SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Mersenne Primes and the Quest to Find Them

av

Leo G. Levenius

2024 - No K30

Mersenne Primes and the Quest to Find Them

Leo G. Levenius

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Per Alexandersson

2024

Abstract

The purpose of this thesis is to explore Mersenne primes. Mersenne primes are prime numbers of the form $2^n - 1$ where n itself is prime. We delve into some properties of Mersenne primes and discuss conjectures about their distribution. We also analyse their connection to other families of integers, such as Sophie Germain primes, Wieferich primes, and perfect numbers. Furthermore, we describe different methods for discovering Mersenne primes. The theory is illustrated with examples and simple `Python` code. Finally, we present the computer software programme GIMPS and how it is used to find Mersenne primes. With the help of GIMPS, we performed Lucas–Lehmer and Fermat primality tests on 200 previously unverified/uncertified potential candidates for Mersenne primes. All tests were, however, negative for new prime numbers.

Key Words: Mersenne prime, Lucas–Lehmer primality test, Fermat primality test, GIMPS.

Sammanfattning på svenska

Syftet med denna uppsats är att undersöka Mersenneprimtal. Mersenneprimtal är primtal på formen $2^n - 1$, där n själv är ett primtal. Vi fördjupar oss i några egenskaper hos Mersenneprimtal och diskuterar förmodanden om deras fördelning. Vi analyserar även deras koppling till andra heltalsfamiljer, såsom Sophie Germain-primtal, Wieferichprimtal och perfekta tal. Vidare beskriver vi olika metoder för att upptäcka Mersenneprimtal. Teorin illustreras med exempel och enkel `Python`-kod. Slutligen presenterar vi datorprogrammet GIMPS och hur det används för att hitta Mersenneprimtal. Med hjälp av GIMPS genomförde vi Lucas–Lehmer och Fermats primtester på 200 tidigare overifierade/ocertifierade potentiella kandidater för Mersenneprimtal. Alla tester var emellertid negativa för nya primtal.

Nyckelord: Mersenneprimtal, Lucas–Lehmers primtest, Fermats primtest, GIMPS.

Foreword

This thesis constitutes the degree project corresponding to 15 ECTS credits for a degree of Bachelor of Science (*filosofie kandidat*) in mathematics. It is written at the Department of Mathematics at Stockholm University.

Working on this thesis was originally supposed to be a side project of mine alongside my full-time actuarial studies. Something that I would work with now and then over the course of a year and finish towards the beginning of autumn 2025. But this turned out to be more fun than expected, and within two months, I was 99 per cent done.

After I was practically finished, something truly unexpected happened. Fellow GIMPS user Luke Durant discovered the 52nd known Mersenne prime on 12th October 2024. This is the first Mersenne prime found using Fermat's primality test (see Corollary 4.9) and the first new Mersenne prime discovered in close to six years. Because of this, I was forced to make several last-minute adjustments to the thesis in order to align it with this new amazing achievement. As can be seen in Table B.2, almost all my certifications were pertaining to the work of Mr Durant. However, i was unfortunately not directly involved with finding the prime number in question.

Wrapping up this foreword, I would like to thank my supervisor Dr Per Alexandersson who, after some hesitance, agreed to accompany me on this journey and who has always been in sync with my goals for this thesis as well as providing valuable feedback. I also want to express deep gratitude to my good friends Mr Luciano Egusquiza Castillo, who has shown an insanely humongous interest in this thesis, and Mr Jack Zhan, who has listened through all my ramblings, to whom I first proposed this idea during an August dinner and who have graciously acted as peer reviewers, not only spotting errors but giving ideas in their own special ways.

Stockholm, 20th November 2024

LGL

Contents

1 Introduction

Prime numbers have fascinated mathematicians for millennia, serving as the building blocks of number theory. As we observe larger numbers, the primes become more and more sparse. So, to find new primes, it is desirable to focus on certain types of primes with useful properties. One such subset is *Mersenne primes*, which can be expressed as $2^n - 1$ for some prime n. The purpose of this thesis is to explore what makes Mersenne primes so special and how one could go about finding new ones.

The starting point of the literature used in this thesis comes mainly from Ribenboim [27] and the works referenced there. The Wikipedia page on Mersenne primes [30] has been a great inspiration for topics, albeit the mathematical rigorousness there is often far from satisfactory. Several of the theorems and proofs presented in this thesis originating from other sources are reworded to be (hopefully) more understandable and concise.

But why is any of this interesting? The dry answer is that prime numbers have real-life applications, e.g. in cryptography, so it is always of interest to find new ones. Expanding empirical evidence is also important to discuss and formulate conjectures of the underlying theory. Further, it is in some way about man's quest to explore the unknown, push the boundaries using evolving technology, and find what those before us could only dream about.

1.1 Preliminary of Primes and Definition of Set Notation

Definition 1.1. Let $\mathbb{F} \subseteq \mathbb{R}$. The set of all elements in $\mathbb{F}$ greater than or equal to $x \in \mathbb{R}$ is denoted by

$$\mathbb{F}_{\geq x} \coloneqq \{\omega \in \mathbb{F} : \omega \geq x\}.$$

In particular, $\mathbb{N} \coloneqq \mathbb{Z}_{\geq 0}$.

Definition 1.2. Let $n \in \mathbb{Z}_{\geq 2}$. If the only divisors[1] of n are 1 and itself, then n is called a *prime* number. Otherwise, we say that n is a *composite* number.

Definition 1.3. We denote the set of all primes by

$$\mathbb{P} \coloneqq \{\omega \in \mathbb{Z}_{\geq 2} : \delta \mid \omega \implies \delta \in \{1, \omega\}\}$$

and the set of all composites by

$$\mathbb{P}^c \coloneqq \mathbb{Z}_{\geq 2} \setminus \mathbb{P}.$$

In 300 BC, Euclid [13, Prop. 20] proved the following.

Theorem 1.4 (Euclid's theorem)**.** There are an infinite number of primes.

[1] Note, throughout this thesis, all divisors are assumed to be positive.

Proof. Assume the opposite. Let $\{a_k\}_{k=1}^N$ be the *finite* set of all primes. Further, let $a \coloneqq \prod_{k=1}^N a_k$ and $b \coloneqq a + 1$. Then, b is either prime or composite. If it is prime, we have a contradiction, as b is not in $\{a_k\}_{k=1}^N$. If b is composite, there must be some a_k that divides b. But since a_k divides a, it must also divide $b - a = 1$. However, no such prime exists. Therefore, our original assumption cannot hold. □

1.2 How do We Know if a Number is Prime?

The simplest algorithm to determine whether n is prime is to check if any integer in $[2, n-1]$ divides n. If not, n is prime. However, this is far from efficient. A simple, yet deterministic and relatively efficient method is discussed in this section.

Lemma 1.5. Let n be composite. Then, there exists a $\delta \leq \sqrt{n}$ such that $\delta \mid n$.

Proof. Assume the opposite. Let $n = \delta_1 \delta_2$, where $\delta_1, \delta_2 > \sqrt{n}$. Then,

$$n = \delta_1 \delta_2 > \sqrt{n}\sqrt{n} = n;$$

a contradiction. □

From Lemma 1.5 we find that when searching for whether n is prime, we only need to test potential factors until $\sqrt{n}$. If no such factor exists, then n is prime. Furthermore, it suffices to test potential factors which are prime. For example, if we know that 3 is not a factor, then $6 = 2 \cdot 3$ cannot possibly be one either. This gives us the following result.

Proposition 1.6. Let $n \in \mathbb{Z}_{\geq 2}$ with no prime factors less than or equal to $\sqrt{n}$. Then, n is prime.

In 1588, Pietro Cataldi used this method to determine that $2^{19} - 1$ is prime, which was the largest known prime number for almost two centuries [31, p. 486]. `Python` code for an algorithm implementing Proposition 1.6 to determine whether $n \in \mathbb{Z}_{\geq 2}$ is prime is shown below.

```
from sympy import primerange
from math import isqrt

def basic_primality_test(n):
    prime_list = primerange(isqrt(n) + 1)

    for d in prime_list:
        if n % d == 0:
            return("Composite")

    else:
        return("Prime")
```

There are, of course, much more advanced primality tests for arbitrary primes. A relatively recent discovery is the *AKS primality test* by Agrawal et al. [1].

