligned}
 S_1 &= 4 \\
 S_2 &= (4)^2 - 2 = 14 \\
 S_3 &= (14)^2 - 2 = 194 \\
 S_4 &= (194)^2 - 2 = 37634 \\
 S_5 &= (37634)^2 - 2 = 1416317954 \\
 S_6 &= (1416317954)^2 - 2 = 2005956546822746114 \\
 &\dots
 \end{aligned}$$

## LUCAS-LEHMER PRIMALITY TEST

For testing  $M_p = 2^p - 1$

Define a sequence  $S_n$ ,  $n \in \mathbb{N}$ , such that

$$\begin{aligned}
 S_1 &= 4 \\
 S_{n+1} &= (S_n)^2 - 2
 \end{aligned}$$

Then  $M_p$  is prime  
iff  
 $S_{p-1} \equiv 0 \pmod{M_p}$ .

# THE LUCAS-LEHMER SEQUENCE

$$\begin{aligned}
 S_1 &= 4 \\
 S_2 &= (4)^2 - 2 = 14 \\
 S_3 &= (14)^2 - 2 = 194 \\
 S_4 &= (194)^2 - 2 = 37634 \\
 S_5 &= (37634)^2 - 2 = 1416317954 \\
 S_6 &= (1416317954)^2 - 2 = 2005956546822746114 \\
 &\dots
 \end{aligned}$$

Check  $p=7$ .  
 $M_7=127$ .

127 divides  $S_6$ .

$S_6 \equiv 0 \pmod{M_7}$

So,  $M_7$  is prime.

## LUCAS-LEHMER PRIMALITY TEST

For testing  $M_p = 2^p - 1$

Define a sequence  $S_n$ ,  $n \in \mathbb{N}$ , such that

$$\begin{aligned}
 S_1 &= 4 \\
 S_{n+1} &= (S_n)^2 - 2
 \end{aligned}$$

Then  $M_p$  is prime  
iff  
 $S_{p-1} \equiv 0 \pmod{M_p}$ .

# MERSENNE PRIMES

DISCOVERED SO FAR

[mersenne.org](http://mersenne.org)

GIMPS

The Great Internet Mersenne Prime Search



2018-Dec-21

## 51st Known Mersenne Prime Found!

**December 21, 2018** — The [Great Internet Mersenne Prime Search](http://mersenne.org) (GIMPS) has discovered the largest known prime number,  $2^{82\,589\,933}-1$ , having 24 862 048 digits. A computer volunteered by Patrick Laroche from Ocala, Florida made the find on December 7, 2018. The new prime number, also known as  $M(82\,589\,933)$ , is calculated by multiplying together 82 589 933 twos and then subtracting one. It is more than one and a half million digits larger than the [previous record prime number](#).

Are there more to discover? We think so!  
We have yet to prove whether there are  
infinitely many Mersenne Primes or not.



31

## IN THIS TALK

### MERSENNE NUMBERS $M_n = 2^n - 1$

One less than a power of two.

$(2 \times 2 \times 2 \dots \times 2) - 1$ .

### MERSENNE COMPOSITES

Some Mersenne Numbers are composite. Their factors have a pattern! →

### MERSENNE PRIMES

Mersenne Numbers are an excellent place to look for huge primes. The largest prime found so far is a Mersenne Prime!

How can we find them? →

### FERMAT'S LITTLE THEOREM

$$a^{(p-1)} \equiv 1 \pmod{p}$$

### LUCAS-LEHMER PRIMALITY TEST

Choose a prime  $p$ . Calculate a certain sequence of numbers. If the  $(p-1)$ th term in the sequence is  $\equiv 0 \pmod{2^p-1}$ , then  $2^p-1$  is prime.

32



## 4.3 A Postgraduate Research Poster

**Summary:** The following poster was designed for the annual Postgraduate conference at the University of Kent. It was a full-day conference of postgraduate-led presentations and workshops, ending in a poster festival.

**Audience:** University staff and students from varied disciplines, along with any friends and family in attendance; an open University setting.

My goal with this poster was to invite viewers of all backgrounds to simply enjoy looking, and to provide concentrated snappy knowledge gems. While absorbed in the layout and intriguing background, I hoped viewers would casually read snippets and build interest. I was aiming for a reaction of “I don’t know what this shows, but I like looking at it,” bypassing the recoil reflex many people have around mathematics. It was received very positively, with one of my favourite quotes from a viewer stating, “Mathematics really is beautiful, isn’t it?”

When presenting the poster, the slow cold-open approach used in Chapter 1 was essential for light-bulb moments of understanding among the audience. The exclamations of “ohhhhh” from the group when something clicked were very satisfying.

At the end of the conference, I was awarded that year’s poster winner for Computing Engineering Maths and Statistics.



# When Midnight is an Odd Number: The Mersenne Composites That Are Revealed in mod(Odd)

## Mersenne Numbers

are numbers that are one less than a power of 2. We write  $M_n = 2^n - 1$ . Sometimes they are prime, sometimes composite.

$n$	$2^n - 1$	prime?
1	1	x x
2	3	✓ ✓
3	7	✓ ✓
4	15	x x
5	31	✓ ✓
6	63	x x
7	127	✓ ✓
8	255	x x
9	511	x x
10	1023	x x
11	2047	n ✓ x $M_n$

$2^{11} - 1$  breaks pattern!  $2047 = 23 \times 89$ . It's unexpectedly composite. Why?

## Modular Arithmetic,

or "clock arithmetic", wraps the number line of integers around a circle, and considers overlapping numbers equivalent, denoted with  $\equiv$ .

On a regular clock,  $0 = 12 \equiv 24$ . This is mod(12). We could also say  $-12 \equiv 0 \equiv 36$ . The entire integer number line is included on the circle.

When the distance,  $d$ , around the circle is odd, then multiplication by 2 in mod( $d$ ) creates beautiful symmetrical lines. Let's look at mod(23).

### Multiplication by 2

$0 \times 2 = 0$
$1 \times 2 = 2$
$2 \times 2 = 4$
$3 \times 2 = 6$
$4 \times 2 = 8$
$5 \times 2 = 10$
$6 \times 2 = 12$
$7 \times 2 = 14$
$8 \times 2 = 16$
$9 \times 2 = 18$
$10 \times 2 = 20$
$11 \times 2 = 22$



The boldened path, called the orbit of 2 in finite field  $F_{23}$ , forms a complete loop, from 1 back to 1. The total distance represented by this loop perfectly wraps the circle.

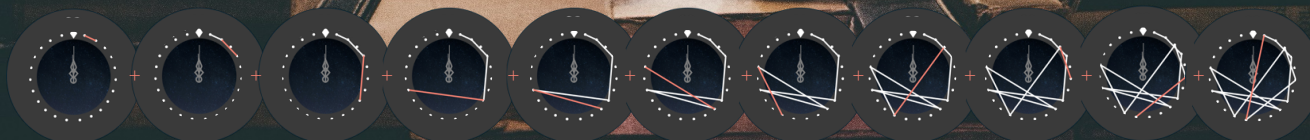
### Multiplication by 2

$0 \times 2 = 0$
$-1 \times 2 = -2$
$-2 \times 2 = -4$
$-3 \times 2 = -6$
$-4 \times 2 = -8$
$-5 \times 2 = -10$
$-6 \times 2 = -12$
$-7 \times 2 = -14$
$-8 \times 2 = -16$
$-9 \times 2 = -18$
$-10 \times 2 = -20$
$-11 \times 2 = -22$



## What does it mean?

Let's look at the steps.



It means 23 divides  $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} = 2^{11} - 1$ .

We are looking at the pattern breaker, the Mersenne composite  $2^{11} - 1$ , in the modular arithmetic environment of one of its divisors, the odd number  $d = 23$ .

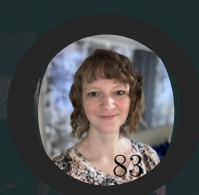
Excitingly, when  $d = 89$  (the other proper divisor  $2^{11} - 1$ ), we get the same behaviour. We have a way to investigate the Mersenne pattern breakers!

Every Mersenne number is odd, so, if it has any proper divisors, those divisors are also odd. We can make any odd  $d$  become midnight, and observe its secrets.

## A note to number theorists

We can predict that 23 divides  $2^{22} - 1$  and 89 divides  $2^{88} - 1$  by Euler's Theorem  $a^{\phi(d)} \equiv 1 \pmod{d}$ , where  $\phi(d)$  is the totient of  $d$ . These diagrams help us understand and probe how the orbit of 2 can telescope from 22 and 88 down to 11, and indeed how all Mersenne candidates with a prime power relate to their divisors.

Library Photo by Jared Craig on Unsplash  
Night Sky Photo by Redd E on Unsplash



**Amy Klintberg**  
PGR Masters Student  
Mathematics  
University of Kent  
2024

These clock diagrams, as pertaining to Mersenne composites, were discovered by Amy in her ongoing affinity for maths visualization, as a tool for community engagement and insight into beauty.

## 4.4 Cardioid Yarn Art of Divisibility Graphs

**Summary:** The main circle diagrams in this thesis, of generative paths of 2 in residue rings, are composed of line segments that are tangent to a cardioid. The paths can be created with yarn on pegs around a circle, preferably an odd number of pegs, to connect with Mersenne concepts, but the cardioid is a lovely mathematical engagement draw. In practice, effective materials have been a hula hoop, push-pins, and white yarn.

**Audience:** Crafters of all persuasions.

Late into my Master's program, Numberphile released a video [10] highlighting the circle for  $p = 7$ , used for modular multiplication just as we have been using it. They reveal that it is called a divisibility graph. It was nice to see the circle diagrams embraced in the wild, not only as a visualization tool, but a handy calculating device. This accessible application of the circle diagrams — along with the beautiful cardioid potential and immediate connection with Mersenne composites — makes this an excellent crafting opportunity that may develop in future community engagement.

When sharing the circle diagrams with fellow students, teachers, family, and friends this year, several have commented that they would like a copy of one of them. This inspired the creation of Appendix D, which displays circle diagrams of odd years in recent and upcoming memory, for even more popularity. Some of the year circles telescope heavily, which makes them an option for crafting with yarn, while having a potential personal connection with the year. One friend says she may create her birth year with yarn art over the winter months. Meanwhile, in practice, the yarn art approach was useful this year for my Mersenne presentations.

# Chapter 5

## Closing Thoughts

Mersenne numbers have many rabbit trails we can follow, being very chasable themselves, and visiting with many mathematical systems. They make wonderfully suitable material for enrichment on number theory, and welcome recreational exploration.

In addition to the areas we have already touched on, Mersenne numbers have many more avenues open to us, both for academic pursuit and for community engagement. As direct companions to powers of 2, they are connected to the Tower of Hanoi puzzle, and may be related to the dragon curve which involves repeatedly folding a piece of paper.

A main approach to Mersenne numbers that we would be remiss not to mention is the framing of the Mersenne sequence as a linear recursive sequence. Indeed, we can write the sequence:

$$M_{n+2} = 3M_{n+1} - 2M_n, \text{ with } M_1 = 1, M_2 = 3.$$

This places Mersenne numbers in the same category as Fibonacci numbers, and gives us further tools to use with them. For Fibonacci numbers, the rank of apparition of a given prime number  $p$  is the smallest index for which the Fibonacci number with that index is divisible by  $p$ . This is exactly the concept we have been



targeting in our Mersenne explorations for this thesis, which is encouraging for future exploration.

To close, we end with one more diagram 5.1, this time a spiral of the linear recursive Mersenne sequence, built using the same method the Fibonacci sequence uses: rotate by a right angle, and scale the previous terms according to the recursive relation.

