4-2020

On the Mersenne Prime Numbers

Julia VanLandingham
Otterbein University, julia.vanlandingham@otterbein.edu

On the Mersenne Prime Numbers

Otterbein University
Department of Mathematics and Actuarial Science
Westerville, Ohio 43081
Julia C. VanLandingham

16 April 2020

Submitted in partial fulfillment of the requirements for
graduation with Honors

Jeremy S. Moore, Ph.D.
Project Advisor

Ryan Berndt, Ph.D.
Second Reader

Halard Lescinsky, Ph.D.
Honors Representative

Acknowledgments

First and foremost, I would like to thank my project advisor Dr. Jeremy Moore for his help and support throughout this entire project. For all the times staring at a whiteboard, a computer, or a book and understanding lots of proofs and concepts, and also all the other times where we made no progress. Thank you for understanding when I needed to take a break because of exams or other projects, but always pushing me to work hard and learn something new every day. I would also like to thank my second reader Dr. Ryan Berndt for reading my paper thoroughly and giving brutal but incredibly helpful notes. And I would like to thank my honors representative Dr. Halard Lescinsky, for taking time out of his busy schedules even in the midst of a pandemic to serve in this position. Last, but certainly not least, I would like to thank all of my family and friends for being with me through the ups and downs of this entire project. For listening to me talk about prime numbers and theorems all the time, making me stop working and relax when needed, and always encouraging me to jump back in even when I didn't feel like it.

Abstract

The prime numbers have been an important field of research for thousands of years and are intertwined with most other fields of mathematics. One topic that has piqued the interest of mathematicians young and old is the Mersenne prime numbers, which have applications in many mathematics and computer science fields. The Mersenne primes get a lot of attention because there is not much known about them. However, we do have a very simple primality test for Mersenne numbers, which is why the largest currently known primes are Mersenne primes. These primes are also very closely related to another class of numbers called the perfect numbers. In fact, every even perfect number has an underlying Mersenne prime, and for every Mersenne prime we can find an even perfect number. However there is still a major question that remains unanswered: Are there an infinite number of Mersenne primes? In this paper we outline the various known results regarding Mersenne prime numbers and how each of these results helps us to move closer to finding the answer to this age old question.

Contents

1 Introduction **1**

2 Prime Numbers **2**

3 Introductory Topics **4**

3.1 Fermat's Little Theorem 5

3.2 Quadratic Residues 6

4 Quadratic Reciprocity **9**

4.1 Lemmas 9

4.2 The Law of Quadratic Reciprocity 13

4.2.1 Part I 13

4.2.2 Part II 14

4.2.3 Part III 15

5 Lucas-Lehmer Test **18**

5.1 Related Theorems 19

5.2 Proof of the Lucas-Lehmer Test 20

6 Perfect Numbers **25**

6.1 Sigma Function 25

6.2 Proof of the Relationship 27

7 Open Problems and Further Research **30**

8 Appendix **32**

8.1 Definitions 32

1 Introduction

Number theory is one of the oldest fields in mathematics and dates back to Pythagoras and his school of thought around 550 BC. One of the first and most well-known theorems in number theory is the Pythagorean theorem, which states that $a^2 + b^2 = c^2$, where a and b are legs of a right triangle and c is the hypotenuse. Over the years, number theory has evolved and now houses some of the most famous mathematical problems. Examples include the Goldbach conjecture, Twin Primes conjecture, and the Riemann hypothesis [6].

Number theory, and especially the study of prime numbers, is intertwined with many other fields of mathematics. For example, the Riemann hypothesis is one of the most important conjectures in the field of analysis, but is also heavily rooted in number theory. The Riemann hypothesis is closely related to the distribution of prime numbers, a topic that has been raising many questions for hundreds of years [3].

Many cryptographic algorithms used for cybersecurity in the 21^{st} century are also heavily based off number theoretic topics. For example, the RSA encryption scheme, currently one of the most commonly used cryptographic algorithms, is based on the hard problem of factoring large numbers into their prime components.

In 1644, Marin Mersenne (1588-1648), a French monk, made the bold (and ultimately false) assertion that the number $2^n - 1$ was prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127,$ and 257 and that it was not prime for any other $n < 257$. However, it was not until almost 300 years later in the early 1900s that the entire range of Mersenne's conjecture had been completely tested. It was determined that the correct list is actually $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107,$ and 127. It was for this reason that the primes of the form $2^n - 1$ were dubbed the Mersenne primes [2].

Definition 1.1 (Mersenne Number)**.** A number M_n is called a *Mersenne number* if it is of the form $M_n = 2^n - 1$ where $n \in \mathbb{N}$

Definition 1.2 (Mersenne Prime)**.** A prime number M_p is called a *Mersenne prime* if it can be written in the form $M_p = 2^p - 1$ with prime $p \in \mathbb{N},$ and $p \geq 2$

This subset of the prime numbers is also very closely linked to another set of special numbers, the perfect numbers (discussed more in section 6). Table 8.1 lists all of the currently known Mersenne primes along with their corresponding perfect numbers. One of the most pressing questions regarding the prime numbers has always been, just how many are there? As it turns out, there are an infinite number of prime numbers (see theorem 2.1). So the natural next question is, are there also an infinite number of Mersenne primes?

For hundreds of years mathematicians have puzzled over this question and attempted to attack it from all angles, but to no avail thus far. In the past 200 years there has been significant work done with the Mersenne primes in other ways. In December of 2018 the 51^{st} Mersenne prime was discovered. Specifically, we now have a relatively simply primality test for any given Mersenne number along with a concrete characterization of the link between the Mersenne primes and the even perfect numbers. As we move through our discussion of the Mersenne prime numbers keep in mind this important question and consider how each theorem has helped in the search for the answer about the infinitude of the Mersenne primes.

2 Prime Numbers

Before we get into the theorems about Mersenne primes, it is important to first take a brief look at general prime numbers.

Definition 2.1 (Prime Number)**.** A *prime number* is a natural number $p > 1$ that is divisible only by itself and 1.

In about 300 BC, Euclid proved that there are an infinite amount of prime numbers. This was a very important discovery for mathematics. The Fundamental Theorem of Arithmetic uses the fact that there are an infinite number of primes and tells us that every integer

greater than 1 has a unique prime factorization. Thus we can see that the prime numbers are the building blocks of mathematics. The prime numbers are interesting to study because, as far as we know at this time, there is no pattern to their distribution, and thus we do not have a way of generating the next prime.

Theorem 2.1. *There are an infinite number of prime numbers.*

Euclid's proof. By way of contradiction, assume that there are a finite number of prime numbers and that the list $p_1, p_2, ..., p_n$ is an exhaustive list of these primes. Let $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Notice that N is not divisible by any of the primes in our list as we will always have a remainder of one, that is $\frac{N}{p_i} = 1, \ \forall\, i = 1, 2, \ldots, n$. Then we have two options, either N is prime or it is composite. If N is prime then we have found a prime number that was not on our list, a contradiction. If N is composite we know that it must have prime factors by the Fundamental Theorem of Arithmetic. But we know none of our primes $p_1, \ldots, p_n$ are factors. Thus there exists another prime that is a factor of N that is not on our original list, a contradiction. Hence, there must be an infinite number of prime numbers. ■

Thus we know that there are infinitely many primes, but we also know that there are an infinite number of some specific types of primes too. For instance, we know that there are infinitely many primes congruent to 3 mod 4. The following proof of this fact is outlined in chapter 12 of [7]. Before we prove this, note that all primes > 2 must be either 1 or 3 mod 4. If a prime p was congruent to 0 or 2 mod 4 then this would mean that 2 divides p and it would not be prime.

Theorem 2.2. *There are infinitely many primes congruent to 3 modulo 4.*

Proof. By way of contradiction, suppose that we have a complete and finite list of all the primes that are congruent to 3 modulo 4,

$$3, p_1, p_2, \ldots, p_r.$$

Then let's consider the number

$$N = 4p_1p_2 \dots p_r + 3.$$

It is important to note here that we have not included the prime 3 in the product above. Then we know that N can be factored into a product of primes,

$$N = q_1q_2 \dots q_s.$$

First, we need to show that one of these q's must be congruent to 3 modulo 4. If this was not true then they all are congruent to 1 mod 4 and thus N is congruent to 1 mod 4. But by the way that we have defined it, N is congruent to 3 mod 4. Thus at least one of the qs has to be 3 mod 4, call this prime q_i.