However, we do not go into further details as it is not used in practice to determine the type of primes we are interested in; *Mersenne primes*.

2 Mersenne Primes

Definition 2.1. A *Mersenne prime* is a prime number that can be expressed as

$$M_n \coloneqq 2^n - 1, \tag{2.1}$$

where $n \in \mathbb{Z}_{\geq 2}$.

Mersenne primes are a subset of *Mersenne numbers* which simply is M_n without the primality requirement. Note that in this thesis we conveniently let $n \geq 2$ (in contrast to including 0 and 1) resulting in all Mersenne numbers being prime or composite. The latter is known as *Mersenne composites*. If $n \in \mathbb{P}$, we call M_n a *prime exponent Mersenne number*, or as I refer to them, PEMN for short. Concerning each subset of Mersenne numbers, PEMNs are by far the most studied, something that will become apparent later on in this text.

2.1 History

Mersenne primes have been known since the ancient Greeks. They are named in honour of the French monk and mathematician Marin Mersenne who studied them in the 17th century. Since then, a total of 52 Mersenne primes have been discovered. The largest, $M_{136,279,841}$, found in 2024, is over 41 million digits long [18] (see [21] where I have compiled $M_{136,279,841}$ in its entirety on 10,407 pages). For almost three decades, all new Mersenne primes have been discovered by the GIMPS project (see Section 5). A list of all discovered Mersenne primes can be seen in Table C.1 in Appendix C.

2.2 In Base 2

Mersenne numbers have a certain property that makes them interesting when expressed in binary form. But first, a lemma that generalises the difference of two squares formula, which we also use generously in several forthcoming proofs.

Lemma 2.2. Let $a, b \in \mathbb{R}$ and $n \in \mathbb{Z}_{\geq 2}$. Then,

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1}. \tag{2.2}$$

Proof. Distribute and expand the sum on the right-hand side;

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} &= \sum_{k=0}^{n-1}(a^{k+1}b^{n-k-1} - a^k b^{n-k}) \\ &= (ab^{n-1} - b^n) + (a^2 b^{n-2} - ab^{n-1}) + \cdots + (a^n - a^{n-1}b) \\ &= -b^n + (ab^{n-1} - ab^{n-1}) + \cdots + (a^{n-1}b - a^{n-1}b) + a^n \\ &= a^n - b^n,\end{aligned}$$

which equals the left-hand side of (2.2). □

If we let $a = 2$ and $b = 1$ in (2.2) we end up with

$$2^n - 1 = (2-1)\sum_{k=0}^{n-1} 2^k 1^{n-k-1},$$

or equivalently

$$M_n = \sum_{k=0}^{n-1} 2^k. \tag{2.3}$$

From (2.3) we can derive the following result when changing the base from decimal to binary.

Proposition 2.3. In base 2, M_n can be expressed as an n-digit repunit, i.e.

$$M_n = \underbrace{11\ldots1}_{n}{}_2. \tag{2.4}$$

Remark 2.4. Want to impress a friend? Tell him/her that you have memorised the world's biggest known prime number, $M_{136,279,841}$. When asked to demonstrate, simply say "one" 136,279,841 times (you never said that it had to be base 10). If you average one "one" each second, every minute, hour, and day, it would only take a bit more than four years to complete.

From Proposition 2.3, we get the trivial corollary when exploring *palindromic numbers*, i.e. numbers which stay the same when the digits are reversed.

Corollary 2.5. In base 2, all Mersenne numbers are palindromic.

2.3 An Alternative Definition

In some literature, Mersenne numbers are synonymous with PEMNs. The reasoning behind this can be explained by the following result.

Theorem 2.6. Let M_n be prime. Then, n is prime.

Proof. Suppose n is composite, i.e. $n = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}_{\geq 2}$. Then, according to Lemma 2.2;

$$M_n = 2^n - 1 = (2^\alpha)^\beta - 1 = (2^\alpha - 1)\cdot\sum_{k=0}^{\beta-1} 2^{\alpha k}.$$

Thus, $M_n \in \mathbb{P}^c$ as both factors are greater than 1.

By contraposition, if M_n is prime, it must follow that n is prime. □

Mersenne primes are ergo a subset of PEMNs. Therefore, when searching for new Mersenne primes, only PEMNs are to be considered. This is why some mathematicians see PEMNs and Mersenne numbers as the same. Furthermore, Theorem 2.6 gives us an equivalent definition to Definition 2.1.

Definition 2.7. A *Mersenne prime* is a prime number that can be expressed as

$$M_n \coloneqq 2^n - 1,$$

where n is prime.

Note that the reversed implication in Theorem 2.6 does not necessarily hold. Otherwise, we would end up with a brilliant prime number generator, making the latter part of this thesis rather redundant.

2.4 Generalisations

In this part, we look at two different ways to generalise Theorem 2.6. (The first theorem was originally proved by Ligh & Neal [22].) It turns out that Mersenne primes are quite unique in their form. The two corollaries follow directly from Theorem 2.6. We finish the section by introducing a generalisation of the two generalisations.

Theorem 2.8. Let M_n be a prime power, i.e. $M_n = p^N$ for some $p \in \mathbb{P}$ and $N \in \mathbb{Z}_{\geq 1}$. Then, $N = 1$.

Proof. We start by looking at the case $p = 2$. That $2^n - 1 \neq 2^N$ for all n and N should be considered trivial. Therefore, this scenario can be ignored.

Henceforth, we let $p \geq 3$. Firstly, assume that n is even, i.e. $n = 2m$ for some $m \in \mathbb{Z}_{\geq 1}$. Then,

$$M_n = 2^n - 1 = (2^m)^2 - 1 = (2^m + 1)(2^m - 1) \overset{!}{=} p^N.$$

For $m \geq 2$, p must divide both $2^m + 1$ and $2^m - 1$, and hence their difference $(2^m + 1) - (2^m - 1) = 2$. The only prime for which this applies is 2, but we assumed $p \geq 3$. Thus, a contradiction. If $m = 1$, however, then $n = 2$ and $M_n = 3$. This means $p^N = 3$ and clearly $N = 1$.

Now, assume n is odd, i.e. $n = 2m + 1$ for some $m \in \mathbb{Z}_{\geq 1}$, and $N \geq 2$. Then,

$$M_n = 2^n - 1 = 2^{2m+1} - 1 = 2(2^{2m} - 1) + 1 \overset{!}{=} p^N. \tag{2.5}$$

Observe that, by invoking Lemma 2.2;

$$2^{2m} - 1 = \sum_{k=0}^{2m-1} 2^k$$

and

$$p^N - 1 = (p - 1) \sum_{k=0}^{N-1} p^k.$$

Equation (2.5) is therefore equivalent to

$$\sum_{k=0}^{2m-1} 2^k = \frac{(p-1)}{2} \sum_{k=0}^{N-1} p^k. \tag{2.6}$$

If N is even, the right-hand side of (2.6) is even, since we have an integer multiplied by a sum of an even number of odd terms. On the other hand, the left-hand side is always odd, as it is a sum of even numbers and 1; a contradiction.

Suppose instead that N is odd. It holds that

$$2^n = p^N + 1 = (p+1) \sum_{k=0}^{N-1} (-p)^k$$

$$\iff \quad \frac{2^n}{p+1} = \sum_{k=0}^{N-1} (-p)^k. \tag{2.7}$$

Here, the right-hand side is an odd number of odd summands, i.e. odd. However, the left-hand side of (2.7) is even as $2^n > p + 1$ (this we know from our assumption $2^n - 1 = p^N > p$); another contradiction. Thus, $N \not\geq 2$, meaning $N = 1$ and the proof is complete. □

Corollary 2.9. Let M_n be a prime power. Then, n is prime.