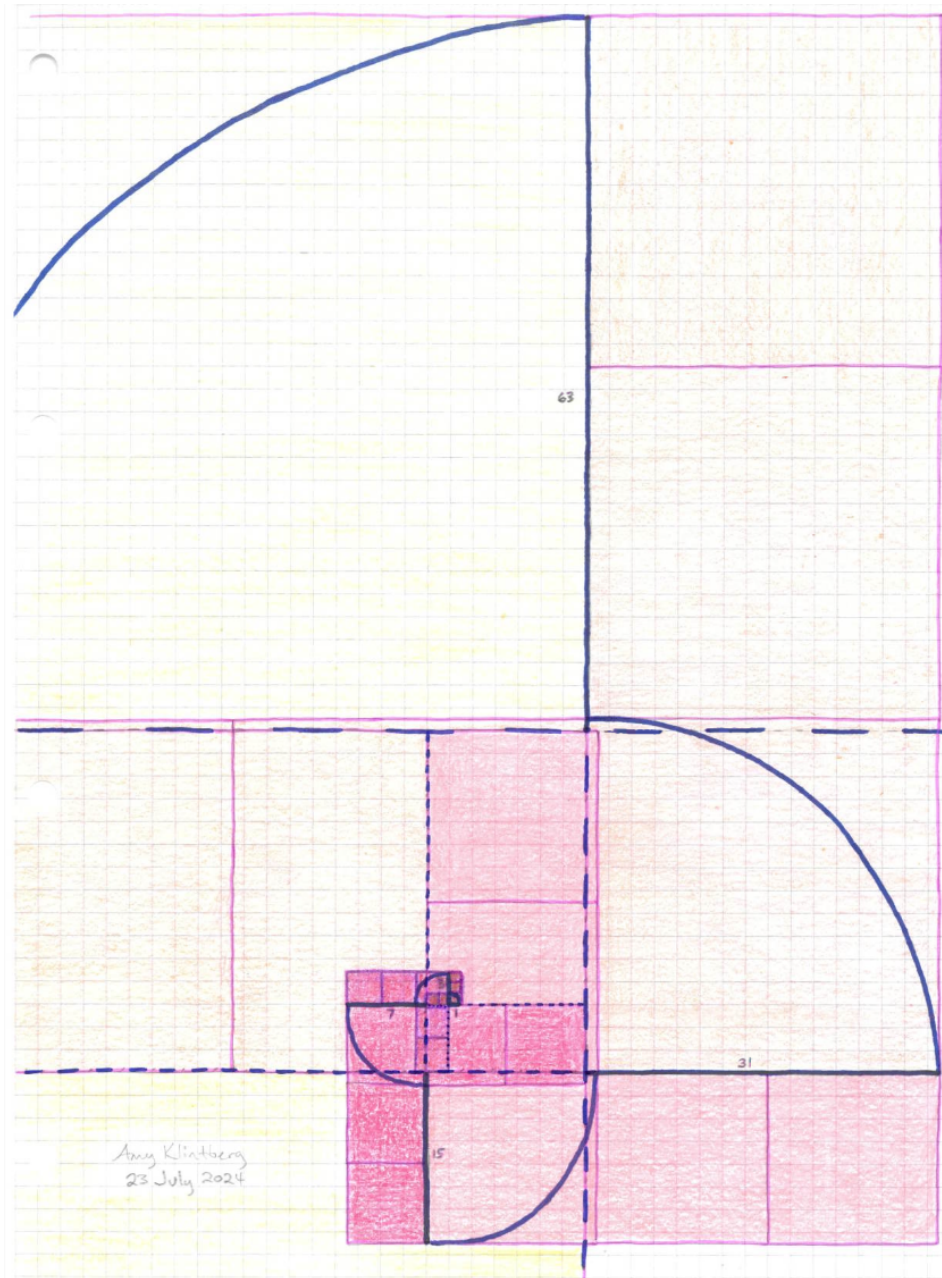


FIGURE 5.1: A diagram of the Mersenne number sequence, as a Fibonacci-like spiral, constructed from its linear recursive relation.



# Appendix A: Maple Code for Circle Diagrams

The code to create the circle diagrams of multiplicative generative pathways was created using the Maplesoft dataplot function, which automatically connects a succession of points, for line graphs.

In development, points were plotted easily in polar coordinates [Figure 5.2] using Euler's  $e^{i\theta}$  formula, and then reflected into our familiar modular clock orientation by subtracting each angle from  $\frac{\pi}{2}$ . A colourful gradient line is available in Cartesian coordinates, which is employed in the final form of the code, from blues to greens.

```
> with(NumberTheory) : with(plots) : with(plottools) :
```

*# These procedures combine to produce the final CircleDisplay.*

```
> Orbit_on_circle := proc(d)
  local A5, A6, i;
  A5 := Array(1 .. Totient(d) + 1, 1 .. 1);
  A6 := Array(1 .. Totient(d) + 1, 1 .. 1);
  for i from 1 to Totient(d) + 1 do
    A5(i, 1) := cos( $\frac{\pi}{2} - (2^{i-1} \bmod d) \cdot \left(\frac{2 \cdot \pi}{d}\right)$ );
    A6(i, 1) := sin( $\frac{\pi}{2} - (2^{i-1} \bmod d) \cdot \left(\frac{2 \cdot \pi}{d}\right)$ );
  end do;

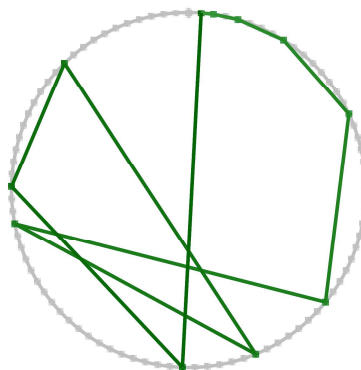
  #GRADIENT FOR PRIME d, BLACK FOR COMPOSITE d.
  if isprime(d) = true then
    dataplot(A5, A6, colorscheme=["LightBlue", "Blue", "LightGreen", "DarkGreen"], axes=None, symbolsize=10);
  else
    dataplot(A5, A6, color=black, axes=None, symbolsize=10);
  end if;

end proc;
#Orbit_on_circle
```

```
> Points_on_circle := proc(d)
  local A7, A8, i;
  A7 := Array(1 .. Totient(d) + 1, 1 .. 1);
  A8 := Array(1 .. Totient(d) + 1, 1 .. 1);
  for i from 1 to d do
    A7(i, 1) := cos( $\frac{\pi}{2} - (i) \cdot \left(\frac{2 \cdot \pi}{d}\right)$ );
    A8(i, 1) := sin( $\frac{\pi}{2} - (i) \cdot \left(\frac{2 \cdot \pi}{d}\right)$ );
  end do;
  dataplot(A7, A8, style=point, color=grey, axes=None, symbolsize=10);
end proc;
#Points_on_circle
```

```
> CircleDisplay := proc(d)
  local p1, p2, p3, point, p4;
  p1 := implicitplot(x^2 + y^2 ≤ 1, color=grey, );
  p2 := Points_on_circle(d);
  p3 := Orbit_on_circle(d);
  point := [[0, 1]]:
  p4 := plot(point, style=POINT, color=grey, symbolsize=25);
  display([p1, p2, p3, p4], scaling=CONSTRAINED);
end proc;
#CircleDisplay. A combined plot of: a unit circle, d-many o'clock points, the orbit of 2 mod(d), and a diamond point at the crown.
```

```
> CircleDisplay(89)
# This orbit shows mainly dark green.
# It telescopes so much that only the
# tail end of the orbit is showing
```



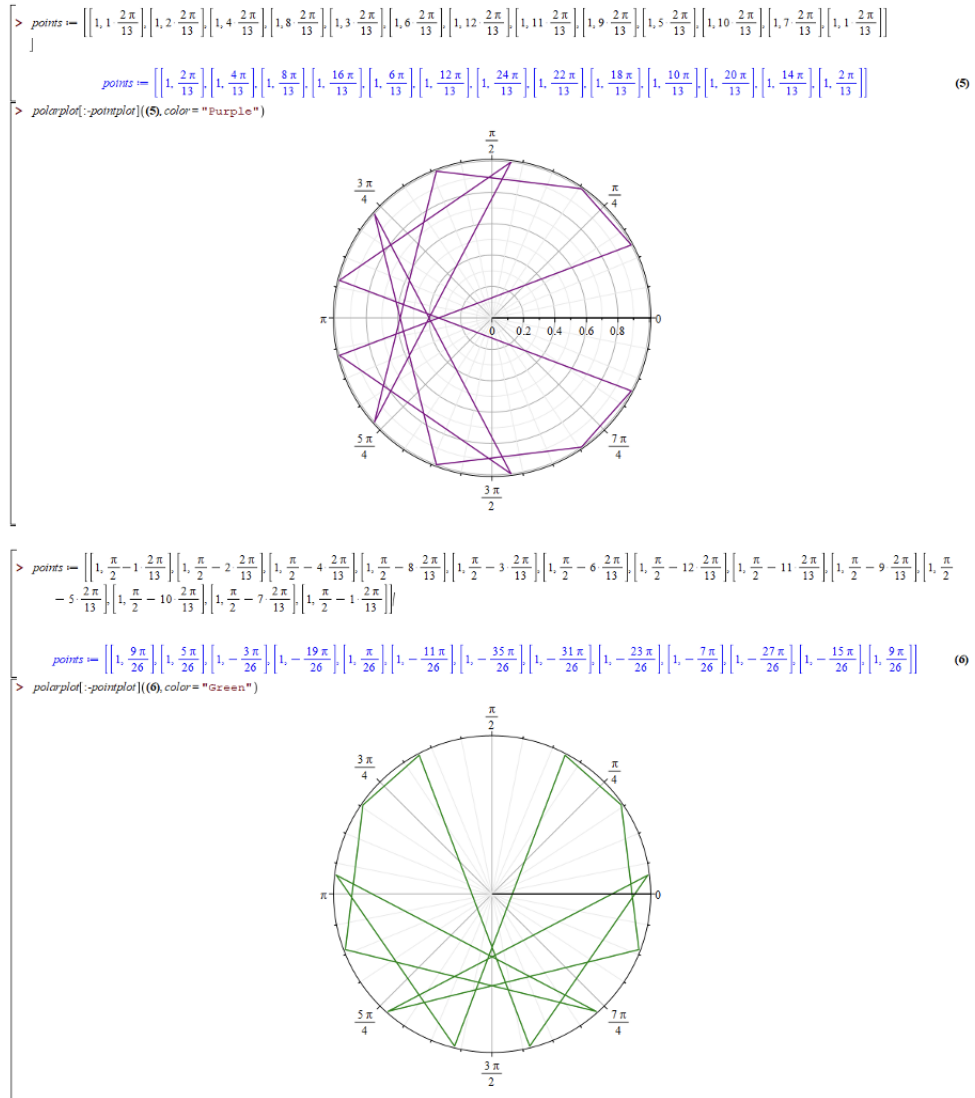


FIGURE 5.2: Code development

# Appendix B: Maple Code for the Binary Algorithm

Below, here is code for the binary algorithm introduced in Chapter 2, which finds the smallest Mersenne number divisible by a given odd input  $d$ . Page breaks are strategically placed so that each page contains a full thought, where possible.

The output displays the essential array along with data of interest about the outcome, listing:

1. The input  $d$ ,
2. whether  $d$  is prime,
3. the dimensions of the array,
4. the reduced dimensions of the array,
5. the totient of  $d$ ,
6. the smallest Mersenne number  $d$  divides, and
7. the resulting telescoping factor.

```

>
>
>

```

```

> Binary_Algorithm :=proc(d)

```

```

# Binary_Algorithm Procedure using arrays A1 A2 A3: The first two arrays create the binary data backwards.
Then A3 cleans up and reverses A2 to be more clearly legible.

```

```

# To start, the procedure will convert odd input "d" to binary in array A2. Note: the binary that is created is
writtten BACKWARDS by design, since array column addresses read left to right, and we can use the array
column numbering (minus one) to keep track of the power of 2 that the column represents.

```

```

# Next, recursively: total contents of A2, convert the total to binary and assign the total to a single row array
A1, tack an extra column on the end of A1 with a "0" in it to serve as a final stop sign, then find the first "0"
entry in A1. Starting from the column with the first zero entry in A1, assign a binary copy of "d" to the next row
of A2. Repeat until there are no zero entries in the binary total, tracked in A1. Since all the entries of A1 are
ones (except the final signpost 0 tacked on the end), the total is a Mersenne number. A2 has grown to the full
array of roughly diagonal "d"s that sum to the Mersenne number.

```

```

# The procedure is effectively complete at this stage, but all binary notation data in A1 and A2 is still
BACKWARDS, and the irrelevant cells of A2 are filled with distracting zeros. Array A3 is built after A2 is done.
A3 is created as an array of blanks matching A2 dimensions. Then, recursively row by row: we identify the first
"1" entry in A2, and copy that entry and the entries that follow, for the full width of "d" in binary, into the same
row of A3 as a mirror image.

```

```

# The final display prints A3 along with relevant data about "d" and the Mersenne outcome.

```

```

local w, indextrule, A2, s, j, i, X, Y, t, y, c, x, A1, v, a, A3;

```

```

# w - width of d in binary

```

```

# indextrule - used to create baseline arrays A2 and A3

```

```

# A2 - an array to ultimately contain the strata of "d" in binary that sum to a Mersenne number

```

```

# s - a sequence used to track how much of a base ten input is left to convert to binary

```

```

# j - index for sequence s

```

```

# i - index to count iterations up to d-1, a simple algorithm termination deadline.

```

```

# (A bit overkill, but more reliable to code than involving the totient of d here.)