Second, we need to show that this q_i was not on our original list. Because of how q_i has been found we know that it evenly divides N. However, notice that none of our original primes $p_1, \dots, p_r$ divided N. Thus q_i is not from our original list and our list is not complete, a contradiction. ■

The proof that there are an infinite number of primes congruent to 1 mod 4 is very similar to the above and thus we will not show it here. So we know that there are infinitely many primes that are congruent to 1 or 3 mod 4. A natural next question is, are there other kinds of primes that have this kind of structure? In fact there are! Dirichlet generalized this idea in the 1830s. The proof for this theorem is unfortunately much too difficult to outline here, so only the statement of this important theorem will be provided.

Theorem 2.3 (Dirichlet's Theorem)**.** *Let a and m be integers with gcd$(a, m) = 1$, then there are infinitely many prime numbers p such that $p \equiv a \mod m$.*

3 Introductory Topics

As we continue our exploration of the Mersenne primes, we must stop to prove some very important and helpful theorems. The importance of these theorems may not be very clear

at first but each of them will play a very important role as we work towards the primality testing of Mersenne primes. In order to prove the theorems that may seem more important and whose functions are more impressive, we must first lay our foundation by proving these building blocks.

3.1 Fermat's Little Theorem

Despite its misleading name, Fermat's Little Theorem is a very important theorem in number theory. This theorem not only gives us another way of looking at a prime p, but also gives us a simple primality test for numbers of reasonably small size. For this reason, it was one of the earliest efficient ways of primality testing. However before we can prove Fermat's Little Theorem, we must first prove an important lemma that will come up many times in following sections. We will also need the following theorem, but since this is tangent to our topic right now, the proof will be left for the reader's exploration.

Theorem 3.1 (Prime Divisibility Property)**.** *Let p be a prime number, and suppose that p divides the product $a_1 a_2 \dots a_r$. Then p divide at least one of the factors $a_1 a_2 \dots a_r$.*

The proof of the above can be found in chapter 7 of [7] and the below can be found in chapter 9 of [7].

Lemma 3.1. *Let p be a prime number and let a be a number with $a \not\equiv 0 \mod p$. Then the numbers $a, 2a, 3a, \dots, (p-1)a \mod p$ are the same as the numbers $1, 2, 3, \dots, (p-1)$ mod p, although they may be in a different order.*

Proof. The list $a, 2a, 3a, \dots, (p-1)a$ contains $p-1$ numbers, and clearly none of them are divisible by p. Suppose that we take two numbers ja and ka in this list, and suppose that they are congruent mod p, so

$$ja \equiv ka \mod p.$$

Then $p|(j-k)a$, so $p|(j-k)$ by theorem 3.1 and since we are assuming that p does not divide a. We know that

$$1 \leq j, k \leq p-1, \text{ so } |j-k| < p-1.$$

There is only one number with absolute value less than $p-1$ that is divisible by p, and that is 0. Thus, $j = k$. This shows that different multiples in the list $a, 2a, 3a, \ldots, (p-1)a$ are distinct modulo p. So we know that the list $a, 2a, 3a, \ldots, (p-1)a$ contains $p-1$ distinct nonzero values modulo p. But there are only $p-1$ distinct nonzero values modulo p, those are the numbers $1, 2, 3, \ldots, (p-1)$. Hence, the list $a, 2a, 3a, \ldots, (p-1)a$ and the list $1, 2, 3, \ldots, (p-1)$ must contain the same numbers modulo p, although the numbers may appear in different orders. ■

Now that we have this lemma under our belt we can move on to the proof of Fermat's Little Theorem. This proof is from chapter 9 of [7].

Theorem 3.2 (Fermat's Little Theorem)**.** *Let p be a prime number, and let a be any number with $a \not\equiv 0 \mod p$. Then $a^p \equiv a \mod p$ or equivalently, $a^{p-1} \equiv 1 \mod p$*

Proof. By lemma 3.1, we know that the lists $a, 2a, 3a, \ldots, (p-1)a$ and $1, 2, 3, \ldots, (p-1)$ are the same modulo p. Thus they have the same product, in other words

$$a(2a)(3a)\ldots((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \mod p.$$

Next we reorganize the $(p-1)$ copies of a in the left hand side, resulting in

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

Now observe that $(p-1)!$ is coprime to p, so we may cancel it from both sides to obtain

$$a^{p-1} \equiv 1 \mod p.$$ ■

3.2 Quadratic Residues

We now consider another important question in number theory and some of its applications, when is a number a square modulo p? However, before we get into much discussion

of this question we must lay out some definitions and notation that will be used throughout the rest of the paper.

Definition 3.1 (Quadratic Residue (QR))**.** A nonzero number that is congruent to a square modulo p is said to be a *quadratic residue* modulo p.

Definition 3.2 (Quadratic Nonresidue (NR))**.** A nonzero number that is not congruent to a square modulo p is said to be a *quadratic nonresidue* modulo p.

Definition 3.3. The *Legendre symbol* of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod p} \\ -1 & \text{if } a \text{ is a nonresidue mod p} \end{cases}$$

Quadratic Residues are an important topic in number theory, so it is not surprising that they make an appearance in many results and proofs related to the Mersenne primes. We use the Legendre symbol as a quantitative representation of whether a number a is a quadratic residue mod p or not. Euler's Criterion gives us another way of writing the Legendre symbol of a number. This will prove to be essential further down the road as we look into more complicated theorems. Before we get into this proof however, we must state two other theorems that we will employ. Because these theorems are not directly related to our topic, we will simply state their conclusions and leave the proofs for the reader to explore. The first theorem here tells us exactly how many roots mod p there may be for a given polynomial. The proof of this theorem can be found in chapter 8 of [7].

Theorem 3.3. *Let p be a prime number and let*

$$f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d$$

be a polynomial of degree $d \geq 1$ with integer coefficients and with $p \not| a_0$. Then the congruence

$$f(x) = 0 \mod p$$

has at most d incongruent solutions.

The next theorem tells us exactly how many quadratic residues and nonresidues we will have for any given prime p. The proof of this theorem can be found in chapter 20 of [7].

Theorem 3.4. *Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues modulo p and exactly $\frac{p-1}{2}$ nonresidues modulo p.*

Now we are ready to prove Euler's criterion regarding the Legendre symbol of a number mod p. This proof is outlined in chapter 21 of [7]. For clarity, throughout the rest of this paper let $P = \frac{p-1}{2}$, this notation will be used heavily in section 4 in particular.

Theorem 3.5 (Euler's Criterion)**.** *Let p be an odd prime. Then*

$$a^P \equiv \left(\frac{a}{p}\right) \mod p, \text{ with } a \in \mathbb{Z}.$$

Proof. Suppose first that a is a quadratic residue, say $a \equiv b^2 \mod p$. Then by Fermat's Little Theorem (3.2) we know that

$$a^P \equiv (b^2)^P = b^{p-1} \equiv 1 \mod p.$$

Hence,

$$a^P \equiv \left(\frac{a}{p}\right) \mod p,$$

Consider the congruence $X^P - 1 \equiv 0 \mod p$. We have just proven that every quadratic residue is a solution to this congruence, and we know that there are exactly $\frac{1}{2}(p-1)$ distinct quadratic residues by theorem 3.4. From theorem 3.3 we know that this congruence can have at most $\frac{1}{2}(p-1)$ distinct solutions. Hence,

$$\{\text{solutions to } X^P - 1 \equiv 0 \mod p\} = \{\text{quadratic residues modulo } p\}.$$

Now let a be a nonresidue. Fermat's Little Theorem (3.2) tells us that $a^{p-1} \equiv 1 \mod p$ so,

$$0 \equiv a^{p-1} - 1 \equiv (a^P - 1)(a^P + 1) \mod p.$$

The first factor is not 0 modulo p, because we already showed that the solutions to $X^P - 1 \equiv 0 \mod p$ are the quadratic residues. Hence the second factor must be 0 modulo p. Thus,

$$a^P \equiv -1 = \left(\frac{a}{p}\right) \mod p.$$

Thus the theorem holds true for all integers. ■

4 Quadratic Reciprocity

One of the most well known and powerful theorems in number theory is the Law of Quadratic Reciprocity. It gives us a concrete set of rules identifying if a prime q is a quadratic residue mod p and thus what its Legendre symbol will be. This will be imperative for the proof of the Lucas-Lehmer test in section 5. There are three distinct parts to this theorem. The first part gives the conditions for when -1 is a QR mod p. The second part gives the conditions for when 2 is a QR mod p. Lastly, the third, and most complicated, part gives us the conditions for all other primes. Before we can fully dive into the proof of this theorem we must prove some lemmas that are outlined in chapter 23 of [7]. You may notice as we go through this section that many of these theorems seem to be stating things that are very similar to each other. Each of these theorems gives us a slightly different way of looking at the definitions we have. Later in section 5.3 and theorem 4.2 we will string many of these theorems together in order to get the desired result from the information we have.