Theorem 2.10. Let $a^n - 1 \in \mathbb{P}$, where $a \in \mathbb{N}$ and $n \in \mathbb{Z}_{\geq 2}$. Then, $a = 2$.

Proof. Because $a^n - 1 \geq 2$, it follows $a \geq 2$. Using Lemma 2.2;

$$a^n - 1 = (a - 1) \cdot \sum_{k=0}^{n-1} a^k. \tag{2.8}$$

The sum is clearly greater than 1. Therefore, for $a^n - 1$ to be prime, $a - 1$ must be equal to 1, so $a = 2$. □

Corollary 2.11. Let $a^n - 1 \in \mathbb{P}$, where $a \in \mathbb{N}$ and $n \in \mathbb{Z}_{\geq 2}$. Then, n is prime.

One might be tempted to combine Corollaries 2.9 and 2.11 to conclude that if $a^n - 1$ is a prime power, then n is prime. Well, it turns out that this is true.

Theorem 2.12. Let $a^n - 1$ be a prime power, where $a \in \mathbb{N}$ and $n \in \mathbb{Z}_{\geq 2}$. Then, n is prime.

Proof. We have $a^n - 1 = p^N$ for some $p \in \mathbb{P}$ and $N \in \mathbb{Z}_{\geq 1}$. Corollary 2.11 tells us the statement is true for $N = 1$, so what we need to consider is $N \geq 2$. The equation $a^n - 1 = p^N$ with the given conditions, is nothing less than a special case of Mihăilescu's theorem (also known as Catalan's conjecture) which famously says the only solution is

$$3^2 - 1 = 2^3.$$

This means $n = 2$, which of course is prime. □

2.5 Wieferich Primes

An interesting subset of primes is the following.

Definition 2.13. Let n be prime. If

$$2^{n-1} \equiv 1 \pmod{n^2}, \tag{2.9}$$

we call n a *Wieferich prime*.

Keeping in the theme of this thesis, we can equivalently define n to be a Wieferich prime if

$$n^2 \mid M_{n-1}. \tag{2.10}$$

Wieferich primes were first studied by the German mathematician Arthur Wieferich at the beginning of the 20th century as an attempt to prove the first case of Fermat's last theorem. As of writing, just two examples have been discovered; 1,093 and 3,511. Albeit, it has been conjectured that there exist infinitely many (see e.g. Crandall et al. [10]). But what is certain is that none of them are also Mersenne primes. (The only source for Theorem 2.14 that I have found is Wikipedia [30] from which I have made significant improvements to the provided proof.)

Theorem 2.14. Let M_n be prime. Then, M_n cannot be a Wieferich prime.

Proof. Assume M_n is a Wieferich prime, then by Definition 2.13;

$$2^{M_n-1} - 1 = M_{M_n-1} \equiv 0 \pmod{M_n^2}. \tag{2.11}$$

From Fermat's little theorem (see Theorem 4.8), we know

$$2^{M_n-1} - 1 \equiv 1 - 1 = 0 \pmod{M_n}.$$

This means that $M_n \mid M_{M_n-1}$, and therefore can (2.11) be rewritten as

$$\frac{M_{M_n-1}}{M_n} \equiv 0 \pmod{M_n}. \tag{2.12}$$

Again, using Fermat's little theorem, we see

$$M_n - 1 = 2^n - 2 \equiv 2 - 2 = 0 \pmod{n},$$

as n is prime by Theorem 2.6. This tells us n divides $M_n - 1$, i.e. $M_n - 1 = nk$, for some $k \in \mathbb{Z}$. Hence, (2.12) can be expressed as

$$\frac{M_{nk}}{M_n} \equiv 0 \pmod{M_n}. \tag{2.13}$$

The left-hand side is a geometric sum;

$$\frac{M_{nk}}{M_n} = \frac{(2^n)^k - 1}{2^n - 1} = \sum_{\ell=0}^{k-1} (2^n)^\ell.$$

As $M_n = 2^n - 1$, it follows that $2^n \equiv 1 \pmod{M_n}$. Thus,

$$\frac{M_{nk}}{M_n} = \sum_{\ell=0}^{k-1} (2^n)^\ell \equiv \sum_{\ell=0}^{k-1} 1^\ell = k \pmod{M_n}. \tag{2.14}$$

Combining (2.13) and (2.14), it follows

$$k \equiv 0 \pmod{M_n}.$$

Now, using $M_n - 1 = nk$, we have

$$-1 \equiv 0 \pmod{M_n};$$

a contradiction. The assumption (2.11) must therefore be false, thus proving that no prime can be both Mersenne and Wieferich. □

2.6 Perfect Numbers

Perfect numbers are one of the oldest concepts in number theory, first studied by mathematicians in ancient Greece. Before we define what they are, we introduce the *sigma function* as the sum of an integer's divisors, or more precisely

$$\varsigma(n) \coloneqq \sum_{\delta:\, \delta \mid n} \delta, \tag{2.15}$$

where $n \in \mathbb{N}$.

Example 2.15. The sum of the divisors of 69 equals 96.

Proof. Using the sigma function, we see

$$\varsigma(69) = 1 + 3 + 23 + 69 = 96. \tag{2.16}$$

□

Something that particularly interested ancient mathematicians was when the sum of the divisors equals twice the original number (or equivalently; the sum of all divisors strictly less than the number equals the number itself).

Definition 2.16. We call $n \in \mathbb{N}$ a *perfect* number if

$$\varsigma(n) = 2n. \tag{2.17}$$

Example 2.17. The number 28 is perfect.

Proof. From Definition 2.16, we find that

$$\varsigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28. \tag{2.18}$$

□

One important property of the sigma function is that it is—under the right conditions—multiplicative.

Lemma 2.18. Let $a, b \in \mathbb{Z}$ such that $\gcd(a,b) = 1$. Then,

$$\varsigma(ab) = \varsigma(a)\varsigma(b). \tag{2.19}$$

Proof. Let $\mathcal{A} \coloneqq \{\delta_{a1}, \delta_{a2}, \dots, \delta_{aN}\}$ and $\mathcal{B} \coloneqq \{\delta_{b1}, \delta_{b2}, \dots, \delta_{bM}\}$ be the sets of divisors of a and b, respectively. Then, the set of divisors of ab is

$$\mathcal{A} \times \mathcal{B} \coloneqq \{\delta_a \delta_b : \delta_a \in A, \delta_b \in B\}.$$

Since $\gcd(a,b) = 1$, there are no "duplicate" divisors of ab, i.e.

$$\delta_{ai}\delta_{bj} \neq \delta_{ak}\delta_{b\ell} \quad \text{if} \quad (i,j) \neq (k,\ell),$$

for all $i, k \in [1, N]$ and $j, \ell \in [1, M]$, and $|\mathcal{A}\times\mathcal{B}| = NM$. It therefore follows that

$$\begin{aligned}\varsigma(ab) &= \sum_{\delta \in \mathcal{A}\times\mathcal{B}} \delta = \sum_{\delta_a \in \mathcal{A}} \sum_{\delta_b \in \mathcal{B}} \delta_a \delta_b \\ &= \sum_{\delta_a \in \mathcal{A}} \delta_a \sum_{\delta_b \in \mathcal{B}} \delta_b = \varsigma(a)\varsigma(b).\end{aligned}$$

□

Remark 2.19. Lemma 2.18 can be generalised to show that $\varsigma(ab) \leq \varsigma(a)\varsigma(b)$ for any $a, b \in \mathbb{Z}$, with equality if and only if $\gcd(a,b) = 1$.

As of writing this thesis, all perfect numbers discovered have been even. Odd perfect numbers have neither been proven nor disproven to exist. If they do, however, we know from Ochem & Rao [26] that they must be at least greater than $10^{1,500}$ (the most recent lower bound is even larger at $10^{2,200}$).