```

```

# X - current max row coordinate of A2

```

```

# Y - current max column coordinate of A2

```

```

# t - a sequence that totals A2, in base ten

```

```

# y - index to iterate columns

```

```

# c - a sequence that totals individual columns of A2, counting the ones

```

```

# x - index to iterate rows

```

```

# A1 - a single row array to track the binary sum represented by A2

```

```

# v - the y-value (column) of A1 with the first zero in it, or A2 with the first one in it

```

```

# a - index to iterate copying binary "d" from the first row of A2 into a new row of A2, shifted right

```

```

# A3 - an array mirror-image of A2 with empty space clarified, for read-out

```

*# On this page, we convert "d" to binary notation within array A2.*

$w := \text{trunc}(\log_2(d)) + 1;$

*# w is the width of d in binary; the number of columns required for binary d.*

*# trunc rounds down. It cuts off the answer at the decimal point and discards the littles. We add 1 to round up.*

$\text{indexrule} := (x, y) \rightarrow 0 :$

$A2 := \text{Array}(1..1, 1..w, \text{indexrule});$

*# A2 has been created.*

*# It starts as a single row of dimensions 1 x w, with 0 for each entry.*

$A2(1, w) := 1;$

$s[1] := d - 2^{w-1};$

*# The last column of A2 now has a 1 in it. Since we're building binary backwards, this is the largest portion of "d" that is a power of 2.*

*# A sequence tracker s has been created to track how much of d is left to add to A2.*

**for j from 1 to w do**

**if  $s[j] \geq 1$  then**

$A2(1, \text{trunc}(\log_2(s[j])) + 1) := 1;$

$s[j+1] := s[j] - 2^{\text{trunc}(\log_2(s[j]))};$

**else;**

$s[j+1] := 0$

**end if;**

**end do;**

*# The first row of A2 has now been created.*

*# It is a single row containing the input odd number d, in base two backwards.*

*# The following monster loop introduces A1. In the loop, A2 will grow until the A1 binary sum that A2 represents is a Mersenne number.*

**for  $i$  from 1 to  $d - 1$  do**

$X, Y := \text{upperbound}(A2);$

$t[0] := 0;$

**for  $y$  from 1 to  $Y$  do**

$c[0] := 0;$

**for  $x$  from 1 to  $X$  do**

$c[x] := c[x - 1] + A2[x, y];$

**end do;**

$t[y] := t[y - 1] + 2^{y-1} \cdot c[X];$

**end do;**

*#  $t[Y]$  is now the total, in base ten, of the binary sum represented by the  $A2$  summand array;*

$\text{indexrule} := (x, y) \rightarrow 0 :$

$A1 := \text{Array}(1..1, 1..\text{trunc}(\log_2(t[Y])) + 1, \text{indexrule});$

$A1(1, \text{trunc}(\log_2(t[Y])) + 1) := 1;$

$s[1] := t[Y] - 2^{\text{trunc}(\log_2(t[Y]))};$

**for  $j$  from 1 to  $\text{trunc}(\log_2(t[Y])) + 1$  do**

**if  $s[j] \geq 1$  then**

$A1(1, \text{trunc}(\log_2(s[j])) + 1) := 1;$

$s[j + 1] := s[j] - 2^{\text{trunc}(\log_2(s[j]))};$

**else;**

$s[j + 1] := 0$

**end if;**

**end do;**

$A1(1, \text{trunc}(\log_2(t[Y])) + 2) := 0;$

*#  $A1$  is now the  $t[Y]$  total, in base two backwards, and has a leading zero at the end of the array, as a stop-sign for  $v$  below.*

$v := 1 :$

**do  $v := v + 1$**

**until  $A1(1, v) = 0;$**

*#  $v$  has found the column coordinate with the first zero entry in the  $A1$  total;*

**if  $v < \text{trunc}(\log_2(t[Y])) + 2$  then**

**for  $a$  from 0 to  $\text{trunc}(\log_2(d))$  do**

$A2(i + 1, v + a) := A2(1, a + 1);$

**end do;**

**end if;**

**end do;**

*#  $A1$ , the backwards binary total, is now a string of 1s with a leading zero at the end. Dimensions:  $1 \times (Y+1)$ .*

*#  $A2$ , the backwards binary array with all the interesting info, is now fully grown. Dimensions:  $X \times Y = [\text{number of times the loop ran}] \times Y$ . Note:  $Y$  is the index of the smallest Mersenne number that  $d$  divides. This is our initial motivation for creating this Binary Algorithm.*

*# Next:  $A3$  is about to be created by reversing  $A2$ . It will be our display output, to see the info forwards instead of backwards.*

*indexrule* := (x, y) → \_ :

*A3* := Array(1..X, 1..Y, indexrule);

*# A3 is created empty, same dimensions as A2, filled with \_ to clean out unnecessary zeros. We already have these final A2 dimensions from the last loop: X, Y.*

*# Note: we did not build the array this way at the start because we didn't know the dimensions of the array until we grew it. Newly spawned rows and columns auto fill with zeros.*

**for** x **from** 1 **to** X **do**

    v := 0 :

**do** v := v + 1

**until** A2(x, v) = 1;

*# v has found the column coordinate with the first 1 entry, in this particular x row of the fully grown A2 array. # w is still the binary width of d. We can use it to tell how much of this row to copy from A2 into A3.*

**for** y **from** v **to** v + w - 1 **do**

            A3(x, Y - y + 1) := A2(x, y);

**end do;**

*# The backwards binary d in this x row of A2 has been flip-copied into the same x row of A3, now a forwards binary d. Loop repeats until the bottom row X is complete.*

**end do;**

*# A3 is complete. We now print our desired display outputs.*

print(d);

print('dPrime', isprime(d));

with(LinearAlgebra) : interface(rtablesizer = infinity) : print(A3);

print('HeightWidthOfArray', X, Y);

print('ReducedDimensionsOfArray',  $\frac{X}{\gcd(X, Y)}$ ,  $\frac{Y}{\gcd(X, Y)}$ );

with(NumberTheory) : print('dTotient', Totient(d));

print('dDivides', M, Y);

print('TelescopingFactor x is',  $\frac{\text{Totient}(d)}{Y}$ );

**end proc:**

*#proc: Binary\_Algorithm*

> Binary\_Algorithm(89)

89

dPrime, true

$$\begin{bmatrix} - & - & - & - & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ - & - & - & - & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ - & - & 1 & 0 & 1 & 1 & 0 & 0 & 1 & - & - \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & - & - & - & - \end{bmatrix}$$

HeightWidthOfArray, 4, 11

ReducedDimensionsOfArray, 4, 11

dTotient, 88

dDivides, M, 11

TelescopingFactor x is, 8

(1



# Appendix C: Circle and Array

## Data, odd divisors 3-103

The following pages display data for odd divisors  $d$ , including those that are composite and those that are prime. The primes are in colour with a gradient path of blues to greens. The composites are in grey with a black pathway.

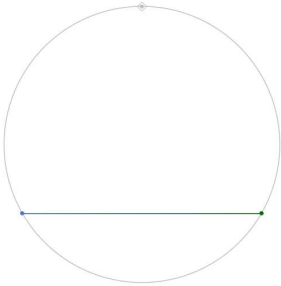
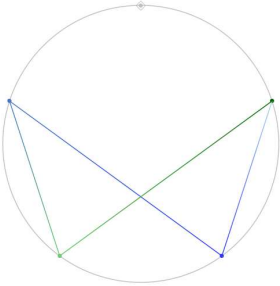
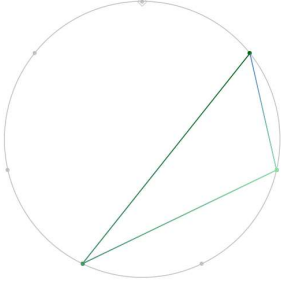
Each page has a layout of four divisors, showing divisors of the form  $8k + 1$ ,  $8k + 3$ ,  $8k + 5$ , and  $8k + 7$ . This is relevant to our discussion of prime divisors in Chapter 2.

Prime divisors of the form  $8k + 1$  or  $8k + 7$  are guaranteed to be telescoping primes for the path of 2, with a telescoping factor that is even. They have symmetrical paths occasionally. When their path is not symmetric, they might divide a Mersenne candidate, and they might not.

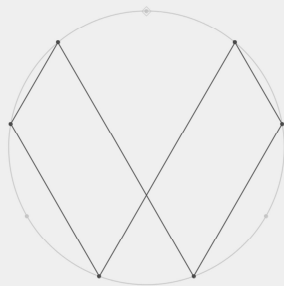
Prime divisors of the form  $8k + 7$  that also happen to be “safe primes”, which are primes of the form  $2g + 1$  with  $g$  also prime — these primes always divide a composite Mersenne candidate.

Primes of the form  $8k + 3$  or  $8k + 5$  are occasionally telescoping primes of the path of 2. Their telescoping factor is always odd. These pathways are always symmetrical, so these primes never divide a Mersenne candidate.

Composite divisors may be telescoping divisors of the path of 2. The telescoping factor of composite  $d$  is connected to the telescoping factors of the prime factors of  $d$ , but can be unpredictable.

	<p>&gt; CircleDisplay(3)  # 3 is prime  # <math>8k+3</math></p>  <p>&gt; ArrayDisplay(3)  <i>dTotient</i>, 2  <i>dDivides</i>, <i>M</i>, 2  <i>TelescopingFactor</i>*<i>x</i>*is, 1</p> <div style="text-align: center;"> <math display="block">\begin{bmatrix} 1 &amp; 1 \end{bmatrix}</math> <i>HeightWidthOfArray</i>, 1, 2  <i>ReducedDimensions</i>, 1, 2 </div>
<p>&gt; CircleDisplay(5)  # 5 is prime  # <math>8k+5</math></p>  <p>&gt; ArrayDisplay(5)  <i>dTotient</i>, 4  <i>dDivides</i>, <i>M</i>, 4  <i>TelescopingFactor</i>*<i>x</i>*is, 1</p> <div style="text-align: center;"> <math display="block">\begin{bmatrix} - &amp; 1 &amp; 0 &amp; 1 \\ 1 &amp; 0 &amp; 1 &amp; - \end{bmatrix}</math> <i>HeightWidthOfArray</i>, 2, 4  <i>ReducedDimensions</i>, 1, 2 </div>	<p>&gt; CircleDisplay(7)  # 7 is prime  # <math>8k+7</math></p>  <p>&gt; ArrayDisplay(7)  <i>dTotient</i>, 6  <i>dDivides</i>, <i>M</i>, 3  <i>TelescopingFactor</i>*<i>x</i>*is, 2</p> <div style="text-align: center;"> <math display="block">\begin{bmatrix} 1 &amp; 1 &amp; 1 \end{bmatrix}</math> <i>HeightWidthOfArray</i>, 1, 3  <i>ReducedDimensions</i>, 1, 3 </div>

> CircleDisplay(9)  
# 9 = (3<sup>2</sup>)



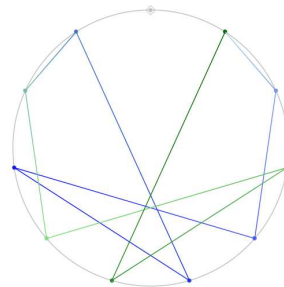
> ArrayDisplay(9)  
dTotient, 6  
dDivides, M, 6  
TelescopingFactor\*x\*is, 1

```

[ 1 0 0 1 ]
[ 1 0 0 1 ]
[ 1 0 0 1 ]
HeightWidthOfArray, 3, 6
ReducedDimensions, 1, 2

```

> CircleDisplay(11)  
# 11 is prime  
# 8k + 3



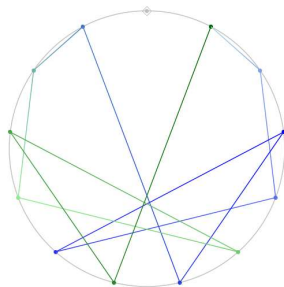
> ArrayDisplay(11)  
dTotient, 10  
dDivides, M, 10  
TelescopingFactor\*x\*is, 1

```

[ 1 0 1 1 ]
[ 1 0 1 1 ]
[ 1 0 1 1 ]
[ 1 0 1 1 ]
[ 1 0 1 1 ]
HeightWidthOfArray, 5, 10
ReducedDimensions, 1, 2

```

> CircleDisplay(13)  
# 13 is prime  
# 8k + 5



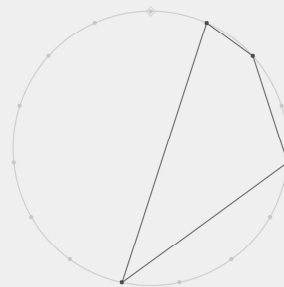
> ArrayDisplay(13)  
dTotient, 12  
dDivides, M, 12  
TelescopingFactor\*x\*is, 1

```

[ 1 1 0 1 ]
[ 1 1 0 1 ]
[ 1 1 0 1 ]
[ 1 1 0 1 ]
[ 1 1 0 1 ]
[ 1 1 0 1 ]
HeightWidthOfArray, 6, 12
ReducedDimensions, 1, 2

```

> CircleDisplay(15)  
# 15 = (3)(5)



> ArrayDisplay(15)  
dTotient, 8  
dDivides, M, 4  
TelescopingFactor\*x\*is, 2

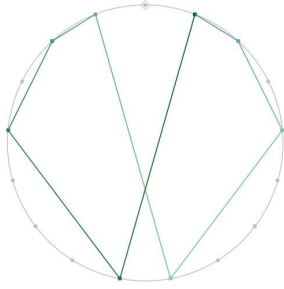
```

[ 1 1 1 1 ]
HeightWidthOfArray, 1, 4
ReducedDimensions, 1, 4

```

> CircleDisplay(17)

# 17 is prime  
#  $8k+1$



> ArrayDisplay(17)

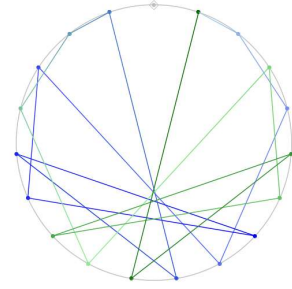
dTotient, 16  
dDivides, M, 8  
TelescopingFactor\*x\*is, 2

```

      1 0 0 0 1
    - - - - -
    1 0 0 0 1
    - - - - -
    1 0 0 0 1
    - - - - -
    1 0 0 0 1
    - - - - -
    HeightWidthOfArray, 4, 8
    ReducedDimensions, 1, 2
  
```

> CircleDisplay(19)

# 19 is prime  
#  $8k+3$



> ArrayDisplay(19)

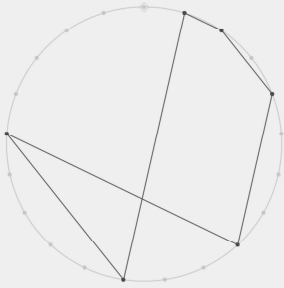
dTotient, 18  
dDivides, M, 18  
TelescopingFactor\*x\*is, 1

```

      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
      1 0 0 1 1
    - - - - -
    HeightWidthOfArray, 9, 18
    ReducedDimensions, 1, 2
  
```

> CircleDisplay(21)