4.1 Lemmas

The first lemma we will look at gives us a new way of looking at the list of numbers $a, 2a, 3a, \ldots, Pa$. This will let us look at the number of negatives that we have once this list is reduced into the given range, this value will come up many times in future proofs.

Lemma 4.1. *Let $a \in \mathbb{Z}$ and $a \not\equiv 0 \mod p$. When the numbers $a, 2a, 3a, \ldots, Pa$ are reduced modulo p into the range $-P$ to P, the reduced values are $\pm 1, \pm 2, \ldots, \pm P$ in some order, with each number appearing once with either a plus or minus sign.*

Proof. Write each multiple ka as $ka = pq_k + r_k$ with $-P \leq r_k \leq P$.
Suppose that two of the r_k values are either the same or negatives for each other. Say $r_i = er_j$ with $e = \pm 1$. Then,

$$ia - eja = (pq_i + r_i) - e(pq_j + r_j) = p(q_i - eq_j).$$

So, $p|a(i - ej)$ but p is prime and a is not divisible by p, so then $p|(i - ej)$. However,

$$|i - ej| \leq |i| + |ej| = i + j \leq P + P = p - 1.$$

So the only way for $i - ej$ to be divisible by p is to have $i - ej = 0$. Since $e = \pm 1$ and i and j are positive then $i = j$. Thus the numbers $r_1, r_2, \ldots, r_P$ are all different, even if we change their signs. Hence it follows that each of the numbers $1, 2, \ldots, P$ with a plus or minus sign appears exactly once in the list of numbers $r_1, r_2, \ldots, r_P$. ■

Before we move on to our next lemma we need the following definitions

Definition 4.1. The *floor function*, denoted $\lfloor t \rfloor$, is the largest integer n such that $n \leq t$.

Definition 4.2. $\mu(a, p)$ is the number of integers in the list $a, 2a, \ldots, Pa$ that become negative when they are reduced modulo p into the interval from $-P$ to P.

Notice that the floor function will effectively just truncate the decimal portion of the number and leave the integer value. Now we are ready to proceed with the proof of our second lemma that will help us prove the Law of Quadratic Reciprocity (4.2). This lemma will give us another way of using $\mu(a, p)$ so that we can relate it better to the number of points we can count. This will come up in theorem 4.2 as we will use a graphical approach to the proof.

Lemma 4.2. *Let p be an odd prime and $a \not\equiv 0 \mod p$ be an odd integer. Then*

$$\sum \left\lfloor \frac{ka}{p} \right\rfloor = \mu(a,p) \mod 2.$$

Proof. We write each multiple of ka as $ka = pq_k + r_k$ with $-P < r_k < P$.
Divide by p to obtain $\dfrac{ka}{p} = q_k + \dfrac{r_k}{p}$. Notice that

$$-\frac{1}{2} < -\frac{1}{2} + \frac{1}{2p} < \frac{r_k}{p} < \frac{1}{2} - \frac{1}{2p} < \frac{1}{2}. \text{ Thus, } -\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}.$$

Taking the floor of both sides we get

$$\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0 \\ q_k - 1 & \text{if } r_k < 0 \end{cases}$$

So adding the values for $\left\lfloor \dfrac{ka}{p} \right\rfloor$, $k = 1, 2, \ldots, P$ we get

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{P} q_k - \mu(a,p) \tag{4.0.1}$$

We need the sum of the q_k'$s \mod 2$. Reducing the formula $ka = q_k p + r_k \mod 2$ and using the fact that a and p are both odd we get $k = q_k + r_k \mod 2$. Thus,

$$\sum_{k=1}^{P} k = \sum_{k=1}^{P} q_k + \sum_{k=1}^{P} r_k \mod 2 \tag{4.0.2}$$

But by lemma 4.1 we know that $r_1, r_2, \ldots, r_P$ are equal to $(\pm 1)(\pm 2)(\pm 3)\ldots(\pm P)$ in some order with each number appearing once with either a plus or minus sign. Since we are working mod 2 the signs are not relevant. Therefore,

$$\sum_{k=1}^{P} r_k \equiv 1 + 2 + \cdots + P \mod 2.$$

Then the sums Σk and Σr_k in Equation (4.0.2) are congruent mod 2. Hence,

$$\sum_{k=1}^{P} q_k \equiv 0 \mod 2.$$

So reducing Equation (4.0.1) mod 2 we get

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{P} q_k - \mu(a,p) = \mu(a,p) \mod 2.$$

■

Gauss's Criterion, like Euler's Criterion (3.5) from above, gives us another way of looking at the Legendre symbol of an equation. This time we are looking at it as it relates to $\mu(a,p)$. Note that at this point you may begin to see how a lot of these theorems are going to string together in order for us to relate two quantities that may be seemingly unrelated at first.

Theorem 4.1 (Gauss's Criterion)**.** *Let p be an odd prime, let a be an integer $\not\equiv 0 \mod p$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}.$$

Proof. Take the list of numbers $a, 2a, \ldots, Pa$ and multiply them together. Then the product is,

$$a \cdot 2a \cdot \ldots \cdot Pa = a^P(1 \cdot 2 \cdot 3 \cdot \ldots \cdot P) = a^P \cdot P! \tag{4.1.1}$$

By lemma 4.1 we know

$$a \cdot 2a \cdot \ldots \cdot Pa \equiv (\pm 1)(\pm 2)(\pm 3)\ldots(\pm P) \mod p$$

where the number of minus signs is $\mu(a,p)$. Then,

$$a \cdot 2a \cdot \ldots \cdot Pa \equiv (-1)^{\mu(a,p)} 1 \cdot 2 \cdot 3 \cdot \ldots \cdot P \mod p \equiv (-1)^{\mu(a,p)} P! \mod p \tag{4.1.2}$$

Combining equations (4.1.1) and (4.1.2) we see $a^P P! \equiv (-1)^{\mu(a,p)} P! \mod p$. Since $P!$ and p are coprime, we may cancel $P!$ from both sides, yielding

$$a^P \equiv (-1)^{\mu(a,p)} \mod p.$$

But by theorem 3.5 we know

$$a^P \equiv \left(\frac{a}{p}\right) \mod p.$$

Thus $\left(\frac{a}{p}\right) \equiv (-1)^{\mu(a,p)} \mod p$. This means that $\left(\frac{a}{p}\right) - (-1)^{\mu(a,p)}$ is divisible by p. But this will only ever take the quantity 2, -2, or 0 while $p \geq 3$. Then $\left(\frac{a}{p}\right) - (-1)^{\mu(a,p)} = 0$. ■

4.2 The Law of Quadratic Reciprocity

Now we finally have all of the theorems we will need for the proof of the Law of Quadratic Reciprocity. This theorem, as discussed above, will allow us in all cases to tell exactly what the Legendre symbol of a number q will be $\mod p$. There are three distinct cases that we must handle in our proof: when $q = -1$, $q = 2$, or q is another odd prime number.

Theorem 4.2 (The Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes.*

PART I

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \mod 4 \\ -1 \text{ if } p \equiv 3 \mod 4 \end{cases}$$

PART II

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \mod 8 \\ -1 \text{ if } p \equiv 3 \mod 8 \end{cases}$$

PART III

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } q \equiv 1 \mod 4 \text{ or } p \equiv 1 \mod 4 \\ -\left(\frac{p}{q}\right) & \text{if } q \equiv 3 \mod 4 \text{ and } p \equiv 3 \mod 4 \end{cases}$$

4.2.1 Part I

We will start off with the case concerning -1 modulo p. Silverman outlines this proof in chapter 21 of [7].

Proof: PART I. Theorem 3.5 says that $(-1)^P \equiv \left(\frac{-1}{p}\right) \mod p$. First we will suppose $p \equiv 1 \mod 4$ say $p = 4k + 1$. Then

$$(-1)^P = (-1)^{2k} = 1, \text{ so } 1 \equiv \left(\frac{-1}{p}\right) \mod p.$$

Thus if $p \equiv 1 \mod 4$ then $\left(\frac{-1}{p}\right) = 1$.

Now suppose that $p \equiv 3 \mod 4$ say $p = 4k + 3$. Then

$$(-1)^P = (-1)^{2k+1} = -1, \text{ so } -1 \equiv \left(\frac{-1}{p}\right) \mod p.$$

Just as above, this shows that $\left(\frac{-1}{p}\right)$ must equal -1. ■

4.2.2 Part II

Before we move on to the proof of Part II, we first define the procedure we will be using. Starting with the even numbers $2, 4, 6, \ldots, p-1$, we multiply these together. Factoring out a 2 we get

$$2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1) = 2^P \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot P = 2^P \cdot P!.$$

Now we take the list $2, 4, 6, \ldots, p-1$ and reduce them modulo p so that each number lies between $-P$ and P, that is, within the interval $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$.