It turns out that there is a bijection relation between Mersenne primes and even perfect numbers. Consequently, the number of known even perfect numbers is the same as known Mersenne primes (i.e. 52), and the discovery of one carries with it the discovery of the other. That a Mersenne prime implies the existence of a corresponding even perfect number ($\implies$ in Theorem 2.20) was first proven by Euclid [13, Prop. 36] (albeit the proof below is rather different). The reverse implication was shown by Euler [14, Sec. 8] around two millennia later.

Theorem 2.20 (Euclid–Euler theorem)**.** The integer ξ is even and perfect if and only if

$$\xi = \frac{M_n(M_n+1)}{2}, \tag{2.20}$$

for some prime M_n.

Proof. $\implies$: For the first implication, we assume that (2.20) is true. Then, we can write

$$\xi = 2^{n-1}(2^n - 1), \tag{2.21}$$

where $2^n - 1$ is assumed to be prime. There are two types of positive divisors for ξ; 2^k and $2^k(2^n-1)$, where $k \in [0, n-1]$. Therefore,

$$\begin{aligned}\varsigma(\xi) &= \sum_{k=0}^{n-1} 2^k + \sum_{k=0}^{n-1} 2^k(2^n-1) = 2^n \sum_{k=0}^{n-1} 2^k \\ &= 2^n(2^n-1) = 2\left(2^{n-1}(2^n-1)\right) = 2\xi,\end{aligned}$$

where we have used the formula for a geometric sum. Thus, by Definition 2.16, ξ is perfect. Furthermore, it is even as 2^{n-1} is a multiple of 2 because $n \geq 2$.

$\impliedby$: Because ξ is even, we can express it as $\xi = 2^N m$, where $N \in \mathbb{Z}_{\geq 1}$ and m is odd. Using Lemma 2.18 and the arguments above, we find

$$\varsigma(\xi) = \varsigma\left(2^N m\right) = \varsigma\left(2^N\right)\varsigma(m) = \left(2^{N+1}-1\right)\varsigma(m).$$

As ξ is perfect, the following must hold;

$$\begin{aligned}&\varsigma(\xi) = 2\xi = 2^{N+1}m \overset{!}{=} \left(2^{N+1}-1\right)\varsigma(m) \\ \iff\quad &\varsigma(m) = 2^{N+1} \cdot \frac{m}{2^{N+1}-1}.\end{aligned} \tag{2.22}$$

Observe that $2^{N+1}-1$ is odd (and greater than 1) and therefore must divide m, as $\varsigma(m)$ is an integer. Thus, $m/(2^{N+1}-1)$ will also divide m. On the other hand, using the definition of the sigma function;

$$\begin{aligned}\varsigma(m) &= \frac{m}{2^{N+1}-1} + m + \sum_{\delta \in \mathcal{D}} \delta \\ &= 2^{N+1} \cdot \frac{m}{2^{N+1}-1} + \sum_{\delta \in \mathcal{D}} \delta,\end{aligned} \tag{2.23}$$

where $\mathcal{D}$ is the subset of divisors of m such that $\{m/(2^{N+1}-1), m\} \nsubseteq \mathcal{D}$. The only way for (2.22) and (2.23) to both be true is if $\sum_{\delta\in\mathcal{D}} \delta = 0$ which implies $\mathcal{D} = \emptyset$. That is, $\{m/(2^{N+1}-1), m\}$ is the complete set of divisors. Furthermore, this tells us

$$\frac{m}{2^{N+1}-1} = 1,$$

as 1 is always a divisor of any integer. Thus, $m = 2^{N+1}-1$. Introducing the substitution $n = N+1$, we get $m = 2^n - 1 = M_n$. A number with solely 1 and itself as divisors is, by Definition 1.2, prime. Hence, we conclude that $M_n \in \mathbb{P}$. Finally, combining our results, we get

$$\xi = 2^N m = 2^{n-1}(2^n-1) = \frac{M_n(M_n+1)}{2},$$

which is the desired form. □

Using Theorem 2.20, we can provide an alternative proof to Example 2.17. We simply observe that

$$28 = \frac{7(7+1)}{2} = \frac{M_3(M_3+1)}{2}, \tag{2.24}$$

where of course M_3 is prime.

2.7 Distribution

A discussion regarding the distribution of Mersenne primes was made by Ribenboim [27, pp. 411–413]. In this section, we focus on two conjectures on the subject. The first was made in 1964 by Gillies [15].

Conjecture 2.21 (Gillies's conjecture)**.** The following three statements are true:

1. The number of Mersenne primes less than x is about
$$\frac{2}{\log 2}\log\log x \approx 2.8854\log\log x. \tag{2.25}$$
2. The expected number of Mersenne primes in the interval $[M_x, M_{2x}]$ is about 2.
3. The probability that M_n is prime is about
$$\frac{2}{\log 2}\cdot\frac{\log 2n}{n} \approx 2.8854\frac{\log 2n}{n}. \tag{2.26}$$

Remark 2.22. The probability theorist within me insists on making the following remark. The third statement of Conjecture 2.21—and Conjecture 2.24 as well—is incorrect from a proper probabilistic viewpoint. (The same also holds for the second statement.) A simple motivation for this is that there is no randomness in the primality of a given integer. Instead, the conjectures should not be viewed using the formal definition of probability, but rather as a frequentist interpretation of the proportion of PEMNs we expect to be prime. If we were to make it proper, this is how it should be done:

Let Ω be some sample space with a corresponding σ-algebra $\mathcal{F}$ to the sequence $(X_n)_{n\geq 2}$, where $X_n : \Omega \mapsto \mathbb{R}$ is the random variable
$$X_n(\omega) \coloneqq \begin{cases} 1 & \text{if} \quad M_n \in \mathbb{P}, \\ 0 & \text{if} \quad M_n \in \mathbb{P}^c; \end{cases} \tag{2.27}$$
for all $\omega \in \Omega$. Let $\mathcal{P} : \mathcal{F} \mapsto [0,1]$ be a probability measure on $(\Omega, \mathcal{F})$. Then,
$$\mathcal{P}(\{\omega \in \Omega : X_n(\omega) = 1\}) = \begin{cases} \mathcal{P}(\Omega) = 1 & \text{if} \quad M_n \in \mathbb{P}, \\ \mathcal{P}(\emptyset) = 0 & \text{if} \quad M_n \in \mathbb{P}^c; \end{cases} \tag{2.28}$$
which follows from the definition of probability measures. Clearly, (2.28) is not the same as (2.26) or (2.30). Furthermore, the result is completely trivial and does not help us in the slightest in acquiring information about Mersenne primes. Which could explain why Gillies and Wagstaff chose different approaches. For more details on probability spaces and random variables, see e.g. [2, Chs. 1–3].

Example 2.23. The second statement of Conjecture 2.21 is precise for $x = 100$ and $x = 100{,}000$.

Proof. We want to show that the intervals $[M_{100}, M_{200}]$ and $[M_{100,000}, M_{200,000}]$ contain two Mersenne primes each. Looking at Table C.1 shows that this is indeed the case, with $\{M_{107}, M_{127}\}$ and $\{M_{110,503}, M_{132,043}\}$ corresponding to the sets of Mersenne primes in each respective interval. □

In 1983, Wagstaff [29] proposed a new conjecture on the distribution of Mersenne primes. His conjecture is a modification of Gillies's, based on further heuristic and empirical evidence.

Conjecture 2.24 (Wagstaff's conjecture)**.** Let $\gamma = 0.57721\ldots$ be the Euler–Mascheroni constant. Then, the following three statements are true:

1. The number of Mersenne primes less than x is about
$$\frac{e^\gamma}{\log 2}\log\log x \approx 2.5695\log\log x. \tag{2.29}$$
2. The expected number of Mersenne primes in the interval $[M_x, M_{2x}]$ is about $e^\gamma \approx 1.7811$.
3. The probability that M_n is prime is about
$$\frac{e^\gamma}{\log 2}\cdot\frac{\log a_n n}{n} \approx 2.5695\frac{\log a_n n}{n}, \tag{2.30}$$
where
$$a_n = \begin{cases} 2 & \text{if} \quad n \equiv 3 \pmod 4, \\ 6 & \text{if} \quad n \equiv 1 \pmod 4. \end{cases} \tag{2.31}$$

Remark 2.25. Wagstaff's conjecture is also known as the Lenstra–Pomerance–Wagstaff conjecture, after Hendrik Lenstra and Carl Pomerance who independently derived (2.29) prior to Wagstaff.