#  $21 = (3)(7)$



> ArrayDisplay(21)

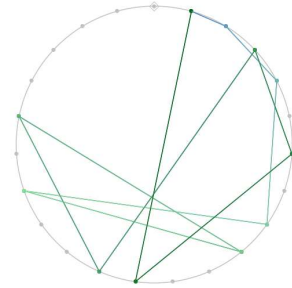
dTotient, 12  
dDivides, M, 6  
TelescopingFactor\*x\*is, 2

```

      1 0 1 0 1
    - - - - -
      1 0 1 0 1
    - - - - -
    HeightWidthOfArray, 2, 6
    ReducedDimensions, 1, 3
  
```

> CircleDisplay(23)

# 23 is prime  
#  $8k+7$



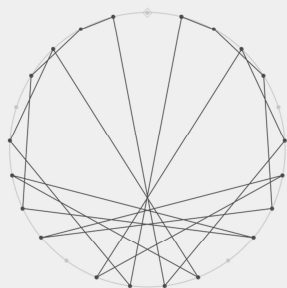
> ArrayDisplay(23)

dTotient, 22  
dDivides, M, 11  
TelescopingFactor\*x\*is, 2

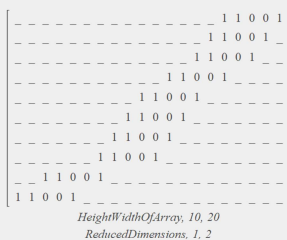
```

      1 0 1 1 1
    - - - - -
      1 0 1 1 1
    - - - - -
      1 0 1 1 1
    - - - - -
      1 0 1 1 1
    - - - - -
    HeightWidthOfArray, 4, 11
    ReducedDimensions, 4, 11
  
```

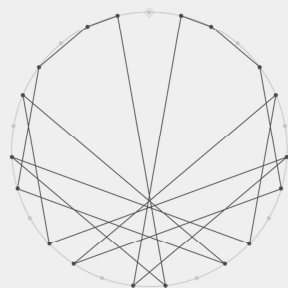
> CircleDisplay(25)  
# 25 = (5<sup>2</sup>)



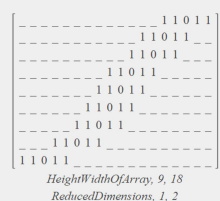
> ArrayDisplay(25)  
dTotient, 20  
dDivides, M, 20  
TelescopingFactor\*x\*is, 1



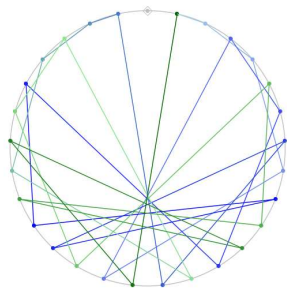
> CircleDisplay(27)  
# 27 = (3<sup>3</sup>)



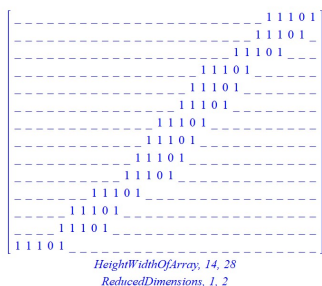
> ArrayDisplay(27)  
dTotient, 18  
dDivides, M, 18  
TelescopingFactor\*x\*is, 1



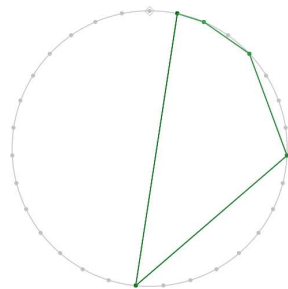
> CircleDisplay(29)  
# 29 is prime  
# 8k + 5



> ArrayDisplay(29)  
dTotient, 28  
dDivides, M, 28  
TelescopingFactor\*x\*is, 1



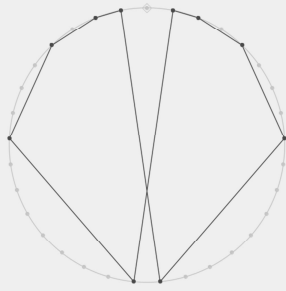
> CircleDisplay(31)  
# 31 is prime  
# 8k + 7



> ArrayDisplay(31)  
dTotient, 30  
dDivides, M, 5  
TelescopingFactor\*x\*is, 6

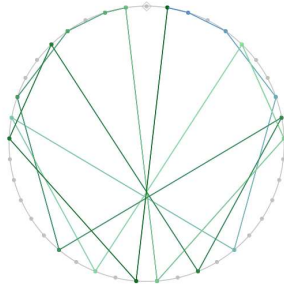


> CircleDisplay(33)  
# 33 = (3)(11)



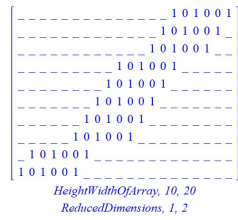
> CircleDisplay(41)

# 41 is prime  
#  $8k+1$



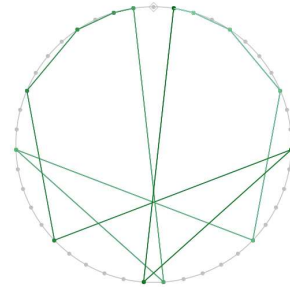
> ArrayDisplay(41)

dTotient, 40  
dDivides, M, 20  
TelescopingFactor\*x\*is, 2



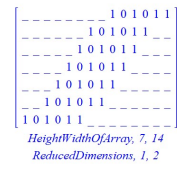
> CircleDisplay(43)

# 43 is prime  
#  $8k+3$



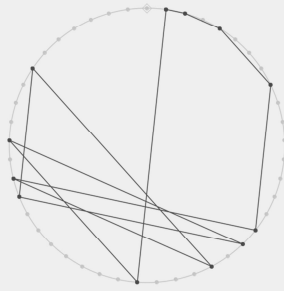
> ArrayDisplay(43)

dTotient, 42  
dDivides, M, 14  
TelescopingFactor\*x\*is, 3



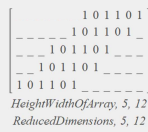
> CircleDisplay(45)

#  $45 = (3^2)(5)$



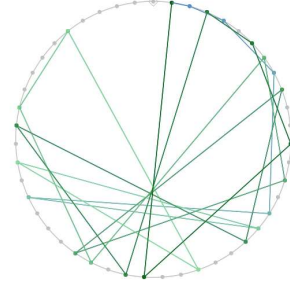
> ArrayDisplay(45)

dTotient, 24  
dDivides, M, 12  
TelescopingFactor\*x\*is, 2



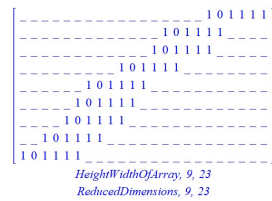
> CircleDisplay(47)

# 47 is prime  
#  $8k+7$

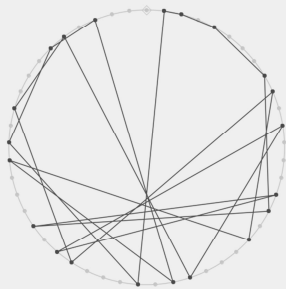


> ArrayDisplay(47)

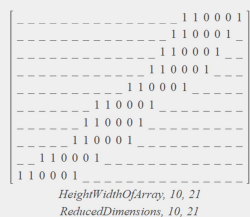
dTotient, 46  
dDivides, M, 23  
TelescopingFactor\*x\*is, 2



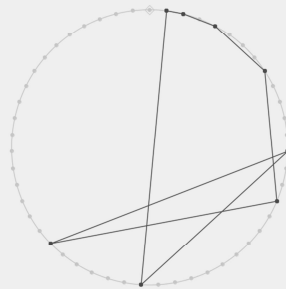
> CircleDisplay(49)  
# 49 = (7<sup>2</sup>)



> ArrayDisplay(49)  
dTotient, 42  
dDivides, M, 21  
TelescopingFactor\*x\*is, 2



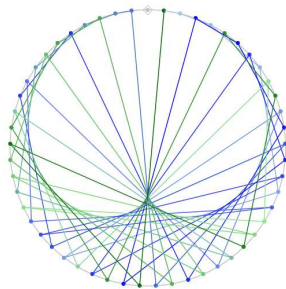
> CircleDisplay(51)  
# 51 = (3)(17)



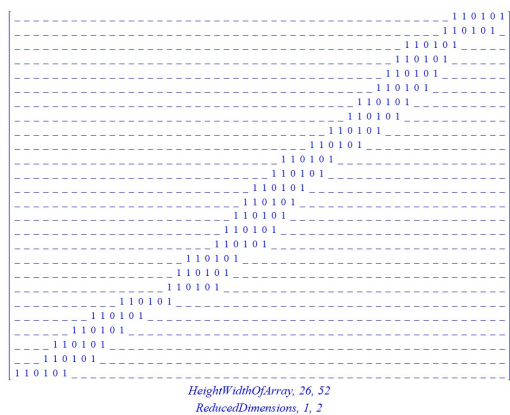
> ArrayDisplay(51)  
dTotient, 32  
dDivides, M, 8  
TelescopingFactor\*x\*is, 4



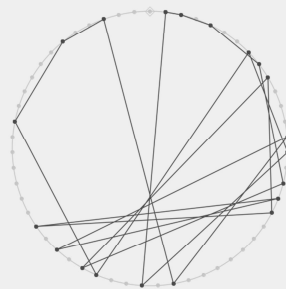
> CircleDisplay(53)  
# 53 is prime  
# 8k + 5



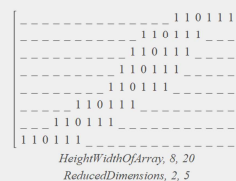
> ArrayDisplay(53)  
dTotient, 52  
dDivides, M, 52  
TelescopingFactor\*x\*is, 1



> CircleDisplay(55)  
# 55 = (5)(11)

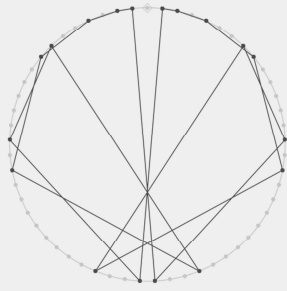


> ArrayDisplay(55)  
dTotient, 40  
dDivides, M, 20  
TelescopingFactor\*x\*is, 2

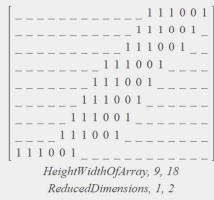




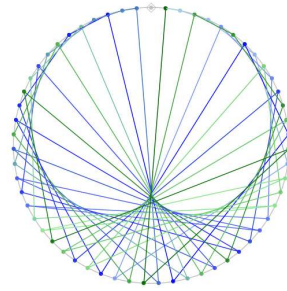
> CircleDisplay(57)  
# 57 = (3)(19)



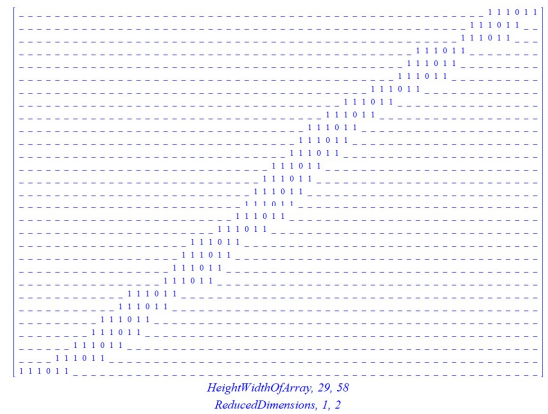
> ArrayDisplay(57)  
dTotient, 36  
dDivides, M, 18  
TelescopingFactor\*x\*is, 2



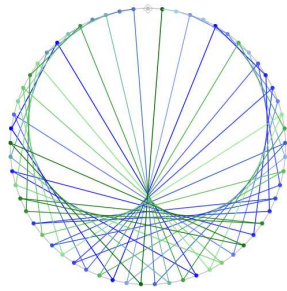
> CircleDisplay(59)  
# 59 is prime  
# 8k+3



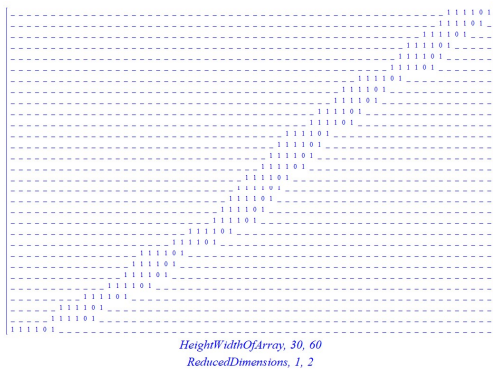
> ArrayDisplay(59)  
dTotient, 58  
dDivides, M, 58  
TelescopingFactor\*x\*is, 1



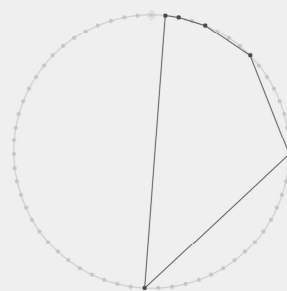
> CircleDisplay(61)  
# 61 is prime  
# 8k+5



> ArrayDisplay(61)  
dTotient, 60  
dDivides, M, 60  
TelescopingFactor\*x\*is, 1



> CircleDisplay(63)  
# 63 = (3^2)(7)



> ArrayDisplay(63)  
dTotient, 36  
dDivides, M, 6  
TelescopingFactor\*x\*is, 6



$$\begin{bmatrix} \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \\ \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \\ \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \\ \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \\ \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \\ \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \\ \_ & \_ & \_ & 1 & 0 & 0 & 0 & 0 & 1 & \_ \end{bmatrix}$$

*HeightWidthOfArray*, 6, 12  
*ReducedDimensions*, 1, 2

[illegible]

HeightWidthOfArray, 11, 22  
ReducedDimensions, 1, 2

*HeightWidthOfArray, 14, 35*  
*ReducedDimensions, 2, 5*

$$\begin{bmatrix} \_ & \_ & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \_ & 1 & 0 & 0 & 1 & 0 & 0 & 1 & \_ \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & \_ & \_ \end{bmatrix}$$

*HeightWidthOfArray*, 3, 9  
*ReducedDimensions*, 1, 3

[illegible]

Figure 1 illustrates the reduction of dimensions in a 15x30 array. The array is represented by a grid of dots. The first 15 rows are labeled "HeightOfArray, 15, 30" and the first 30 columns are labeled "ReducedDimensions, 1, 2". The diagram shows the array being reduced to a single row of 30 dots, which are then grouped into 15 pairs, resulting in 15 dots in the final row.