At some point in the list, namely $\frac{p-1}{2}$, the values will become negative. Recall that definition 4.2 speaks to this exact process and gives us some helpful notation. Thus we have

$$2^P \cdot P! \equiv (-1)^{\mu(2,p)} \cdot P! \mod p.$$

We can cancel $P!$ from both sides because $\gcd(P!, p) = 1$. Then we have our fundamental formula

$$2^P \equiv (-1)^{\mu(2,p)} \mod p.$$

Now for the proof of the case concerning 2. Note that there are four separate cases for this part and that they will all follow the above outline. For this reason the reader is not obliged to read through the details of each case as one will suffice to show the methodology. The process outline from above, along with the cases for $p \equiv 3$ and $p \equiv 7 \mod 8$, are from chapter 21 of [7]. The proofs of the other two cases are original, but follow the same outline.

Proof: PART II. Let $p \equiv 7 \mod 8$, say $p = 8k + 7$. So the even numbers $2, 4, 6, \ldots, p-1$ are the numbers from 2 to $8k + 6$. The midpoint is $P = 4k + 3$ so the cutoff for when the numbers will be negative by our process is between $(4k + 2)$ and $(4k + 4)$. Thus there are $2k + 2$ numbers to the right of the cutoff because

$$\frac{8k + 6 - (4k + 4) + 2}{2} = \frac{4k + 4}{2} = 2k + 2. \text{ So } \mu(2, p) = 2k + 2. \text{ Thus,}$$

$2^P \equiv (-1)^{\mu(2,p)} \equiv (-1)^{2k+2} \equiv 1 \mod p$. Then by theorem 3.5, we have that 2 is a quadratic residue mod p.

Now let $p \equiv 3 \mod 8$, say $p = 8k + 3$. The midpoint is $P = 4k + 1$. So the cutoff here is between $(4k)$ and $(4k + 2)$. There are $2k + 1$ numbers to the right of the cutoff because $\frac{8k + 2 - (4k + 2) + 2}{2} = 2k + 1$. And thus $\mu(2, p) = 2k + 1$. Therefore, $2^P \equiv (-1)^{\mu(2,p)} \equiv (-1)^{2k+1} \equiv -1 \mod p$. Then by theorem 3.5, we have that 2 is a quadratic nonresidue mod p.

Now let $p \equiv 5 \mod 8$, say $p = 8k + 5$. Then just as before we find that in this case $\mu(2, p) = 2k + 1$. Thus $2^P \equiv (-1)^{\mu(2,p)} \equiv (-1)^{2k+1} \equiv -1 \mod p$. Therefore by theorem 3.5, 2 is a quadratic nonresidue mod p.

Now let $p \equiv 1 \mod 8$, say $p = 8k + 1$. Then as before we find that in this case $\mu(2, p) = 2k$. Thus $2^P \equiv (-1)^{\mu(2,p)} \equiv (-1)^{2k} \equiv 1 \mod p$. Therefore by theorem 3.5, 2 is a quadratic residue mod p. ■

4.2.3 Part III

Now for the third, and arguably most important, part. This part is the crux of the theorem, allowing us to state for all other values of q exactly what its Legendre symbol will be mod p. Note that we will be proving that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu(p,q)+\mu(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

but this is equivalent to the original statement of the problem. The proof for this part is from chapter 23 of [7]

Proof: PART III. Let $Q = \dfrac{q-1}{2}$ and $T(q,p)$ be the triangle in the xy-plane whose vertices are the points $\Big(0,0\Big)$, $\Big(\frac{p}{2},0\Big)$ and $\Big(\frac{p}{2},\frac{q}{2}\Big)$ (Figure 4.1).

We will count the integer points in $T(q,p)$ with $x=1$ then $x=2$, and so on. Notice that the hypotenuse of the triangle lies on the line $y=\dfrac{q}{p}x$. Then for $x=1$ we have $\left\lfloor \dfrac{q}{p} \right\rfloor$ points, for $x=2$ we get $\left\lfloor \dfrac{2q}{p} \right\rfloor$ points and so on. Thus,

$$\text{N} = (\text{The number of points with integer coordinates in } T(q,p)) = \sum_{k=1}^{P} \left\lfloor \frac{kq}{p} \right\rfloor.$$

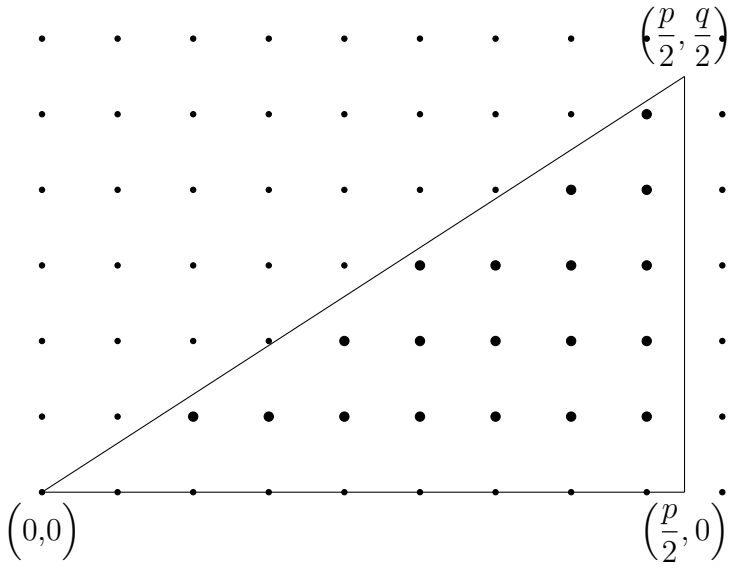

Figure 4.1: Integer Points in T(q,p)

Next let $T'(p,q)$ be the triangle with vertices $\Big(0,0\Big)$, $\Big(0,\frac{q}{2}\Big)$, and $\Big(\frac{p}{2},\frac{q}{2}\Big)$ (Figure 4.2). We count these integer points horizontally. By the same process as above we find

$$\text{M} = (\text{The number of points with integer coordinates in } T'(p,q)) = \sum_{k=1}^{Q} \left\lfloor \frac{kp}{q} \right\rfloor$$

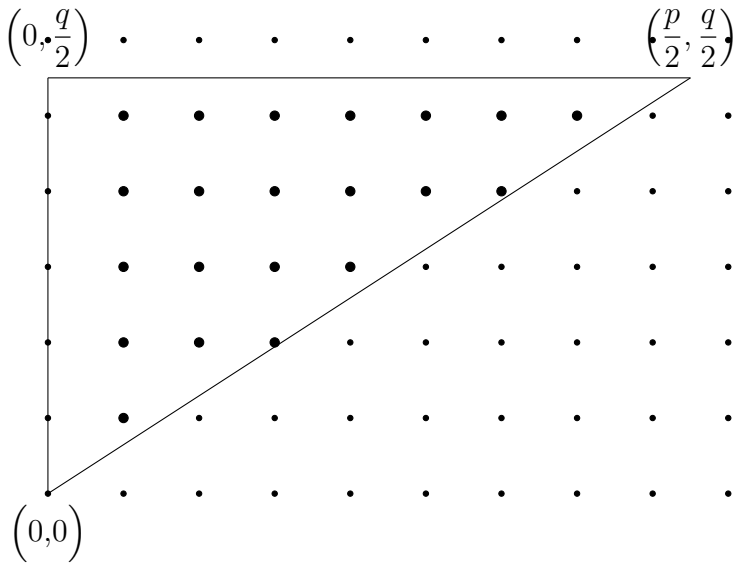

Figure 4.2: Integer Points in $T'(p,q)$

This along with lemma 4.2 gives us

$$N + M = \sum_{k=1}^{Q} \left\lfloor \frac{kp}{q} \right\rfloor + \sum_{k=1}^{P} \left\lfloor \frac{kq}{p} \right\rfloor = \mu(p,q) + \mu(q,p) \mod 2. \tag{4.2.1}$$

Consider the rectangle formed by putting these two triangles together (Figure 4.3). It has vertices $\left(0,0\right)$, $\left(0,\frac{q}{2}\right)$, $\left(\frac{p}{2},0\right)$, and $\left(\frac{p}{2},\frac{q}{2}\right)$.