Remark 2.26. Note that (2.30), as written in [27, p. 412], is incorrect.

Both conjectures can obviously not be true simultaneously. Arguments have been made in favour of both of them; however, no definitive proof has been presented. In the following section, I argue in favour of rejecting Conjecture 2.21, while abstaining from drawing conclusions regarding Conjecture 2.24.

2.7.1 Linear Regression

In this section, we analyse how well Gillies and Wagstaff's conjectures apply to the empirical evidence. To be able to easily illustrate the distribution of Mersenne primes, we approximate M_n with 2^n. Then,
$$\log\log M_n \approx \log\log 2^n = \log n + \log\log 2. \tag{2.32}$$

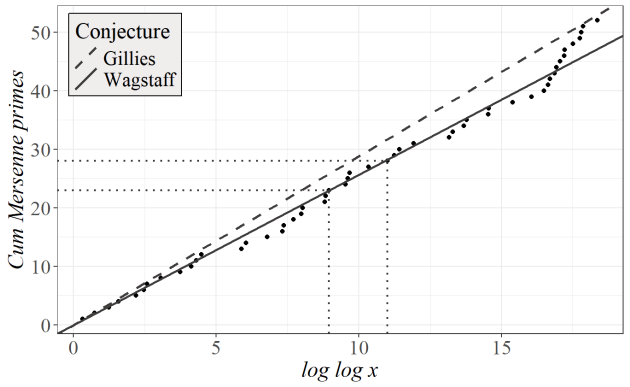

Figure 2.1: Plot of the number of Mersenne primes less than x and the expected ditto according to Gillies and Wagstaff's conjectures. The dotted lines indicate the number and size of Mersenne primes known at the time of writing the respective conjectures (Gillies's conjecture to the lower left).

As shown in Figure 2.1, when applying the log–log scale, the distribution seems to grow fairly linearly. However, there seems to be somewhat of an increase in the slope for the largest observed primes. Note that we have tacitly assumed that there are no unknown Mersenne primes less than $M_{136,279,841}$ (cf. the last paragraph of Section 6). If this is not the case, the slope would be even steeper. Both conjectures approximately follow the data, albeit Wagstaff's seems to have a better fit. An interesting observation is how—so far—extrapolating the model from its inception is still fairly accurate; indicating it is not unreasonable to believe the conjecture is true.

To test this further, we perform a simple linear regression on the 52 known Mersenne primes. Our conjectured model is

$$y(x) \coloneqq \beta_0 \log\log x, \tag{2.33}$$

where $y(x)$ is the expected number of Mersenne primes less than or equal to x. Under Gillies's conjecture, we assume $\beta_0 = 2/\log 2$, and for Wagstaff's, $\beta_0 = e^\gamma/\log 2$. We now fit the model

$$\hat{y}(x) \coloneqq \hat{\beta} \log\log x, \tag{2.34}$$

where $\hat{y}(x)$ is the estimated number of Mersenne primes less than or equal to x, and $\hat{\beta}$ is the least-square estimate of the slope defined as

$$\hat{\beta} \coloneqq \frac{\sum_{i=1}^{52}(\log\log x_i - \log\log\bar{x})(y_i - \bar{y})}{\sum_{i=1}^{52}(\log\log x_i - \log\log\bar{x})^2}; \tag{2.35}$$

where $y_i \coloneqq y(x_i)$, and $\log\log\bar{x} \coloneqq \frac{1}{52}\sum_{i=1}^{52}\log\log x_i$ and $\bar{y} \coloneqq \frac{1}{52}\sum_{i=1}^{52} y_i$ are the sample means. We find $\hat{\beta} \approx 2.5881$. Using a t-test, we can compare whether $\hat{\beta}$ is plausible given one of the two assumptions for β_0. Let

$$t \coloneqq \frac{\hat{\beta} - \beta_0}{s_{\hat{\beta}}}, \tag{2.36}$$

where $s_{\hat{\beta}}$ is the standard error such that

$$s_{\hat{\beta}} \coloneqq \sqrt{\frac{\frac{1}{52-1}\sum_{i=1}^{52}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{52}(\log\log x_i - \log\log\bar{x})^2}}. \tag{2.37}$$

Then, t has a Student's t-distribution with 51 degrees of freedom. This means that we can calculate the probability, or p-value, of observing $\hat{\beta}$ given that β_0 is true. The corresponding p-values are approximately $2.6 \cdot 10^{-19}$ ($t \approx -14$) for Gillies's conjecture and 0.89 ($t \approx 0.38$) for Wagstaff's. So, when using a standard threshold of significance at 0.05, we can confidently reject Gillies's conjecture.

However, in Wagstaff's conjecture, we cannot conclude its truthfulness. Judging from Figure 2.1, Wagstaff's conjecture seems to follow the empirical data rather well; albeit not perfect—especially for larger x. We most likely need to observe more Mersenne primes—if there are any (see Section 2.9)—to be able to make a conservative conclusion.

Remark 2.27. For a rigorous analysis, we would have to look at the model assumptions. As this is out of scope of this thesis, we will not delve into it. For further reading on linear regression, see e.g. [20, Ch. 3].

2.8 New Mersenne Conjecture

In 1644, Mersenne [24] made the following conjecture.

Conjecture 2.28 (Mersenne's conjecture)**.** Let $n \leq 257$. Then, M_n is prime if and only if

$$n \in \{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}.$$

Mersenne's conjecture was, however, incorrect. Not only are M_{67} and M_{257} composites, he also did not account for the primality of M_{61}, M_{89}, and M_{107}. This inspired Bateman et al. [3] to produce a new, and hopefully true, conjecture.

Conjecture 2.29 (New Mersenne conjecture)**.** Let $n \geq 1$ be odd. If two of the following statements hold, then so does the third:

1. $n = 2^k \pm 1$ or $n = 4^k \pm 3$.
2. M_n is prime.
3. $\frac{2^n+1}{3}$ is prime.

Each of the statements in Conjecture 2.29 are true for $n \in \{3, 5, 7, 13, 17, 19, 31, 61, 127\}$. No further examples have been found and all primes $n < 2 \cdot 10^7$ have

been checked [8]. Bateman et al. even argued that no number greater than 127 satisfies all three conditions. Given this, the conjecture could be rewritten as: for $n > 127$, either one or none of the statements holds.

2.9 How Many Mersenne Primes are There?

Perchance the most important and widely researched unanswered question regarding Mersenne primes is whether there exist infinitely many or not. The leading theory is that there are infinitely many, which is also the hypothesis presented in this thesis.

Conjecture 2.30. There are an infinite number of Mersenne primes.

Many mathematicians support this claim, see e.g. Ribenboim [27, p. 97]. Further, both Gillies and Wagstaff's conjectures imply that this would be the case. What is also not known is the infinitude of composite PEMNs. Thus, if one were to prove that one of the two groups is finite, then by complement the other would have to be infinite in size. Also, an interesting result if Conjecture 2.30 were to be proven true, is that it would imply there exists an infinite number of periodic primes in base 2 as per Corollary 2.5.

Before the discovery of $M_{136,279,841}$ this year, a counterargument to Conjecture 2.30 was that we had not discovered a new Mersenne prime since 2018. Such a long time between new primes had never occurred since the foundation of GIMPS. The fault in that thinking is that, as we have shown above, Mersenne primes seem to grow on a log–log scale. This is unbelievably slow. With this in mind, when observing Figure 2.1, the gap between the two largest known Mersenne primes no longer seems to be unprecedented.

2.10 Double Mersenne Primes

Looking at Definition 2.7, it is not unreasonable to ask oneself what happens when n itself is a Mersenne prime.