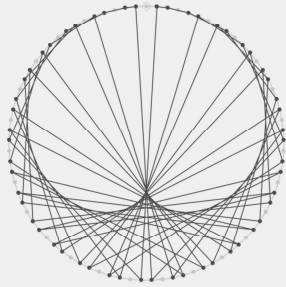
```

                                     1001111
                                1001111
                           1001111
                      1001111
                 1001111
            1001111
        1001111
    1001111
1001111

```

*HeightWidthOfArray, 17, 39  
ReducedDimensions, 17, 39*

> CircleDisplay(81)  
# 81 = (9<sup>2</sup>)

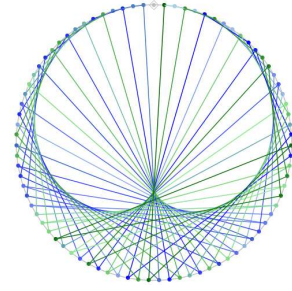


> ArrayDisplay(81)  
dTotient, 54  
dDivides, M, 54  
TelescopingFactor\*x\*is, 1

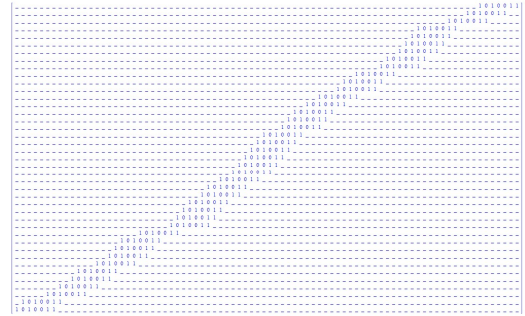


HeightWidthOfArray, 27, 54  
ReducedDimensions, 1, 2

> CircleDisplay(83)  
# 83 is prime  
# 8k+3

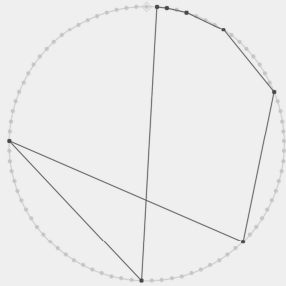


> ArrayDisplay(83)  
dTotient, 82  
dDivides, M, 82  
TelescopingFactor\*x\*is, 1



HeightWidthOfArray, 41, 82  
ReducedDimensions, 1, 2

> CircleDisplay(85)  
# 85 = (5)(17)

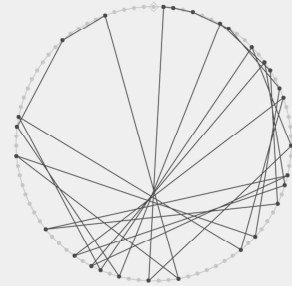


> ArrayDisplay(85)  
dTotient, 64  
dDivides, M, 8  
TelescopingFactor\*x\*is, 8

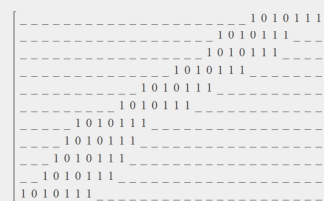


HeightWidthOfArray, 2, 8  
ReducedDimensions, 1, 4

> CircleDisplay(87)  
# 87 = (3)(29)



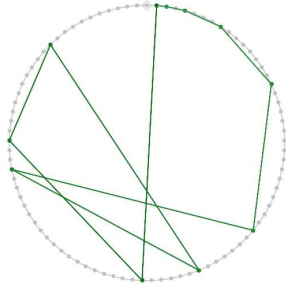
> ArrayDisplay(87)  
dTotient, 56  
dDivides, M, 28  
TelescopingFactor\*x\*is, 2



HeightWidthOfArray, 11, 28  
ReducedDimensions, 11, 28

> CircleDisplay(89)

# 89 is prime  
#  $8k+1$



> ArrayDisplay(89)

dTotient, 88  
dDivides, M, 11  
TelescopingFactor\*x\*is, 8

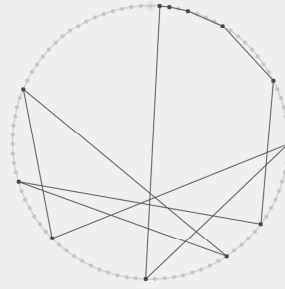
```

  --- 1011001
  --- 1011001
  --- 1011001
  --- 1011001
  HeightWidthOfArray, 4, 11
  ReducedDimensions, 4, 11

```

> CircleDisplay(91)

#  $91 = (7)(13)$



> ArrayDisplay(91)

dTotient, 72  
dDivides, M, 12  
TelescopingFactor\*x\*is, 6

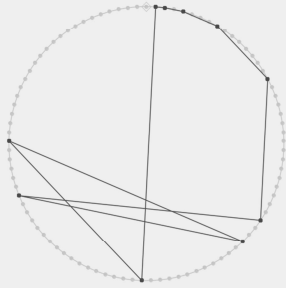
```

  --- 1011011
  --- 1011011
  --- 1011011
  --- 1011011
  HeightWidthOfArray, 4, 12
  ReducedDimensions, 1, 3

```

> CircleDisplay(93)

#  $93 = (3)(31)$



> ArrayDisplay(93)

dTotient, 60  
dDivides, M, 10  
TelescopingFactor\*x\*is, 6

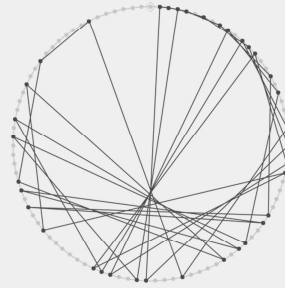
```

  --- 1011101
  --- 1011101
  --- 1011101
  HeightWidthOfArray, 3, 10
  ReducedDimensions, 3, 10

```

> CircleDisplay(95)

#  $95 = (5)(19)$



> ArrayDisplay(95)

dTotient, 72  
dDivides, M, 36  
TelescopingFactor\*x\*is, 2

```

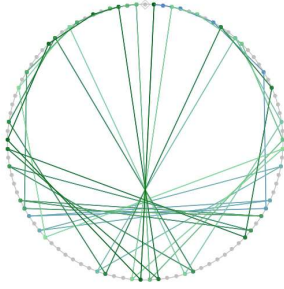
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  --- 1011111
  HeightWidthOfArray, 14, 36
  ReducedDimensions, 7, 18

```



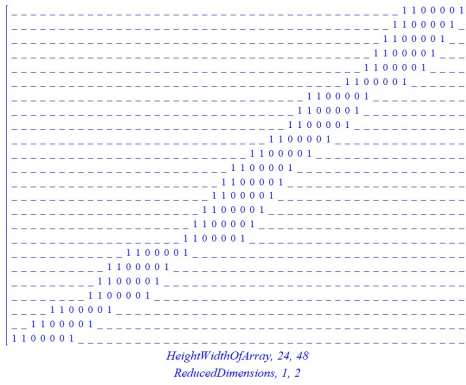
> CircleDisplay(97)

# 97 is prime  
#  $8k+1$



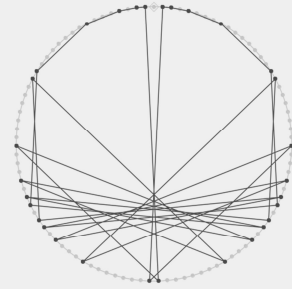
> ArrayDisplay(97)

dTotient, 96  
dDivides, M, 48  
TelescopingFactor\*x\*is, 2



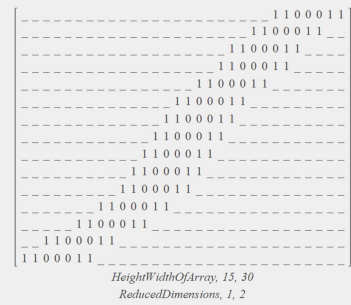
> CircleDisplay(99)

#  $99 = (3^2)(11)$



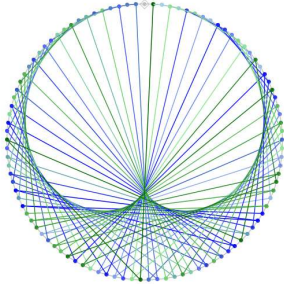
> ArrayDisplay(99)

dTotient, 60  
dDivides, M, 30  
TelescopingFactor\*x\*is, 2



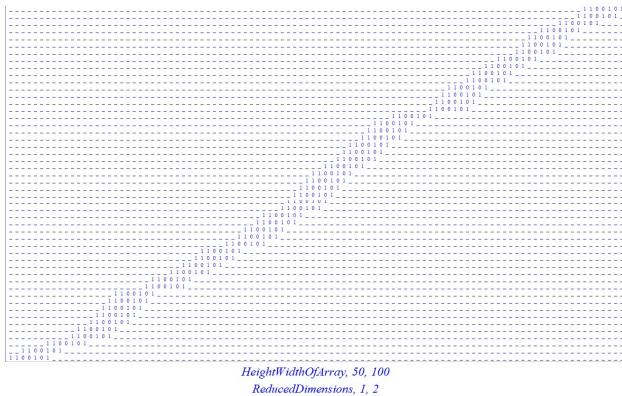
> CircleDisplay(101)

# 101 is prime  
#  $8k+5$



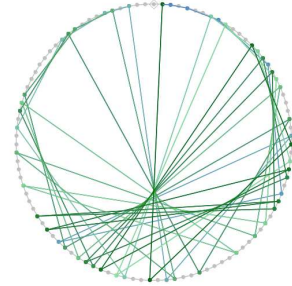
> ArrayDisplay(101)

dTotient, 100  
dDivides, M, 100  
TelescopingFactor\*x\*is, 1



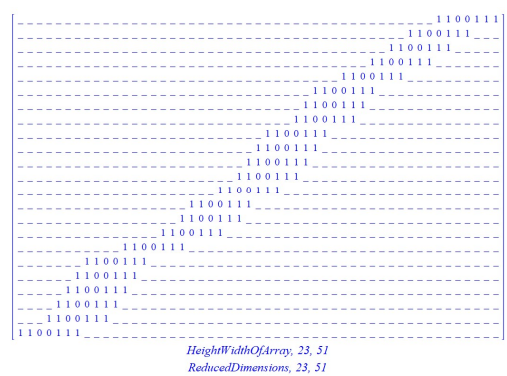
> CircleDisplay(103)

# 103 is prime  
#  $8k+7$



> ArrayDisplay(103)

dTotient, 102  
dDivides, M, 51  
TelescopingFactor\*x\*is, 2



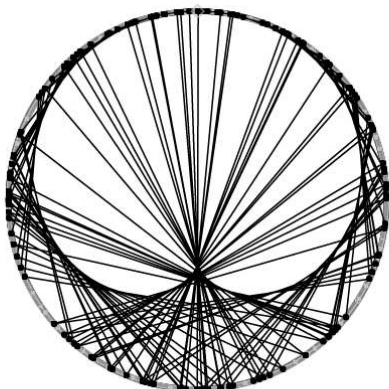
## Appendix D: Circle Data, odd divisors 1897-2039

The following pages contain diagrams of novelty circles, showing odd divisors that numerically are relatively recent years with some personal meaning. This shows us some examples of divisors in the thousands. The display is of circles only, without the arrays (that can be thousands of digits wide). The layout is 8 per page, with the same layout as before, simply doubled:  $8k+1$ ,  $8k+3$ ,  $8k+5$ ,  $8k+7$ ,  $8k+1$ ,  $8k+3$ ,  $8k+5$ ,  $8k+7$ .

Prime divisors are displayed in colour with the same gradient path of blues to greens. Composite divisors are displayed with paths in black.