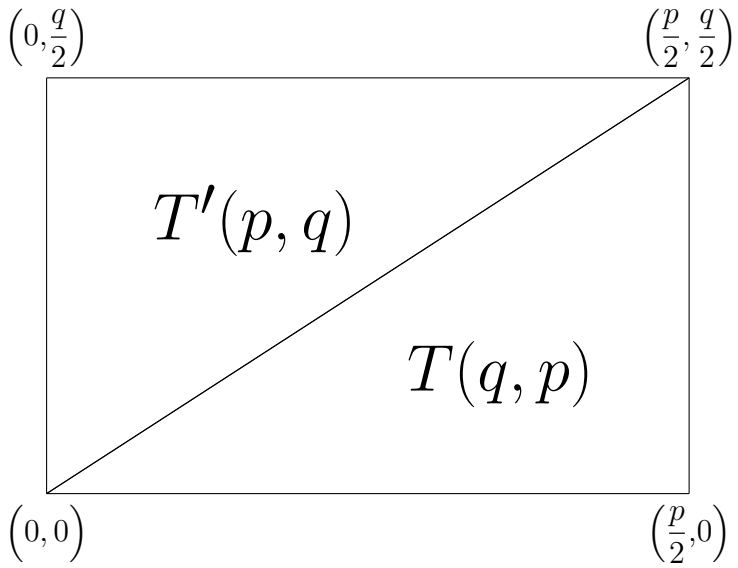

Figure 4.3: The Rectangle Formed From $T(q,p)$ and $T'(p,q)$

This rectangle contains $\left\lfloor \frac{p}{2} \right\rfloor$ columns of integer points and $\left\lfloor \frac{q}{2} \right\rfloor$ integer points in each column. Let $\mathbb{X}$ be the number of integer points in the rectangle. Then,

$$N + M = \mathbb{X} = \left\lfloor \frac{p}{2} \right\rfloor \cdot \left\lfloor \frac{q}{2} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{4.2.2}$$

Combining equations (4.2.1) and (4.2.2) we get

$$\mu(q,p) + \mu(p,q) \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \mod 2.$$

Hence by theorem 4.1,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu(p,q)} \cdot (-1)^{\mu(q,p)} = (-1)^{\mu(p,q)+\mu(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad \blacksquare$$

5 Lucas-Lehmer Test

Now that we have proven the Law of Quadratic Reciprocity, we have the major tools we need to prove the Lucas-Lehmer test. The Lucas-Lehmer test is a test for the primality of a Mersenne number. When this was proven in 1856 (and subsequently improved upon in 1877

and the 1930s) it was a groundbreaking find in the field of number theory. Because of this test, we can now know if a Mersenne number is prime much easier than ever before. For this reason, all of the largest prime numbers known are also Mersenne primes. Before we are quite ready to prove this big theorem we still have just a couple more helper theorems that we will employ in our proof of the test later.

5.1 Related Theorems

The Binomial mod p theorem, while not expressly related to Mersenne primes, is a theorem that we will employ in the proof of the Lucas Lehmer test. For this reason, we include it here. Sometimes this proof can seem a bit deceptive. If you are having a hard time believing this proof, write out a few small examples and it should become readily apparent.

Theorem 5.1 (Binomial mod p Theorem)**.** *Let p be a prime number and x, y be any integers. Then $(x+y)^p = x^p + y^p \mod p$.*

Proof. $(x+y)^p = \binom{p}{0}x^p y^0 + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}x^0 y^p.$

Notice that,

$$\binom{p}{0} = \binom{p}{p} = 1 \text{ and } \binom{p}{1} = \binom{p}{p-1} = p.$$

Also, p divides $\binom{p}{k}$ where $0 < k < p$. Then when we take the first equation modulo p we get

$$(x+y)^p \equiv x^p + y^p \mod p. \qquad \blacksquare$$

This next theorem is a general characterization of what Mersenne numbers look like. While the theorem has been known for a long time, this version of the proof is original.

Theorem 5.2. *For any Mersenne number $M_n \equiv 7 \mod 12$ for odd $n > 1$.*

Proof. First, note that $2^n \equiv 4$ or $8 \mod 12$. Now we claim that when n is odd, according to our assumption, then it is $\equiv 8 \mod 12$, $\forall\, k \geq 1$. Let $n = 2k+1$. We will show that $2^{2k+1} \equiv 8 \mod 12$. We proceed by induction.

Let $k = 1$. Then

$$2^{2k+1} \equiv 2^{2\cdot 1+1} \equiv 2^3 \equiv 8 \mod 12.$$

Now assume this holds for k, we will prove it holds for $k+1$.

$$2^{2(k+1)+1} \equiv 2^{2k+2+1} \equiv 2^{2k+3} \equiv 2^{2k+1} \cdot 2^2 \equiv 8 \cdot 4 \equiv 8 \mod 12.$$

Therefore $2^n \equiv 8 \mod 12 \implies 2^n - 1 \equiv 7 \mod 12$ ■

This corollary can be very clearly seen from the above theorem, but we will prove it here for extra clarity. As you will see in theorem 5.3 this corollary is actually what we will employ.

Corollary 5.1. *All Mersenne numbers $M_n \equiv 3 \mod 4$ for odd $n > 1$.*

Proof. Let M_n be a Mersenne number with $n > 1$ and odd. Then by the above, $M_n \equiv 7 \mod 12$ and by definition, $M_n = 12k + 7$ for some $k \in \mathbb{N}$. Taking both sides modulo 4 gives $M_n \equiv 3 \mod 4$. ■

5.2 Proof of the Lucas-Lehmer Test

We are now finally ready to begin our discussion of the Lucas-Lehmer test. We start by defining a recursive relation. This relation is actually what will allow us to determine the primality of a given Mersenne number.

Definition 5.1 (Lucas-Lehmer Recursive Relation)**.**

$$s_i = \begin{cases} 4 & \text{if } i = 0 \\ s_{i-1}^2 - 2 & \text{otherwise} \end{cases}$$

Next we must prove a short lemma about the recurrence relation itself as well as define some notation for ease and clarity throughout the proof of the theorem. J. W. Bruce outlines the proof of the following lemma in [1].

Lemma 5.1. *let* $\omega = 2 + \sqrt{3}$ *and* $\overline{\omega} = 2 - \sqrt{3}$*, then* $s_i = \omega^{2^i} + \overline{\omega}^{2^i}\ \forall\ i$

Proof. First notice that $\langle s_i \rangle$ is a recurrence relation with a closed form solution. We proceed by induction. If $i = 0$ we have,

$$s_0 = \omega^{2^0} + \overline{\omega}^{2^0} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4.$$

Now assume this holds true for $n - 1$, we will prove it is true for n.
First notice that $(\omega\overline{\omega}) = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$.

$$\begin{aligned} s_n &= s_{n-1}^2 - 2 \\ &= (\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}})^2 - 2 \\ &= \omega^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} + \overline{\omega}^{2^n} - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} + 2 - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} \text{ thus,} \\ s_i &= \omega^{2^n} + \overline{\omega}^{2^n}\ \forall\ i. \end{aligned}$$

■

Now that we have all our notation defined and this lemma under our belt we can finally prove the Lucas Lehmer test. Since the statement of this theorem is quite simple, it may be difficult to see its importance. This test gives us a precise way to test if a Mersenne number is prime by looking at only one number, namely s_{p-2}. Even though by lemma 5.1 we know the closed form solution to the relation, it still takes a lot of time to test large numbers because of the extremely large exponential calculations involved.

Theorem 5.3 (Lucas-Lehmer Test)**.** M_p *is prime* $\iff s_{p-2} \equiv 0 \mod M_p,\ \ p > 2.$

Proof. ($\Longleftarrow$) Suppose $s_{p-2} \equiv 0 \mod M_p$. Then $\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} \equiv 0 \mod M_p$ by lemma 5.1. Therefore,

$$\begin{aligned}
\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} &= kM_p && \text{for some integer } k. \text{ Thus,} \\
\omega^{2^{p-2}} &= kM_p - \overline{\omega}^{2^{p-2}} \\
(\omega^{2^{p-2}})^2 &= \omega^{2^{p-2}}(kM_p - \overline{\omega}^{2^{p-2}}) \\
(\omega^{2^{p-2}})^2 &= kM_p\omega^{2^{p-2}} - (\omega\overline{\omega})^{2^{p-2}} \\
\omega^{2^{p-1}} &= kM_p\omega^{2^{p-2}} - 1 && \text{by lemma 5.1} \qquad (5.3.1)
\end{aligned}$$

By way of contradiction, suppose M_p is composite and let q be the smallest prime factor of M_p. Since Mersenne numbers are odd we have $q > 2$. Define the set $\mathbb{X} = \left\{a + b\sqrt{3} | a, b \in \mathbb{Z}_q\right\}$ with q^2 elements, where $\mathbb{Z}_q$ is the integers mod q. Define the multiplication operation in $\mathbb{X}$ as

$$(a + b\sqrt{3})(c + d\sqrt{3}) = \left[(ac + 3bd) \mod q\right] + \left[(bc + ad) \mod q\right]\sqrt{3}.$$

Since $q > 2$, ω and $\overline{\omega}$ are in $\mathbb{X}$. Any product of two numbers in $\mathbb{X}$ will be in $\mathbb{X}$. However it is not a group under multiplication because not every $x \in \mathbb{X}$ has an inverse $x^{-1} \in \mathbb{X}$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$. If we consider only the elements that have inverses, we get a group $\mathbb{X}^*$ of at most $q^2 - 1$ elements, because 0 has no inverse.