Definition 2.31. A *double Mersenne prime* is a prime number that can be expressed as

$$M_{M_n} = 2^{2^n-1} - 1, \tag{2.38}$$

where M_n is prime.

At the time of writing, four double Mersenne primes have been discovered:

$$\begin{aligned} M_{M_2} &= M_3 = 7, \\ M_{M_3} &= M_7 = 127, \\ M_{M_5} &= M_{31} = 2{,}147{,}483{,}647, \\ M_{M_7} &= M_{127} = 1.701\ldots \times 10^{38}. \end{aligned}$$

Before the age of computers, it was conjectured that all double PEMNs were prime. This is not the case, as M_{M_n} where $n \in \{13, 17, 19, 31\}$ are confirmed composites. For $n > 31$, the results are unknown. Although it has been conjectured that there exist no more primes than the four listed above (see e.g. Caldwell [7]).

2.10.1 Triple and Quadruple Mersenne Primes

If we take it one step further, we get *triple Mersenne primes*, i.e. primes of the form

$$M_{M_{M_n}} = 2^{2^{2^n-1}-1} - 1, \tag{2.39}$$

where M_{M_n} is prime. There are two known triple Mersenne primes:

$$\begin{aligned} M_{M_{M_2}} &= M_{M_3} = M_7 = 127, \\ M_{M_{M_3}} &= M_{M_7} = M_{127}. \end{aligned}$$

Lastly, observe that

$$M_{127} = M_{M_7} = M_{M_{M_3}} = M_{M_{M_{M_2}}},$$

making it the only known *quadruple Mersenne prime*.

This gives us the following beautiful result that

$$2^2 - 1, \quad 2^{2^2-1} - 1, \quad 2^{2^{2^2-1}-1} - 1, \quad \text{and} \quad 2^{2^{2^{2^2-1}-1}-1} - 1$$

are all primes. It is not certain if the pattern continues, as the next entry

$$2^{2^{2^{2^{2^2-1}-1}-1}-1} - 1 = M_{M_{M_{M_{M_2}}}} = M_{M_{127}},$$

simply is too large to calculate at the present moment (GIMPS allows users to test exponents up to 10^{10}).

2.10.2 A Conjecture

I would like to believe that the pattern continues for $k \geq 5$ and therefore propose the following conjecture. Maybe someday someone will prove (or disprove) its truthfulness.

Conjecture 2.32. Let the recursive sequence $(\mu_k)_{k\geq 1}$ be defined as

$$\mu_k \coloneqq \begin{cases} M_2 & \text{if } k = 1, \\ M_{\mu_{k-1}} & \text{else.} \end{cases} \tag{2.40}$$

Then, all elements of $(\mu_k)_{k\geq 1}$ are prime.

There are four key observations to make regarding Conjecture 2.32:

1. If Conjecture 2.32 is true, it would imply the more famous Conjecture 2.30—the existence of an infinite number of Mersenne primes.

2. If Conjecture 2.32 is true, it would also imply that there are an infinite number of double, triple, quadruple, et cetera, Mersenne Primes. Thus, if we can prove that one of those groups is finite, then the conjecture must be false.

3. If μ_5 is prime, then it would contradict Conjecture 2.29 as $(2^{M_{127}}+1)/3$ is proven composite (see [25]) while the first condition of the conjecture is true for all elements of $(\mu_k)_{k\geq 1}$.

4. If we prove that μ_p is composite for some $p \geq 5$, then we have shown that all elements of $(\mu_k)_{k\geq p}$ are composite, according to Theorem 2.6.

Remark 2.33. When researching Conjecture 2.32, I found that Catalan [9, p. 96] beat me to it with about 150 years (cf. Catalan–Mersenne numbers). Furthermore, some mathematicians, see e.g. Caldwell [7] and Good [16], believe the conjecture to be false.

3 Determining if M_n is composite

A great task in the quest of finding new Mersenne primes is rejecting Mersenne numbers which are *not* prime. It turns out that certain useful properties are associated with composite Mersenne numbers that can be used to drastically simplify this process. We discuss some of them in this section.

3.1 Sophie Germain Primes

A set of numbers connected to Mersenne numbers are *Sophie Germain primes*, named after the French mathematician Sophie Germain of the early 19th century.

Definition 3.1. Let n be prime. If $m = 2n+1$ is prime as well, we call n a *Sophie Germain prime*, while m is known as a *safe prime*.

The first five Sophie Germain primes are 2, 3, 5, 11, and 23 (and the corresponding safe primes are 5, 7, 11, 23, and 47). As shown in the theorem below [27, pp. 90–91], Sophie Germain primes can be used to easily find a composite PEMN.

Theorem 3.2. Let $n \geq 11$ be a Sophie Germain prime such that $n \equiv 3 \pmod 4$. Then, M_n is composite and the corresponding safe prime is one of its divisors.

Proof. Denote the safe prime by $m = 2n+1$. Because $n \equiv 3 \pmod 4$, we can write $n = 4k+3$ for some $k \in \mathbb{Z}$. Observe that

$$m = 2(4k+3)+1 = 8k+7 \equiv 7 \equiv -1 \pmod 8.$$

Then, by Lemma A.3; $(2/m) = 1$, where $(\cdot/\cdot)$ denotes the Legendre symbol (see Appendix A). That is, there exists some $b \in \mathbb{Z}$ such that $b^2 \equiv 2 \pmod m$. It follows,

$$\begin{aligned} M_n &= 2^n - 1 = 2^{(m-1)/2} - 1 \\ &\equiv b^{m-1} - 1 \equiv 1 - 1 = 0 \pmod m, \end{aligned}$$

according to Fermat's little theorem. Thus, m divides M_n. Moreover, as $n \geq 11$;

$$M_n = 2^n - 1 > 2n + 1 = m,$$

so M_n is composite. □

Remark 3.3. It can also be shown that if $2n+1$ divides M_n where $n \in \mathbb{P}$, then $2n+1 \in \mathbb{P}$, i.e. n is a Sophie Germain prime.

A consequence of Theorem 3.2 is that with the discovery of a new Sophie Germain prime, we can with limited computation trivially classify a Mersenne number as composite and obtain one of its prime factors.

Example 3.4. The Mersenne number M_{23} is composite.

Proof. We see that $23 \in \mathbb{P}$ is a Sophie Germain prime as $23 \cdot 2 + 1 = 47 \in \mathbb{P}$. Furthermore, $23 \equiv 3 \pmod 4$. Thus, by Theorem 3.2, $M_{23} \in \mathbb{P}^c$ with 47 as a divisor (the remaining being 178,481). □

3.1.1 "Mersenne–Germain Primes"

While studying Theorem 2.14, the question of if there exist primes that are both Mersenne and Sophie Germain—or what I would like to call *Mersenne–Germain primes*—occurred to me. I have not found any literature on the subject; however, the answer is rather simple.

Proposition 3.5. The number 3 is the only Mersenne–Germain prime.

Proof. Let M_n be prime. For M_n to be a Sophie Germain prime, then

$$2M_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 1 = M_{n+1}$$

must also be prime. Using Theorem 2.6, this tells us that n and $n+1$ must be primes. But the only solution to this is $n = 2$ and therefore $M_2 = 3$ is the single number that satisfies this property. □

3.2 Properties of Factors

When dealing with large Mersenne numbers, all methods to minimise the number of computations are highly appreciated. As shown here, Mersenne composites have some additional properties to e.g. Proposition 1.6. (The foundation of the proof of (3.1) is credited to Ribenboim [27, p. 91] and the statement[2] of (3.2) to Wagstaff [29, p. 385].) But we first introduce a lemma on multiplicative order.

[2] The author never proves (3.2), but instead writes "[i]t is well known".

Lemma 3.6. Let $\gcd(a, x) = 1$ for some $a \in \mathbb{Z}$ and $x \in \mathbb{Z}_{\geq 1}$. Further, let n be the multiplicative order of a modulo x, i.e. n is the smallest positive integer such that $a^n \equiv 1 \pmod{x}$. Then, $a^m \equiv 1 \pmod{x}$ if and only if m is a multiple of n.