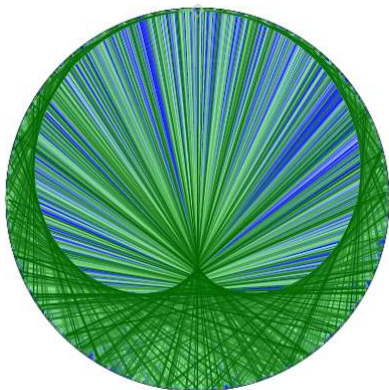
> CircleDisplay(1897)  
# 1897 = (7)(271)

1897



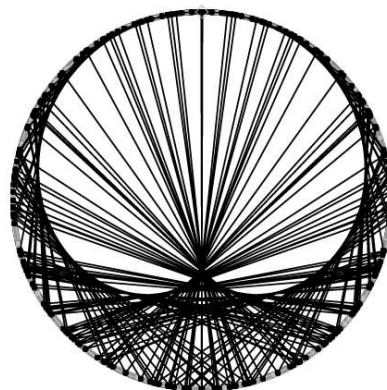
> CircleDisplay(1901)  
# 1901 is prime  
# 8k+5

1901



> CircleDisplay(1899)  
# 1899 = (3^2)(211)

1899



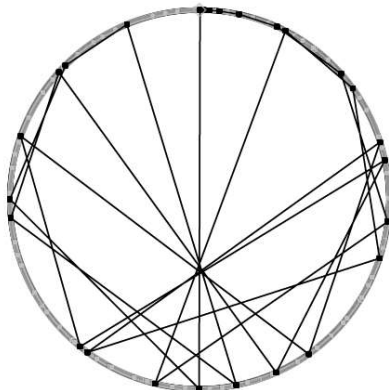
> CircleDisplay(1903)  
# 1903 = (11)(173)

1903



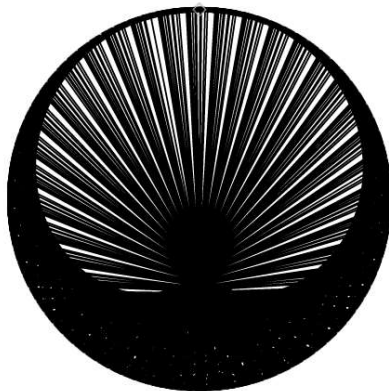
> CircleDisplay(1905)  
# 1905 = (3)(5)(127)

1905



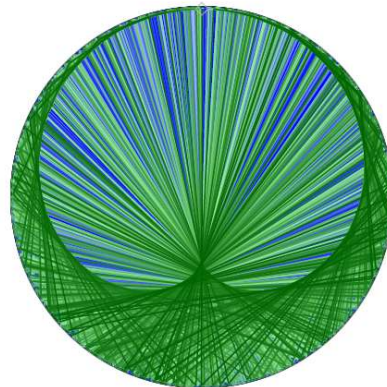
> CircleDisplay(1909)  
# 1909 = (23)(83)

1909



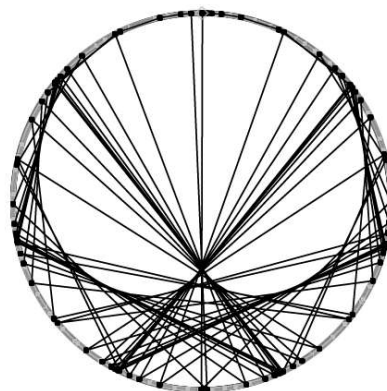
> CircleDisplay(1907)  
# 1907 is prime  
# 8k+3

1907



> CircleDisplay(1911)  
# 1911 = (3)(7^2)(13)

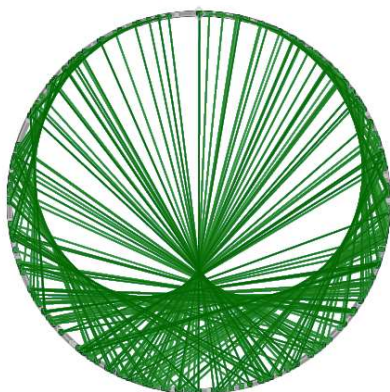
1911





> CircleDisplay(1913)  
# 1913 is prime  
#  $8k+1$

1913



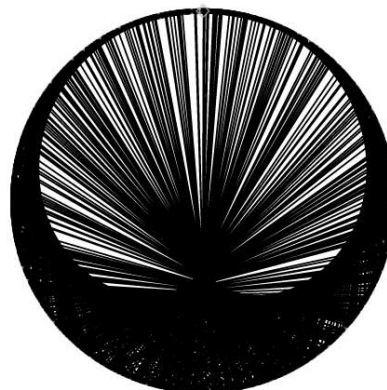
> CircleDisplay(1917)  
# 1917 =  $(3^2)(71)$

1917



> CircleDisplay(1915)  
# 1915 =  $(5)(383)$

1915



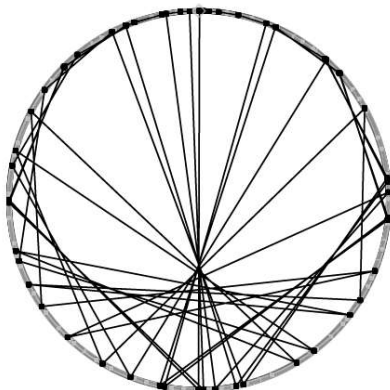
> CircleDisplay(1919)  
# 1919 =  $(19)(101)$

1919



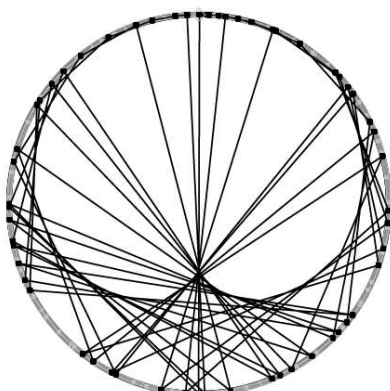
> CircleDisplay(1921)  
# 1921 =  $(17)(113)$

1921



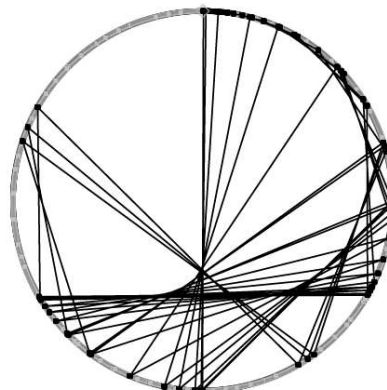
> CircleDisplay(1925)  
# 1925 =  $(5^2)(7)(11)$

1925



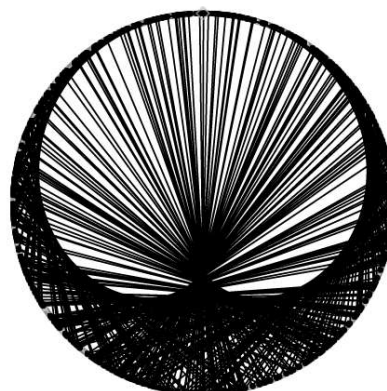
> CircleDisplay(1923)  
# 1923 =  $(3)(641)$

1923



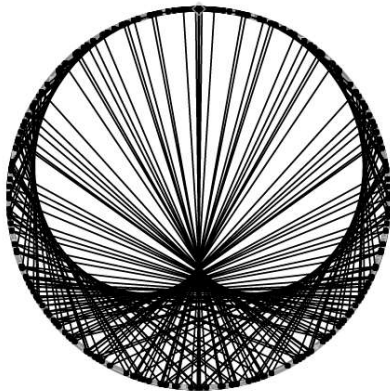
> CircleDisplay(1927)  
# 1927 =  $(41)(47)$

1927



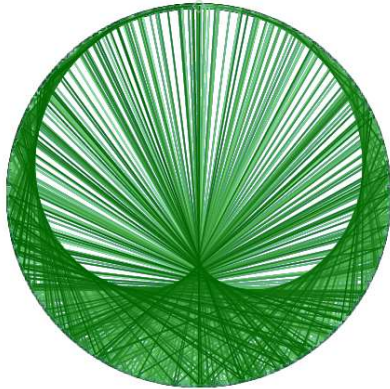
> CircleDisplay(1929)  
# 1929 = (3)(643)

1929



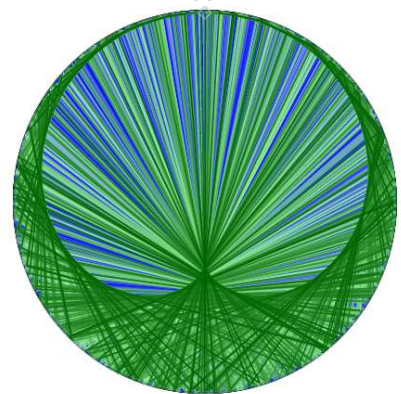
> CircleDisplay(1933)  
# 1933 is prime  
# 8k+5

1933



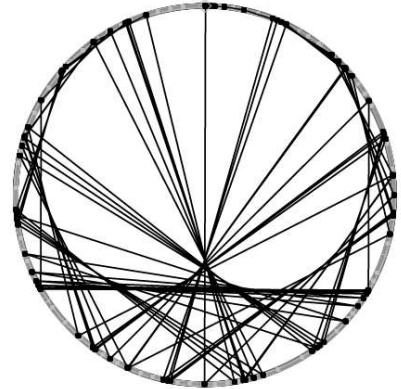
> CircleDisplay(1931)  
# 1931 is prime  
# 8k+3

1931



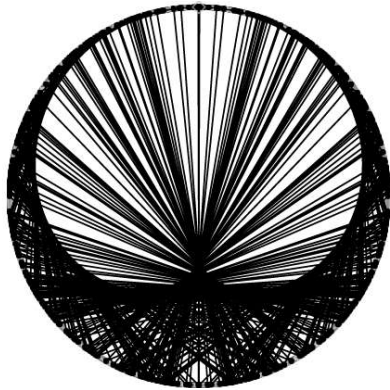
> CircleDisplay(1935)  
# 1935 = (3^2)(5)(43)

1935



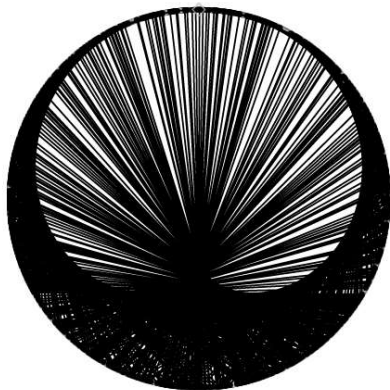
> CircleDisplay(1937)  
# 1937 = (13)(149)

1937



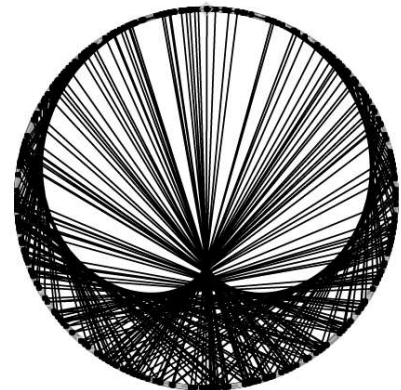
> CircleDisplay(1941)  
# 1941 = (3)(647)

1941



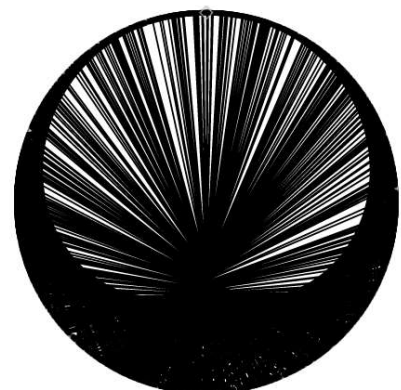
> CircleDisplay(1939)  
# 1939 = (7)(277)

1939



> CircleDisplay(1943)  
# 1943 = (29)(67)

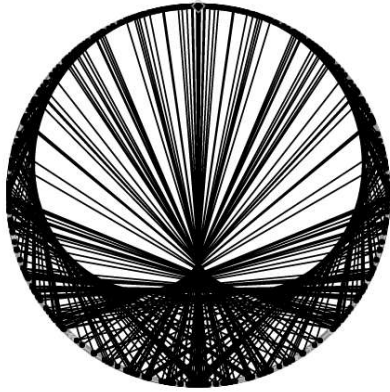
1943





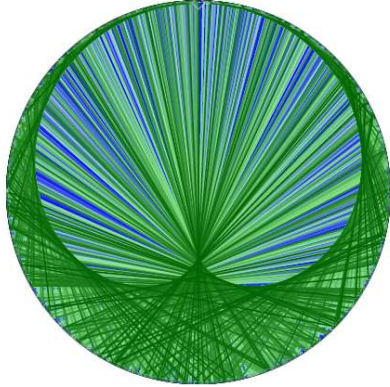
> CircleDisplay(1945)  
# 1945 = (5)(389)

1945



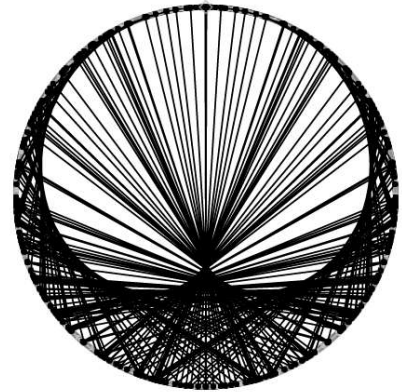
> CircleDisplay(1949)  
# 1949 is prime  
# 8k+5

1949



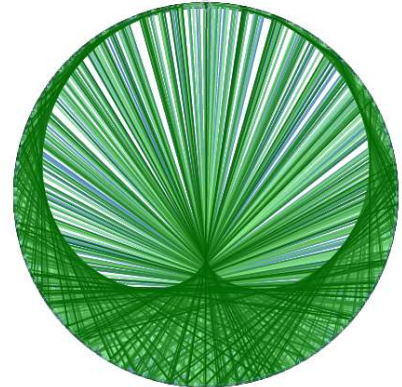
> CircleDisplay(1947)  
# 1947 = (3)(11)(59)