Since $M_p \equiv 0 \mod q$ and $\omega \in \mathbb{X}$, we have that $kM_p\omega^{2^{p-2}} = 0$ in $\mathbb{X}$ for some integer k. Then by equation (5.3.1) we have $\omega^{2^{p-1}} = -1$.

Squaring both sides gives $\omega^{2^p} = 1$, showing that ω is invertible with inverse $\omega^{2^{p-1}}$, because $\omega * \omega^{2^{p-1}} = \omega 2^p = 1$. Thus $\omega \in \mathbb{X}^*$ and has order dividing 2^p. Actually the order must be equal to 2^p because $\omega^{2p-1} \neq 1$ by above. Then the order does not divide 2^{p-1}. Since the order of an element is at most the order of the group, we conclude that

$$2^p \leq q^2 - 1 < q^2.$$

But since q is the smallest prime factor of the composite M_p, we must have

$$q^2 \leq M_p = 2^p - 1.$$

Therefore, $2^p < 2^p - 1$, a contradiction. Hence, M_p is prime.

Suppose M_p is prime, we will show $s_{p-2} \equiv 0 \mod M_p$. Notice that 3 is a quadratic non-residue mod M_p, since by corollary 5.1, $2^p - 1$ for odd $p > 1$ only is congruent to 3 mod 4. Then by legendre symbol properties, $\left(\frac{3}{M_p}\right) = -1$. Theorem 3.5 gives us $3^{(M_p-1)/2} \equiv -1 \mod M_p$. Also notice that 2 is a quadratic residue mod M_p, since $2^p \equiv 1 \mod M_p$ and thus

$$2 \equiv 2^{p+1} \equiv (2^{(p+1)/2})^2 \mod M_p.$$

Theorem 3.5 gives us $2^{(M_p-1)/2} \equiv 1 \mod M_p$.

Define $\sigma = 2\sqrt{3}$ and $\mathbb{X}^*$ as we did before as the multiplicative group of $\left\{a + b\sqrt{3} | a, b, \in \mathbb{Z}_{M_p}\right\}$. Then in the group $\mathbb{X}^*$ we have

$$\begin{aligned}
(6+\sigma)^{M_p} &= 6^{M_p} + 2^{M_p}(\sqrt{3}^{M_p}) && \text{by theorem 5.1} \\
&= 6 + 2(\sqrt{3}^{M_p}) && \text{by theorem 3.2} \\
&= 6 + 2(3^{(M_p-1)/2})\sqrt{3} \\
&= 6 + 2(-1)\sqrt{3} \\
&= 6 - \sigma.
\end{aligned}$$

We chose this σ such that $\omega = (6+\sigma)^2/24$. Notice that

$$24^{(M_p-1)/2} = (2^{(M_p-1)/2})^3(3^{(M_p-1)/2}) = (1)^3(-1) = -1.$$

Therefore, we can use this to help compute $\omega^{(M_p+1)/2}$ in $\mathbb{X}^*$

$$\begin{aligned}
\omega^{(M_p+1)/2} &= \left[(6+\sigma)^{(M_p+1)/2}\right]^2 / 24^{(M_p+1)/2} \\
&= (6+\sigma)^{(M_p+1)} / 24^{(M_p+1)/2} \\
&= (6+\sigma)^{M_p}(6+\sigma)/(24 \cdot 24^{(M_p-1)/2}) \\
&= (6-\sigma)(6+\sigma)/(-24) \\
&= 24/(-24) \\
&= -1
\end{aligned}$$

Thus, $\omega^{(M_p+1)/2} \equiv -1$ in $\mathbb{X}^*$.

Since $M_p \equiv 3 \bmod 4$ by corollary 5.1, we multiply both sides of the above equation by $\omega^{(M_p+1)/4}$ and use the fact that $\omega\overline{\omega} = 1$. Thus,

$$\begin{aligned}
\omega^{(M_p+1)/2}\overline{\omega}^{(M_p+1)/4} &= -\overline{\omega}^{(M_p+1)/4} \\
\omega^{(M_p+1)/4} &= -\overline{\omega}^{(M_p+1)/4} \\
\omega^{(M_p+1)/4} + \overline{\omega}^{(M_p+1)/4} &= 0 \\
\omega^{(2^p-1+1)/4} + \overline{\omega}^{(M_p+1)/4} &= 0 \\
\omega^{(2^p/4)} + \overline{\omega}^{(2^p/4)} &= 0 \\
\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} &= 0 \\
s_{p-2} &= 0 \qquad \text{by lemma 5.1.}
\end{aligned}$$

Since s_{p-2} is an integer and is 0 in $\mathbb{X}^*$, it is 0 mod M_p. ■

We now take a moment to review what has been shown up to this point and why it is significant. We have just proved a test that will allow us to see if a Mersenne number is prime with relative ease compared to the primality tests we had before. This is one of the reasons why the number of Mersenne primes as well as the value of the largest prime has increased

greatly in the past 100 years. Of course the ever looming question about the infinitude of the Mersenne primes continues to lay unanswered, but the search has only been helped by this monumental test.

6 Perfect Numbers

We now turn our attention to another set of numbers that could potentially help in our search for the answer about the infinitude of the Mersenne primes, the perfect numbers.

Definition 6.1 (Perfect Number)**.** A number n is called a *perfect number* if the sum of its proper divisors is equal to itself.

The first few even perfect numbers are 6, 28, 492, 8128, 33550336, and 8589869056. Upon first glance it may seem that there is no structural pattern to these numbers, however this is certainly not the case. The set of perfect numbers is actually very closely linked to the set of Mersenne prime numbers. In fact, for every Mersenne prime we have, we have a formula that will give us a perfect number "for free". See Table 8.1 for a full list of the Mersenne primes and their related perfect numbers. Before we start looking at the relationship between these two kinds of special numbers we must first discuss a special function that we will use in the following proofs.

6.1 Sigma Function

Definition 6.2. $\sigma(n)$ is the sum of all divisors of n (including 1 and n).

This function holds some special properties that we will now prove that are essential for its various uses. Silverman states the theorem and sets up the idea behind part (b) as well as the proof of part (a) in chapter 15 of [7], however the proof of part (b) is original.

Theorem 6.1. *(Sigma Function Formulas)* ***(a)*** *If p is prime and $k \geq 1$, then*

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

(b) *If* $\gcd(m,n) = 1$*, then*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Proof. **(a)** Notice that $\sigma(p) = p + 1$ because the only divisors of a prime number are itself and 1. We can easily see that in general the only divisors of a prime power are the powers of that prime below itself. Namely the numbers,

$$1 + p + p^2 + \cdots + p^k.$$

Thus it is clear that

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

by the geometric partial sum formula.

(b) Let $m, n \in \mathbb{N}$ and $\gcd(m,n) = 1$. Suppose $x_1, x_2, \ldots, x_r$ are all the divisors of m and $y_1, y_2, \ldots, y_s$ are all the divisors of n. Let $j|mn$. If $j|m$, then $j = x_i$ for some i. If $j|n$ then $j = y_k$ for some k. Suppose that $\gcd(j,m) = d$ but j does not divide m. Notice that $d = x_i$ for some i as it is a divisor of m. We have $j = da$ with $a \in \mathbb{N}$ and $m = db$ with $b \in \mathbb{N}$. Note that $\gcd(a,b) = 1$ because if it was anything else then the $\gcd(j,m) \neq d$. Thus a and b are coprime. So if we substitute into $j|mn$ we have that $da|dbn \implies a|bn$ and thus $a|n$. Note that this means that $a = y_k$ for some k as it is a divisor of n. Hence we have $j = da = x_i y_k$ for any divisor j of mn. Furthermore, since m and n are coprime we know that each of the products of divisors is unique. Thus, the divisors of mn are

$$x_1y_1, x_1y_2, \ldots, x_1y_s, x_2y_1, x_2y_2, \ldots x_2y_s, \ldots, x_ry_1, x_ry_2, \ldots, x_ry_s.$$

So,

$$\begin{aligned}
\sigma(mn) &= x_1y_1 + x_1y_2 + \cdots + x_1y_s + \cdots + x_ry_1 + x_ry_2 + \cdots + x_ry_s \\
&= x_1(y_1 + y_2 + \cdots + y_s) + x_2(y_1 + y_2 + \cdots + y_s)\cdots + x_r(y_1 + y_2 + \ldots y_s) \\
&= (x_1 + x_2 + \cdots + x_r)(y_1 + y_2 + \cdots + y_s) \\
&= \sigma(m)\sigma(n).
\end{aligned}$$

■

Now that we have these operations regarding the σ function we can look at the relationship between the Mersenne primes and the even perfect numbers.