Proof. $\Longrightarrow$: As m is a multiple of n, we can write $m = nk$ for some $k \in \mathbb{Z}$. Thus,

$$a^m = a^{nk} = (a^n)^k \equiv 1^k = 1 \pmod{x}.$$

$\Longleftarrow$: Let $m = nk + r$ for some $k, r \in \mathbb{Z}$ such that $0 \leq r < n$. Then,

$$a^m = a^{nk+r} = (a^n)^k a^r \equiv 1^k \cdot a^r = a^r \overset{!}{\equiv} 1 \pmod{x}.$$

If $r > 0$ it contradicts the definition of n as the order of a modulo x. Thus, $r = 0$ and m is a multiple of n. □

Remark 3.7. Lemma 3.6 can—with an analogous proof—be generalised to apply to the order of an element in a finite group (cf. [4, Thm 20.4]).

Theorem 3.8. Let $\delta \mid M_n$ such that $n \in \mathbb{P}_{\geq 3}$. Then,

$$\delta \equiv 1 \pmod{n} \quad \text{and} \quad \delta \equiv \pm 1 \pmod{8}. \tag{3.1}$$

Furthermore,

$$\delta = 2nk + 1, \tag{3.2}$$

where $k \equiv 0$ or $k \equiv -n \pmod{4}$.

Proof. The theorem is clearly true for $\delta = 1$. To prove (3.1), it suffices to show it holds for prime factors as composites follow trivially. We therefore let $\delta \in \mathbb{P}_{\geq 7}$ (no smaller prime fulfils the second part of the equation). That δ divides M_n implies

$$2^n \equiv 1 \pmod{\delta}. \tag{3.3}$$

Because n is prime and $\gcd(2, \delta) = 1$, it from follows from Lemma 3.6 that n is the multiplicative order of 2 modulo δ. Further, from Fermat's little theorem, we know

$$2^{\delta - 1} \equiv 1 \pmod{\delta}.$$

Then, by the same lemma, there exists some $m \in \mathbb{Z}$ such that $\delta - 1 = mn$ or, since $\delta - 1$ is even, $\delta - 1 = 2kn$, for some $k \in \mathbb{Z}$. Therefore,

$$\delta = 2kn + 1 \equiv 1 \pmod{n}, \tag{3.4}$$

proving the first part of (3.1). Now, using Theorem A.2 and (3.3);

$$\left(\frac{2}{\delta}\right) = 2^{\frac{\delta-1}{2}} = 2^{\frac{2kn}{2}} = (2^n)^k \equiv 1^k = 1 \pmod{\delta}.$$

Lastly, by Lemma A.3, the remaining part of (3.1) follows.

Note that in (3.4) we in passing showed (3.2). We now prove the aforementioned condition for k. As n is odd, we have $n \equiv 1$ or $n \equiv 3 \pmod{4}$. This gives us four cases to examine:

1. $n \equiv 1 \pmod{4}$ and $\delta \equiv 1 \pmod{8}$.

   We have

   $$\begin{aligned} & \delta = 2kn + 1 \equiv 1 \pmod{8} \\ \iff \quad & 2kn = 8\ell \\ \iff \quad & kn = 4\ell, \end{aligned}$$

   for some $\ell \in \mathbb{Z}$. By assumption $kn \equiv k \pmod{4}$. Thus, $k \equiv 0 \pmod{4}$.

2. $n \equiv 1 \pmod{4}$ and $\delta \equiv -1 \pmod{8}$.

   If $\delta \equiv -1 \pmod{8}$, we analogously have $kn + 1 \equiv 4\ell \pmod{4}$, for some $\ell \in \mathbb{Z}$. This tells us $k \equiv -1 \equiv -n \pmod{4}$.

3. $n \equiv 3 \pmod{4}$ and $\delta \equiv 1 \pmod{8}$.

   Now we analyse the case $n \equiv 3 \equiv -1 \pmod{4}$. The modulo 8 results from earlier do not change. When $\delta \equiv 1 \pmod{8}$, we have $kn \equiv -k \equiv 0 \pmod{4}$, i.e. $k \equiv 0 \pmod{4}$.

4. $n \equiv 3 \pmod{4}$ and $\delta \equiv -1 \pmod{8}$.

   For $\delta \equiv -1 \pmod{8}$, observe $kn + 1 \equiv -k + 1 \equiv 0 \pmod{4}$ or $k \equiv 1 \equiv -3 \equiv -n \pmod{4}$.

To conclude, $k \equiv 0$ or $k \equiv -n \pmod{4}$. □

Remark 3.9. Note that Theorem 3.8 holds even when M_n is prime.

Example 3.10. The divisors of M_{11} fulfil Theorem 3.8.

Proof. Note $M_{11} = 2047 = 23 \cdot 89$. Thus, if $\delta \mid M_{11}$, then $\delta \in \{1, 23, 89, 2047\}$. Now, observe that

$$\begin{aligned} 1 &\equiv 1 \pmod{11} \quad \text{and} \quad 1 \equiv 1 \pmod{8}, \\ 23 &\equiv 1 \pmod{11} \quad \text{and} \quad 23 \equiv -1 \pmod{8}, \\ 89 &\equiv 1 \pmod{11} \quad \text{and} \quad 89 \equiv 1 \pmod{8}, \\ 2047 &\equiv 1 \pmod{11} \quad \text{and} \quad 2047 \equiv -1 \pmod{8}; \end{aligned}$$

thereby satisfying (3.1). Moreover,

$$\begin{aligned} 1 &= 2 \cdot 11 \cdot 0 + 1, \\ 23 &= 2 \cdot 11 \cdot 1 + 1, \\ 89 &= 2 \cdot 11 \cdot 4 + 1, \\ 2047 &= 2 \cdot 11 \cdot 93 + 1; \end{aligned}$$

where $0 \equiv 4 \equiv 0 \pmod{4}$ and $1 \equiv 93 \equiv -11 \pmod{4}$, fulfilling (3.2) and the theorem. □

Using Theorem 3.8, Leonhard Euler proved in 1772 that M_{31} is prime. Instead of testing all 4,792 potential prime factors, he limited his search to 372 factors (fewer if excluding composites) [31, p. 486].

Theorem 3.8 also tells us the following.

Corollary 3.11. Let $\delta \mid M_n$ such that $\delta > 1$ and $n \in \mathbb{P}_{\geq 3}$. Then, $\delta \geq 2n + 1$.

Remark 3.12. I have not seen Corollary 3.11 explicitly written before—perhaps it is too obvious. But I believe that it is significant, as it provides a lower bound to Proposition 1.6 for Mersenne numbers. Furthermore, it implies that when M_n increases, so does its smallest divisor (excluding 1).

3.3 Uniqueness of Factors

Another useful result on factors, shown by Edington [11], is Theorem 3.16 listed below. However, the author's proof is somewhat hard to follow, which prompted me to this alternative method. Furthermore, Edington restricts his statement to prime factors; an assumption that I disregard, as it is not needed for this proof. But first, we introduce some lemmas.

Lemma 3.13. We have $\delta \mid a$ and $\delta \mid b$ if and only if $\delta \mid \gcd(a, b)$.

Proof. $\implies$: We can rewrite a and b such that $a = \alpha \gcd(a, b)$ and $b = \beta \gcd(a, b)$ for some $\alpha, \beta \in \mathbb{Z}$. So, given $\delta \mid \gcd(a, b)$, the divisibility of a and b follows.

$\impliedby$: It holds that $a = k\delta$ and $b = \ell\delta$, for some $k, l \in \mathbb{Z}$. Bézout's identity tells us

$$ax + by = \gcd(a, b), \tag{3.5}$$

for some $x, y \in \mathbb{Z}$. Substitution gives

$$\gcd(a, b) = k\delta x + \ell\delta y = \delta(kx + \ell y)$$

and thus $\delta \mid \gcd(a, b)$. □

Lemma 3.14. Let $a, b \in \mathbb{Z}_{\geq 1}$ such that $a \mid b$ and $b \mid a$. Then, $a = b$.