1947



> CircleDisplay(1951)  
# 1951 is prime  
# 8k+7

1951



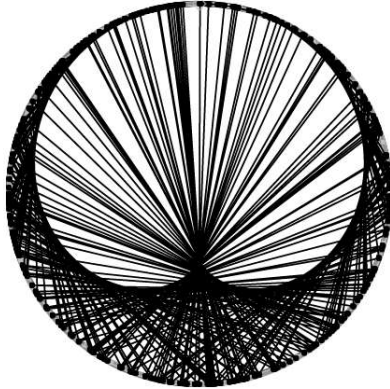
> CircleDisplay(1953)  
# 1953 = (3^2)(7)(31)

1953



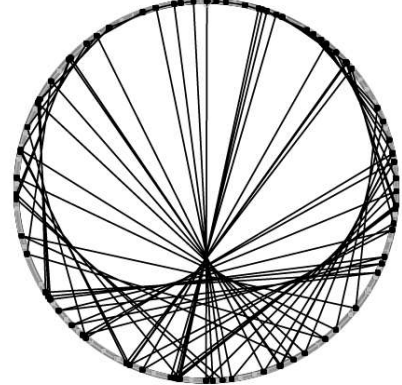
> CircleDisplay(1957)  
# 1957 = (19)(103)

1957



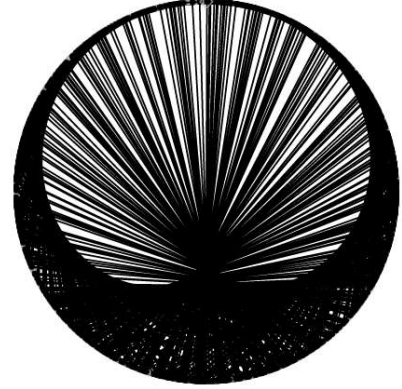
> CircleDisplay(1955)  
# 1955 = (5)(17)(23)

1955



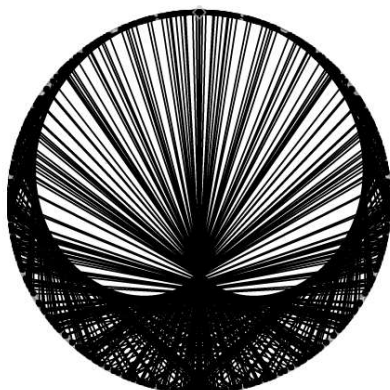
> CircleDisplay(1959)  
# 1959 = (3)(653)

1959



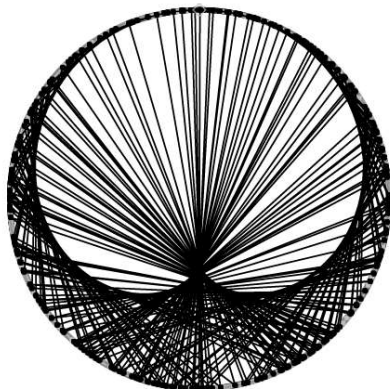
> CircleDisplay(1961)  
# 1961 = (37)(53)

1961



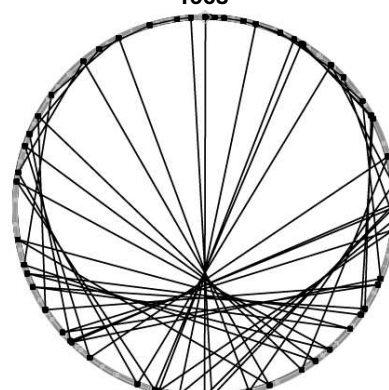
> CircleDisplay(1965)  
# 1965 = (3)(5)(131)

1965



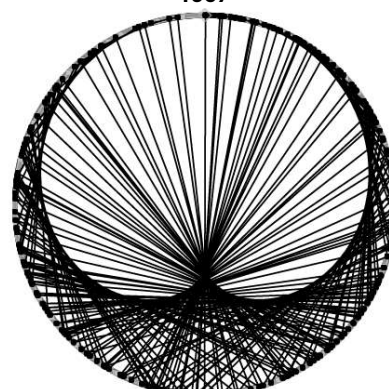
> CircleDisplay(1963)  
# 1963 = (13)(151)

1963



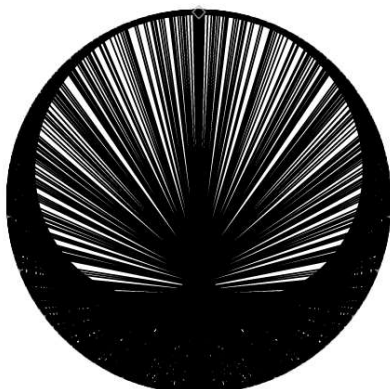
> CircleDisplay(1967)  
# 1967 = (7)(281)

1967



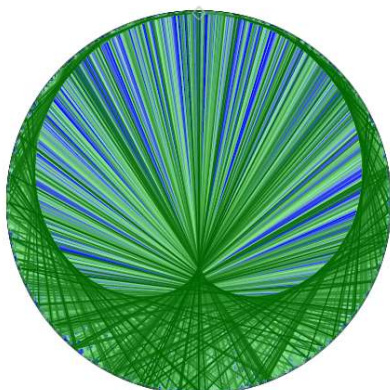
> CircleDisplay(1969)  
# 1969 = (11)(179)

1969



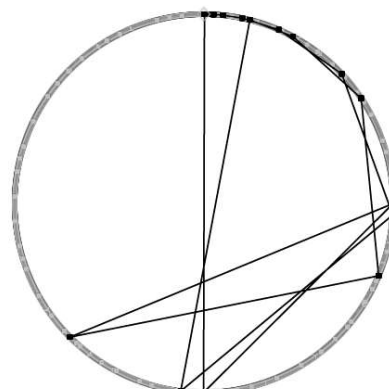
> CircleDisplay(1973)  
# 1973 is prime  
# 8k+5

1973



> CircleDisplay(1971)  
# 1971 = (3^3)(73)

1971



> CircleDisplay(1975)  
# 1975 = (5^2)(79)

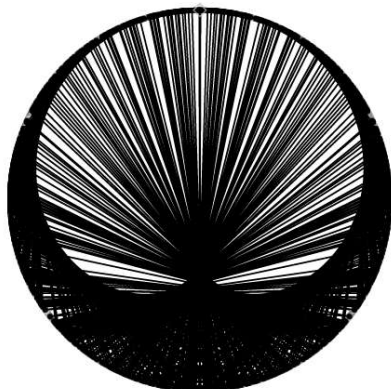
1975





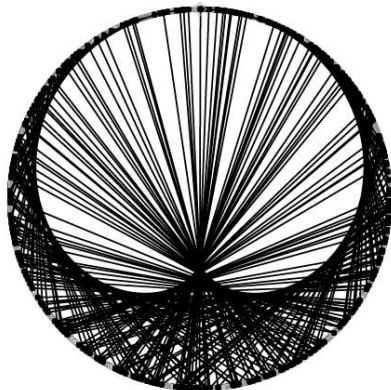
> CircleDisplay(1977)  
# 1977 = (3)(659)

1977



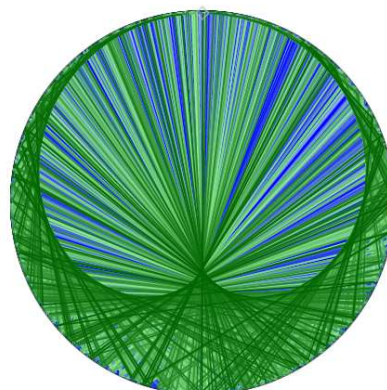
> CircleDisplay(1981)  
# 1981 = (7)(283)

1981



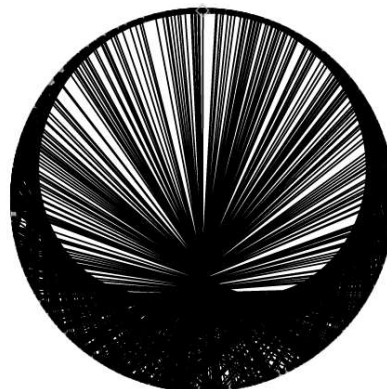
> CircleDisplay(1979)  
# 1979 is prime  
# 8k+3

1979



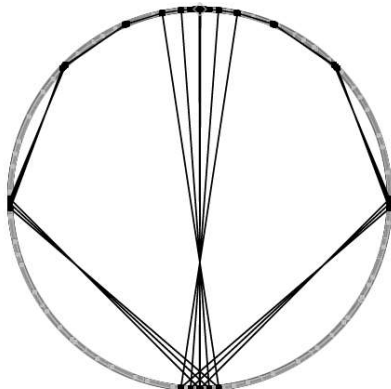
> CircleDisplay(1983)  
# 1983 = (3)(661)

1983



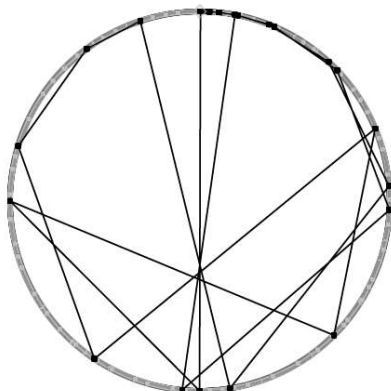
> CircleDisplay(1985)  
# 1985 = (5)(397)

1985



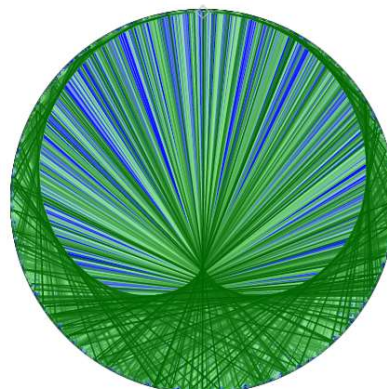
> CircleDisplay(1989)  
# 1989 = (3^2)(13)(17)

1989



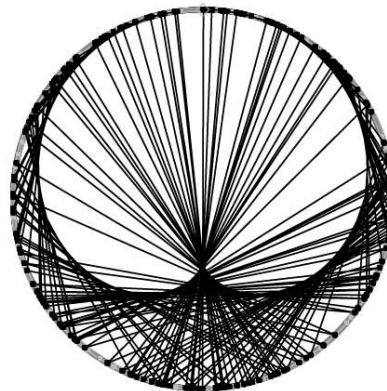
> CircleDisplay(1987)  
# 1987 is prime  
# 8k+3

1987



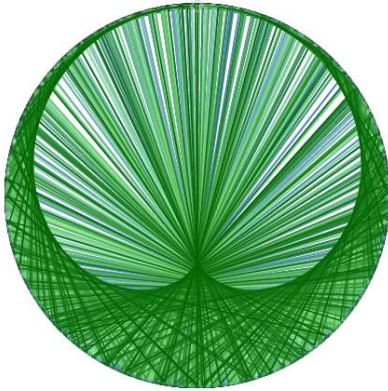
> CircleDisplay(1991)  
# 1991 = (11)(181)

1991



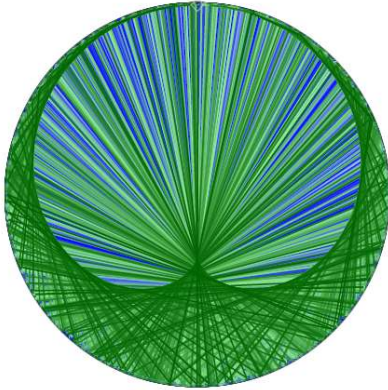
> CircleDisplay(1993)  
# 1993 is prime  
#  $8k+1$

1993



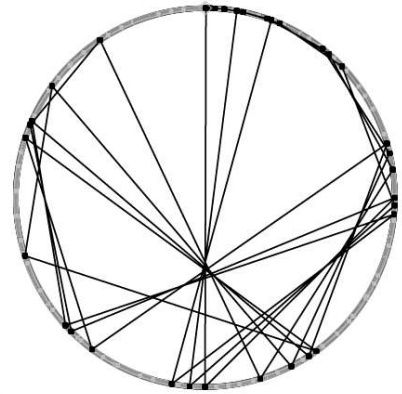
> CircleDisplay(1997)  
# 1997 is prime  
#  $8k+5$

1997



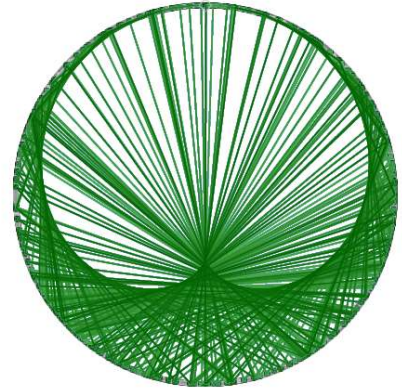
> CircleDisplay(1995)  
# 1995 = (3)(5)(7)(19)

1995



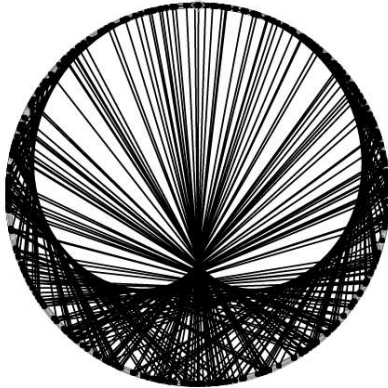
> CircleDisplay(1999)  
# 1999 is prime  
#  $8k+7$

1999



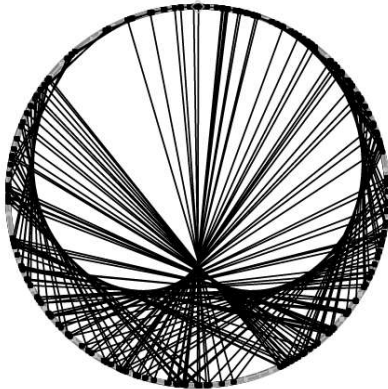
> CircleDisplay(2001)  
# 2001 = (3)(23)(29)