6.2 Proof of the Relationship

This theorem gives us a rigorous way of looking at the structure of an even perfect number and how the underlying Mersenne prime plays its role. Silverman proves this in chapter 15 of [7], however it was originally proved by Euler in the 18^{th} century.

Theorem 6.2. *If n is an even perfect number, then n is of the form*

$$n = 2^{p-1}(2^p - 1)$$

where $2^p - 1$ is a Mersenne prime.

Proof. Suppose that n is an even perfect number. Since n is even we know we can factor it as $n = 2^k m$ with $k \geq 1$ and m odd.
Next we will use the sigma formulas to compute $\sigma(n)$.

$$\begin{aligned}
\sigma(n) &= \sigma(2^k m) && \text{since } n = 2^k m \\
&= \sigma(2^k)\sigma(m) && \text{using our multiplication property and that } \gcd(2^k, m) = 1 \\
&= (2^{k+1} - 1)\sigma(m) && \text{using the formula for } \sigma(p^k) \text{ with } p = 2
\end{aligned}$$

But n is supposed to be perfect, which means that $\sigma(n) = 2n = 2^{k+1}m$. So we have two different expressions for $\sigma(n)$ and they must be equal,

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m).$$

The number $2^{k+1} - 1$ is clearly odd, and $(2^{k+1} - 1)\sigma(m)$ is a multiple of 2^{k+1}, so 2^{k+1} must divide $\sigma(m)$. Thus we know there exists some number c such that $\sigma(m) = 2^{k+1}c$. We can substitute this into the above equation to get

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m) = (2^{k+1} - 1)2^{k+1}c,$$

and then canceling 2^{k+1} from both sides gives us $m = (2^{k+1} - 1)c$. So we know that there exits an integer c such that

$$m = (2^{k+1} - 1) \text{ and } \sigma(m) = 2^{k+1}c.$$

We are going to show that this integer c must be equal to 1 by assuming that $c > 1$. Suppose that $c > 1$. Then $m = (2^{k+1} - 1)c$ would be divisible by the distinct numbers 1, c, and m. Of course it is possible that m itself is divisible by many other number. In any case we see that,

$$\sigma(m) \geq 1 + c + m = 1 + c + (2^{k+1} - 1)c = 1 + 2^{k+1}c.$$

However, we also know that $\sigma(m) = 2^{k+1}c$, so

$$2^{k+1}c \geq 1 + 2^{k+1}c.$$

Hence $0 \geq 1$, a contradiction. Thus our assumption was wrong and $c = 1$. Thus,

$$m = (2^{k+1} - 1) \text{ and } \sigma(m) = 2^{k+1} = m + 1.$$

From this we see that m must be prime, because $\sigma(m) = m + 1$ exactly when m is prime. Thus we have proved that if n is an even perfect number then

$$n = 2^k(2^{k+1} - 1) \qquad \text{with } 2^{k+1} - 1 \text{ a prime number.}$$

But we know that if $2^{k+1} - 1$ is prime then $k + 1$ is prime, so let $k + 1 = p$. Then every even perfect number is of the form $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ a Mersenne prime. ■

The next theorem allows us to go the other way, giving us a formula for finding even perfect numbers given a Mersenne prime. This, coupled with the above, is a very powerful result that shows clearly just how closely related the Mersenne primes and the perfect numbers are. Like the above theorem, Silverman proves this one in chapter 15 of [7], however it was also originally proved by Euler in the 18^{th} century.

Theorem 6.3. *If $2^p - 1$ is a prime number, then $2^{p-1}(2^p - 1)$ is a perfect number.*

Proof. For ease of notation, let $q = 2^p - 1$. Then we need to verify that $2^{p-1}q$ is a perfect number. Notice that the proper divisors of $2^{p-1}q$ can be split into two groups:

$$1, 2, 4, \ldots, 2^{p-1} \text{ and } q, 2q, 4q, \ldots, 2^{p-2}q.$$

We can add these numbers together using the formula for a Geometric Series. If we rearrange the formula slightly we have,

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}.$$

Then substitute $x = 2$ and $n = p$ in the above formula we get,

$$1 + 2 + 4 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1 = q. \tag{6.3.1}$$

Also, we can use the formula to compute

$$\begin{aligned} q + 2q + 4q + \cdots + 2^{p-2}q &= q(1 + 2 + 4 + \cdots + 2^{p-2}) \\ &= q\left(\frac{2^{p-1} - 1}{2 - 1}\right) \\ q + 2q + 4q + \cdots + 2^{p-2}q &= q(2^{p-1} - 1). \end{aligned} \tag{6.3.2}$$

Then, combining equations 6.3.1 and 6.3.2 we get

$$\begin{aligned} 1 + 2 + 4 + \cdots + 2^{p-1} + q + 2q + 4q + \cdots + 2^{p-2}q &= q + q(2^{p-1} - 1) \\ &= q + q2^{p-1} - q \\ &= q2^{p-1}. \end{aligned}$$

Hence, $2^{p-1}q$ is a perfect number. ■

Now that we have these two theorems under our belt, we have a solid and clearly characterized relationship between the Mersenne primes and the even perfect numbers. Because of the Lucas-Lehmer test (theorem 5.3) it is much easier at this time to find Mersenne primes

than it is for use to find even perfect numbers. Since these theorems tell us exactly how to get an even perfect number given a Mersenne prime and vice versa. If it were determined that there was an infinite amount of either kind of number we would automatically also know that there was an infinite amount of the other as well.

7 Open Problems and Further Research

While we know quite a bit about the prime numbers, Mersenne primes, and perfect numbers, there are still many open problems in this field. One of the most well known open problems in number theory is the Riemann Hypothesis (which is unfortunately much too complicated to even state here). This conjecture has been around for over a hundred years and relates to many other fields of mathematics as well. In the fall of 2018, Michael Atiyah claimed to have proven this 160 year old hypothesis. However, the proof that he gave was quickly picked apart and is not accepted by the mathematical community as a whole.

Mathematicians have also been trying for years to find a nice pattern to the primes or to characterize the distribution of the primes. Along with this comes the question of if there are an infinite number of Mersenne primes as well as we have discussed throughout this paper. So far there has been significant work done on both of these problems, however with no proofs resultant as of yet. Another major open problem is the Twin primes conjecture, which hypothesises that there are an infinite number of pairs of primes that differ by two. Such pairs of primes are called twin primes. Interestingly, it is thought that progress on this conjecture may also help with the Riemann Hypothesis [4]. We also still do not know if there are any odd perfect numbers. Mathematicians have attempted to find an odd perfect number for over 2000 years with no luck thus far.

Thus it is clear that while we know a good deal about prime numbers and the Mersenne primes, there is a lot to still investigate. The prime numbers have baffled mathematicians for several hundred years and this will likely be the case for hundreds more. They have always

attracted a great amount of research, perhaps now more than ever before. However some questions still remain unsolved. The mystery of the Mersenne primes, ever so elusive, will likely continue on for many years to come.

8 Appendix

Table 8.1 (following page) gives a complete list of the known Mersenne primes at the time of publishing, along with their associated perfect numbers, the date they were discovered, and who discovered them (information from [5]). The * denotes that it has not been verified that this is the "next" Mersenne prime.

8.1 Definitions

Definition 1.1 (Mersenne Number)**.** A number M_n is called a *Mersenne number* if it is of the form $M_n = 2^n - 1$ where $n \in \mathbb{N}$

Definition 1.2 (Mersenne Prime)**.** A prime number M_p is called a *Mersenne prime* if it can be written in the form $M_p = 2^p - 1$ with prime $p \in \mathbb{N},$ and $p \geq 2$

Definition 2.1 (Prime Number)**.** A *prime number* is a natural number $p > 1$ that is divisible only by itself and 1.

Definition 3.1 (Quadratic Residue (QR))**.** A nonzero number that is congruent to a square modulo p is said to be a *quadratic residue* modulo p.

Definition 3.2 (Quadratic Nonresidue (NR))**.** A nonzero number that is not congruent to a square modulo p is said to be a *quadratic nonresidue* modulo p.

Definition 3.3. The *Legendre symbol* of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod p} \\ -1 & \text{if } a \text{ is a nonresidue mod p} \end{cases}$$

Definition 4.1. The *floor function*, denoted $\lfloor t \rfloor$, is the largest integer n such that $n \leq t$.

Definition 4.2. $\mu(a, p)$ is the number of integers in the list $a, 2a, \ldots, Pa$ that become negative when they are reduced modulo p into the interval from $-P$ to P.

Definition 5.1 (Lucas-Lehmer Recursive Relation)**.**

$$s_i = \begin{cases} 4 & \text{if } i = 0 \\ s_{i-1}^2 - 2 & \text{otherwise} \end{cases}$$

Definition 6.1 (Perfect Number)**.** A number n is called a *perfect number* if the sum of its proper divisors is equal to itself.

Definition 6.2. $\sigma(n)$ is the sum of all divisors of n (including 1 and n).

References

[1] J. W. Bruce. A really trivial proof of the lucas-lehmer test. `https://fermatslibrary.com/s/a-really-trivial-proof-of-the-lucas-lehmer-test`.

[2] Chris K. Caldwell. Mersenne primes: History, theorems and lists, 2018. `https://primes.utm.edu/mersenne/index.html#hist`.

[3] Gerald Tenenbaum et al. *The Prime Numbers and Their Distribution.* American Mathematical Society, 2001.

[4] William L. Hosch. Twin prime conjecture, 2017. `https://www.britannica.com/science/twin-prime-conjecture`.

[5] Mersenne Research Inc. List of known mersenne primes, 2019. `https://www.mersenne.org/primes/`.

[6] Oystein Ore. *Number Theory and Its History.* Dover, 1988.

[7] Joseph H. Silverman. *A Friendly Introduction to Number Theory.* Pearson, fourth edition, 2012.

	$2^p - 1$	Date	Discovered By	Perfect Number
1	$2^2 - 1$	c. 500 BC	Ancient Greek mathematicians	$2^1(2^2 - 1)$
2	$2^3 - 1$	c. 500 BC	Ancient Greek mathematicians	$2^2(2^3 - 1)$
3	$2^5 - 1$	c. 275 BC	Ancient Greek mathematicians	$2^4(2^5 - 1)$
4	$2^7 - 1$	c. 275 BC	Ancient Greek mathematicians	$2^6(2^7 - 1)$
5	$2^{13} - 1$	1456	Anonymous	$2^{12}(2^{13} - 1)$
6	$2^{17} - 1$	1588	Pietro Cataldi	$2^{16}(2^{17} - 1)$
7	$2^{19} - 1$	1588	Pietro Cataldi	$2^{18}(2^{19} - 1)$
8	$2^{31} - 1$	1772	Leonhard Euler	$2^{30}(2^{31} - 1)$
9	$2^{61} - 1$	1883	Ivan Mikheevich Pervushin	$2^{60}(2^{61} - 1)$
10	$2^{89} - 1$	1911 Jun	R. E. Powers	$2^{88}(2^{89} - 1)$
11	$2^{107} - 1$	1914 Jun 11	R. E. Powers	$2^{106}(2^{107} - 1)$
12	$2^{127} - 1$	1876 Jan 10	Edouard Lucas	$2^{126}(2^{127} - 1)$
13	$2^{521} - 1$	1952 Jan 30	Raphael M. Robinson	$2^{520}(2^{521} - 1)$
14	$2^{607} - 1$	1952 Jan 30	Raphael M. Robinson	$2^{606}(2^{607} - 1)$
15	$2^{1,279} - 1$	1952 Jun 25	Raphael M. Robinson	$2^{1,278}(2^{1,279} - 1)$
16	$2^{2,203} - 1$	1952 Oct 07	Raphael M. Robinson	$2^{2,202}(2^{2,203} - 1)$
17	$2^{2,281} - 1$	1952 Oct 09	Raphael M. Robinson	$2^{2,280}(2^{2,281} - 1)$
18	$2^{3,217} - 1$	1957 Sep 08	Hans Riesel	$2^{3,216}(2^{3,217} - 1)$
19	$2^{4,253} - 1$	1961 Nov 03	Alexander Hurwitz	$2^{4,252}(2^{4,253} - 1)$
20	$2^{4,423} - 1$	1961 Nov 03	Alexander Hurwitz	$2^{4,422}(2^{4,423} - 1)$
21	$2^{9,689} - 1$	1963 May 11	Donald B. Gillies	$2^{9,688}(2^{9,689} - 1)$
22	$2^{9,941} - 1$	1963 May 16	Donald B. Gillies	$2^{9,940}(2^{9,941} - 1)$
23	$2^{11,213} - 1$	1963 Jun 02	Donald B. Gillies	$2^{11,212}(2^{11,213} - 1)$
24	$2^{19,937} - 1$	1971 Mar 04	Bryant Tuckerman	$2^{19,936}(2^{19,937} - 1)$
25	$2^{21,701} - 1$	1978 Oct 30	Landon Curt Noll & Laura Nickel	$2^{21,700}(2^{21,701} - 1)$
26	$2^{23,209} - 1$	1979 Feb 09	Landon Curt Noll	$2^{23,208}(2^{23,209} - 1)$
27	$2^{44,497} - 1$	1979 Apr 08	Harry Lewis Nelson & David Slowinski	$2^{44,496}(2^{44,497} - 1)$
28	$2^{86,243} - 1$	1982 Sep 25	David Slowinski	$2^{86,242}(2^{86,243} - 1)$
29	$2^{110,503} - 1$	1988 Jan 28	Walter Colquitt & Luke Welsh	$2^{110,502}(2^{110,503} - 1)$
30	$2^{132,049} - 1$	1983 Sep 19	David Slowinski	$2^{132,048}(2^{132,049} - 1)$
31	$2^{216,091} - 1$	1985 Sep 01	David Slowinski	$2^{216,090}(2^{216,091} - 1)$
32	$2^{756,839} - 1$	1992 Feb 19	David Slowinski & Paul Gage	$2^{756,838}(2^{756,839} - 1)$
33	$2^{859,433} - 1$	1994 Jan 04	David Slowinski & Paul Gage	$2^{859,432}(2^{859,433} - 1)$
34	$2^{1,257,787} - 1$	1996 Sep 03	David Slowinski & Paul Gage	$2^{1,257,786}(2^{1,257,787} - 1)$
35	$2^{1,398,269} - 1$	1996 Nov 13	Joel Armengaud	$2^{1,398,268}(2^{1,398,269} - 1)$
36	$2^{2,976,221} - 1$	1997 Aug 24	Gordon Spence	$2^{2,976,220}(2^{2,976,221} - 1)$
37	$2^{3,021,377} - 1$	1998 Jan 27	Roland Clarkson	$2^{3,021,376}(2^{3,021,377} - 1)$
38	$2^{6,972,593} - 1$	1999 Jun 01	Nayan Hajratwala	$2^{6,972,592}(2^{6,972,593} - 1)$
39	$2^{13,466,917} - 1$	2001 Nov 14	Michael Cameron	$2^{13,466,916}(2^{13,466,917} - 1)$
40	$2^{20,996,011} - 1$	2003 Nov 17	Michael Shafer	$2^{20,996,010}(2^{20,996,011} - 1)$
41	$2^{24,036,583} - 1$	2004 May 15	Josh Findley	$2^{24,036,582}(2^{24,036,583} - 1)$
42	$2^{25,964,951} - 1$	2005 Feb 18	Martin Nowak	$2^{25,964,950}(2^{25,964,951} - 1)$
43	$2^{30,402,457} - 1$	2005 Dec 15	Curtis Cooper & Steven Boone	$2^{30,402,456}(2^{30,402,457} - 1)$
44	$2^{32,582,657} - 1$	2006 Sep 04	Curtis Cooper & Steven Boone	$2^{32,582,656}(2^{32,582,657} - 1)$
45	$2^{37,156,667} - 1$	2008 Sep 06	Hans-Michael Elvenich	$2^{37,156,666}(2^{37,156,667} - 1)$
46	$2^{42,643,801} - 1$	2009 Jun 04	Odd M. Strindmo	$2^{42,643,800}(2^{42,643,801} - 1)$
47	$2^{43,112,609} - 1$	2008 Aug 23	Edson Smith	$2^{43,112,608}(2^{43,112,609} - 1)$
48*	$2^{57,885,161} - 1$	2013 Jan 25	Curtis Cooper	$2^{57,885,160}(2^{57,885,161} - 1)$
49*	$2^{74,207,281} - 1$	2016 Jan 07	Curtis Cooper	$2^{74,207,280}(2^{74,207,281} - 1)$
50*	$2^{77,232,917} - 1$	2017 Dec 26	Jon Pace	$2^{77,232,916}(2^{77,232,917} - 1)$
51*	$2^{82,589,933} - 1$	2018 Dec 07	Patrick Laroche	$2^{82,589,932}(2^{82,589,933} - 1)$

Table 8.1: Mersenne Primes and Associated Perfect Numbers