2001



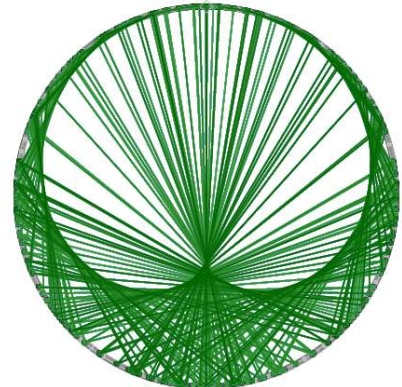
> CircleDisplay(2005)  
# 2005 = (5)(401)

2005



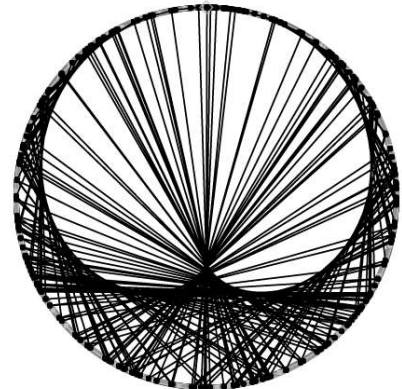
> CircleDisplay(2003)  
# 2003 is prime  
#  $8k+3$

2003



> CircleDisplay(2007)  
# 2007 = (3^2)(223)

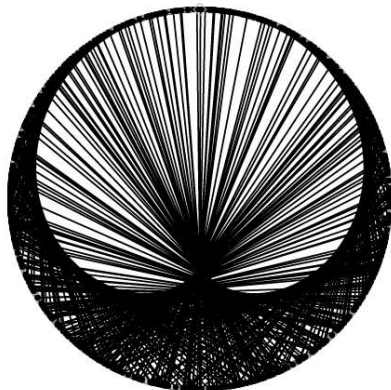
2007





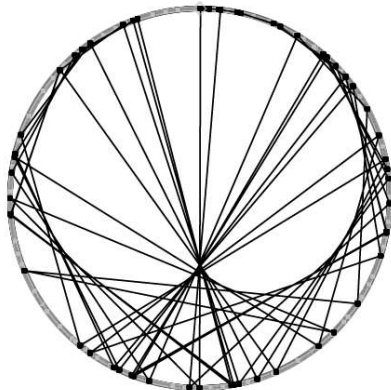
> CircleDisplay(2009)  
# 2009 =  $(7^2)(41)$

2009



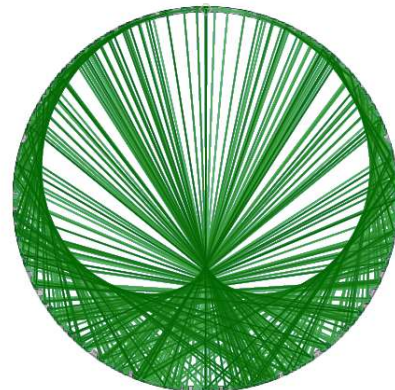
> CircleDisplay(2013)  
# 2013 =  $(3)(11)(61)$

2013



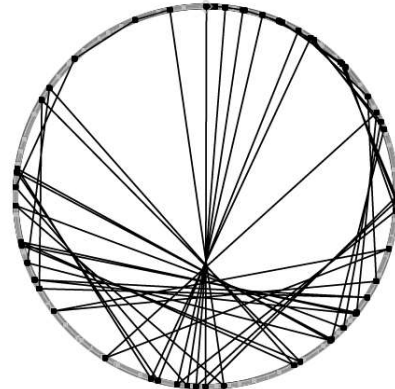
> CircleDisplay(2011)  
# 2011 is prime  
#  $8k+3$

2011



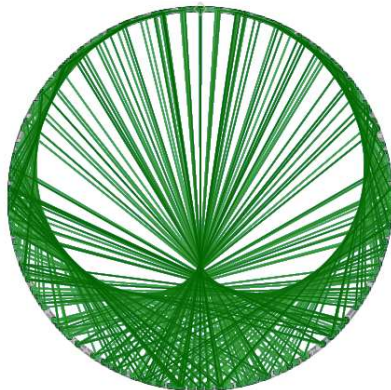
> CircleDisplay(2015)  
# 2015 =  $(5)(13)(31)$

2015



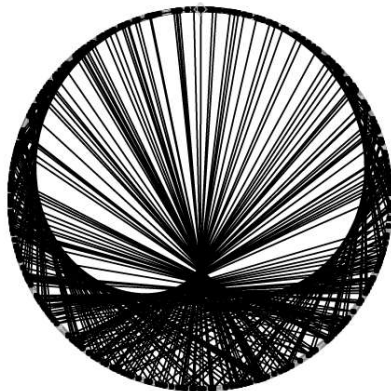
> CircleDisplay(2017)  
# 2017 is prime  
#  $8k+1$

2017



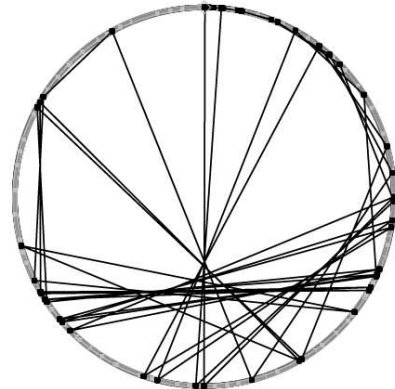
> CircleDisplay(2021)  
# 2021 =  $(43)(47)$

2021



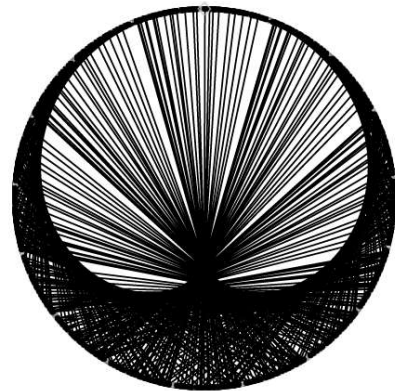
> CircleDisplay(2019)  
# 2019 =  $(3)(673)$

2019



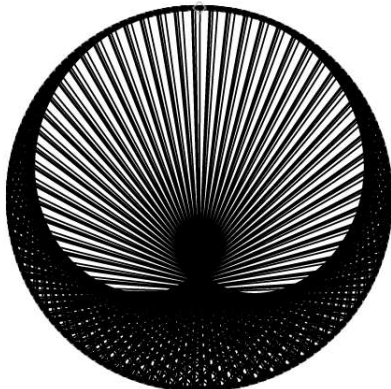
> CircleDisplay(2023)  
# 2023 =  $(7)(17^2)$

2023



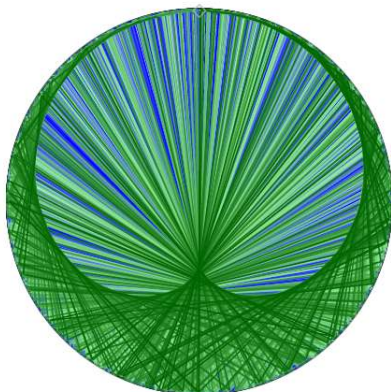
> CircleDisplay(2025)  
# 2025 = (3^9)(5^2)

2025



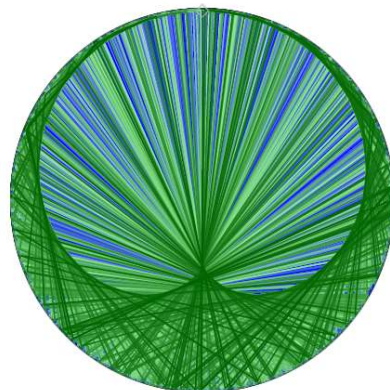
> CircleDisplay(2029)  
# 2029 is prime  
# 8k+5

2029



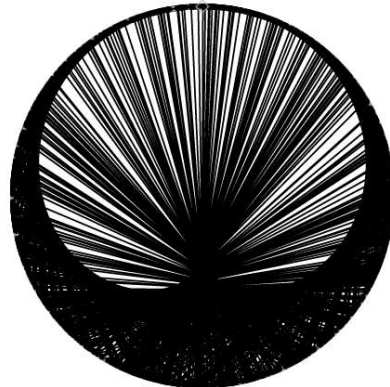
> CircleDisplay(2027)  
# 2027 is prime  
# 8k+3

2027



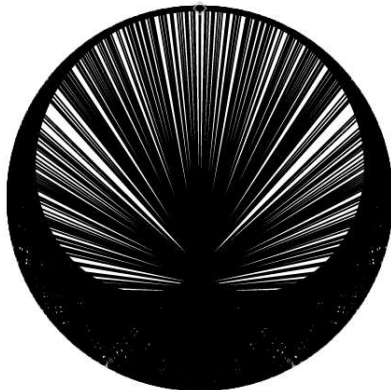
> CircleDisplay(2031)  
# 2031 = (3)(677)

2031



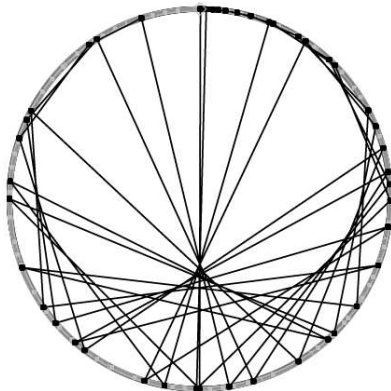
> CircleDisplay(2033)  
# 2033 = (19)(107)

2033



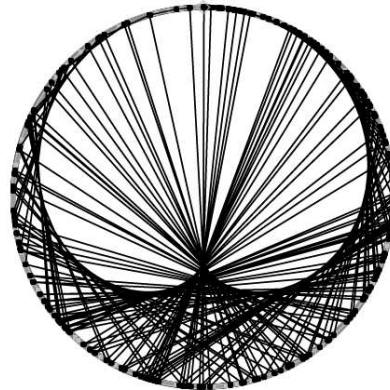
> CircleDisplay(2037)  
# 2037 = (3)(7)(97)

2037



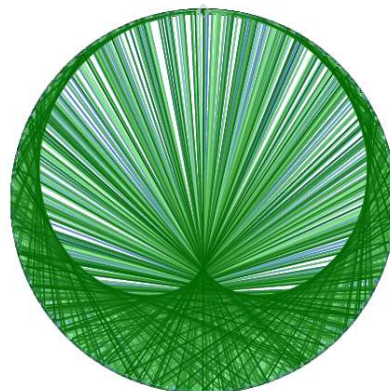
> CircleDisplay(2035)  
# 2035 = (5)(11)(37)

2035



> CircleDisplay(2039)  
# 2039 is prime  
# 8k+7

2039







# Bibliography

- [1] Carmichael number. <https://mathworld.wolfram.com/CarmichaelNumber.html>.
- [2] The online encyclopedia of integer sequences. <https://oeis.org/>.
- [3] Sophie Germain prime. <https://mathworld.wolfram.com/SophieGermainPrime.html>.
- [4] Wagstaff prime. <https://mathworld.wolfram.com/WagstaffPrime.html>.
- [5] Great Internet Mersenne Prime Search (GIMPS), 2024. <https://www.mersenne.org/>, Last accessed 01 Sept, 2024.
- [6] J. W. Bruce. A really trivial proof of the Lucas-Lehmer test. *The American Mathematical Monthly*, 100(4):370–371, 1993.
- [7] H. Davenport. *The Higher Arithmetic*. Cambridge University Press, sixth edition, 1992.
- [8] E. Dummit. 3527 Lecture 32 Applications of quadratic reciprocity, 2024. [https://dummit.cos.northeastern.edu/teaching\\_sp20\\_3527/3527\\_lecture\\_32\\_applications\\_of\\_quadratic\\_reciprocity.pdf](https://dummit.cos.northeastern.edu/teaching_sp20_3527/3527_lecture_32_applications_of_quadratic_reciprocity.pdf).
- [9] F. Farand. Lucas lehmer primality test presentation, May 2021. <https://www.youtube.com/watch?v=NwJOMjGGKzc>.
- [10] B. Haran and J. Grime. Solving seven - numberphile, June 2024. <https://www.youtube.com/watch?v=Ki-M1DJIZsk&t=6s>.

- 
- [11] A. Hone. Huge primes school enrichment project, University of Kent. Participating schools: Simon Langton Grammar School for Boys, Simon Langton Grammar School for Girls, 2023.
  - [12] J. O' Connor, E. Robertson, and J. Daniell. Marin Mersenne biography, 2005. <https://mathshistory.st-andrews.ac.uk/Biographies/Mersenne/>.
  - [13] B. Poonen. Linear recursive sequences, 1998. <https://mathcircle.berkeley.edu/sites/default/files/BMC6/ps/linear.pdf>.
  - [14] PrimePages. Mersenne primes: History, theorems, and lists, 2021. <https://t5k.org/mersenne/>.
  - [15] Ö. J. Rödseth. A note on primality tests for  $N = h \cdot 2^n - 1$ . *BIT Numerical Mathematics*, 34:451–454, 1994.
  - [16] K. H. Rosen. *Elementary Number Theory and its Applications*. AT&T Bell Laboratories, Murray Hill, New Jersey, third edition, 1993.
  - [17] D. R. Stinson. *Cryptography Theory and Practice*. Chapman & Hall / CRC Press, second edition, 2002.