Proof. The assumptions can be reformulated as $b = ka$ and $a = \ell b$, for some $k, \ell \in \mathbb{Z}_{\geq 1}$. Combining the two, tells us $a = \ell k a$ or $k\ell = 1$. But k and ℓ are integers, so therefore $k = \ell = 1$. Thus, $a = 1 \cdot b = b$. □

Lemma 3.15. Let $a, n, m \in \mathbb{Z}_{\geq 1}$. Then,

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(n,m)} - 1. \tag{3.6}$$

Proof. For convenience, let $\delta_1 \coloneqq \gcd(a^n - 1, a^m - 1)$ and $\delta_2 \coloneqq \gcd(n, m)$. It holds

$$a^n \equiv 1 \pmod{\delta_1} \quad \text{and} \quad a^m \equiv 1 \pmod{\delta_1}.$$

We can now write

$$1 \equiv a^n a^m \equiv (a^n)^x (a^m)^y = a^{nx+my} \pmod{\delta_1},$$

for all $x, y \in \mathbb{Z}$. Choose x and y such that $nx + my = \gcd(n, m) = \delta_2$. Then, it follows

$$a^{\delta_2} \equiv 1 \pmod{\delta_1}$$

or equivalently

$$\gcd(a^n - 1, a^m - 1) \mid (a^{\gcd(n,m)} - 1). \tag{3.7}$$

On the other hand, we have the following. We can write $n = \alpha\delta_2$ and $m = \beta\delta_2$ for some $\alpha, \beta \in \mathbb{Z}$. It follows using Lemma 2.2;

$$a^n - 1 = (a^{\delta_2})^\alpha - 1 = (a^{\delta_2} - 1) \sum_{k=0}^{\alpha-1} a^{\delta_2 k},$$
$$a^m - 1 = (a^{\delta_2})^\beta - 1 = (a^{\delta_2} - 1) \sum_{k=0}^{\beta-1} a^{\delta_2 k}.$$

From this, it is clear that $a^{\delta_2} - 1$ divides $a^n - 1$ and $a^m - 1$, which from Lemma 3.13 tells us $a^{\delta_2} - 1$ divides δ_1. Or, to be more precise;

$$(a^{\gcd(n,m)} - 1) \mid \gcd(a^n - 1, a^m - 1). \tag{3.8}$$

Combining (3.7) and (3.8) with Lemma 3.14, finally gives us

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(n,m)} - 1.$$

□

Letting $a = 2$ in (3.6), we find

$$\gcd(M_n, M_m) = M_{\gcd(n,m)}. \tag{3.9}$$

Theorem 3.16. Let $\delta \in \mathbb{Z}_{\geq 2}$ and $n, m \in \mathbb{P}$ such that $\delta \mid M_n$ and $\delta \mid M_m$. Then, $n = m$.

Proof. Assume the opposite, i.e. $\delta \mid M_n$ and $\delta \mid M_m$ for some $n \neq m$. Then, from Lemma 3.13, it follows that δ divides $\gcd(M_n, M_m)$. But by Lemma 3.15 with $a = 2$, we get

$$\begin{aligned}\gcd(M_n, M_m) &= \gcd(2^n - 1, 2^m - 1) \\ &= 2^{\gcd(n,m)} - 1 = 2^1 - 1 = 1,\end{aligned}$$

as n and m are distinct primes and therefore coprime to each other. What we have thus shown, is that $\delta \mid 1$, but $\delta > 1$ so it cannot divide 1. That is, our original assumption must be wrong. □

A way to paraphrase Theorem 3.16 is that an integer greater than 1 can at most divide one unique PEMN. An important consequence of this, is that when searching for potential factors for a suspected Mersenne prime, we do not need to test numbers which are known factors in other PEMNs. Thereby, making the algorithm deduced from combining Proposition 1.6, Theorem 3.8, and Corollary 3.11 even more efficient. This also motivates the study of computing factors for known composite PEMNs.

4 Determining if M_n is Prime

4.1 Lucas–Lehmer Primality Test

The *Lucas–Lehmer primality test* was the first systematic method introduced to determine whether a Mersenne number is prime or not. It is named after Édouard Lucas who developed it in the late 19th century and D. H. Lehmer who proved it about 50 years later. The test follows a simple algorithm and was until 2018 the method of choice for GIMPS in finding new Mersenne primes. In fact, all Mersenne primes from M_{521} until $M_{82,589,933}$ have been uncovered using the Lucas–Lehmer test [18]. We express the test as the following theorem.

Theorem 4.1 (Lucas–Lehmer primality test)**.** Let the recursive sequence $(s_k)_{k\geq 1}$ be defined as

$$s_k \coloneqq \begin{cases} 4 & \text{if } k = 1, \\ s_{k-1}^2 - 2 & \text{else.} \end{cases} \tag{4.1}$$

Then, M_n is prime, where $n \in \mathbb{P}_{\geq 3}$, if and only if

$$s_{n-1} \equiv 0 \pmod{M_n}. \tag{4.2}$$

Proof. See Section 4.1.1. □

Example 4.2. The Mersenne number $M_5 = 31$ is prime.

Proof. We find the first four terms in $(s_k)_{k\geq 1}$ to be 4, 14, 194, and 37,634. Observe that $37,634 = 31 \cdot 1,214$; i.e. $37,634 \equiv 0 \pmod{31}$. Thus, according to Theorem 4.1; $M_5 \in \mathbb{P}$. □

It is not hard to see that s_k increases rapidly for large values of k. As we are only interested in the remainder (or lack thereof) of our final term, we can use the rules of modular arithmetic and perform a reduction modulo M_n in each step. Hence, limiting the squaring operation to numbers less than M_n. However, for humongous Mersenne numbers, squaring the remainder is still computationally demanding. In practice, this is addressed by splitting the number into pieces forming a large array. We then perform a fast *Fourier transform*, square it, and finally use an inverse Fourier transform to obtain the squared number. We do not go into further detail on this procedure. Instead, we refer to Egusquiza Castillo's [12] *tour de force* on Fourier transforms.

Simple `Python` code for the Lucas–Lehmer primality test (where we use the remainder from dividing with M_n at each term) can be seen below.

```
def Lucas_Lehmer_primality_test(n):
    M_n = 2 ** n - 1
    s_k = 4

    for k in range(2, n):
        s_k = (s_k ** 2 - 2) % M_n

    if s_k == 0:
        return("Prime")

    else:
        return("Composite")
```

4.1.1 Proof of the Lucas–Lehmer Primality Test

To prove the Lucas–Lehmer primality test, it is convenient to express s_k in closed form. It turns out that this is possible.

Lemma 4.3. Let s_k be defined as in (4.1). Then, for all $k \geq 1$;

$$s_k = \omega^{2^{k-1}} + \bar{\omega}^{2^{k-1}}, \tag{4.3}$$

where $\omega \coloneqq 2 + \sqrt{3}$ and $\bar{\omega} \coloneqq 2 - \sqrt{3}$.

Proof. The proof is done using induction:

Our base case is $k = 1$ and we see

$$s_1 = \omega^{2^0} + \bar{\omega}^{2^0} = \omega + \bar{\omega} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4,$$

which agrees with (4.1).

Now, assume (4.3) holds for some $k = p$ where $p \geq 1$, i.e.

$$s_p = \omega^{2^{p-1}} + \bar{\omega}^{2^{p-1}}.$$

Then, it holds for $k = p + 1$, as

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

where we have used that

$$\omega\bar{\omega} = (2 + \sqrt{3})(2 - \sqrt{3}) = 1. \tag{4.4}$$

Thus, according to the principle of induction, (4.3) holds for all $k \geq 1$. □

Remark 4.4. The reason (4.3) is not used in practice is because it is insanely computationally demanding for large values of k.

We also introduce the following two lemmas, where the first one is a true case of the *freshman's dream*.

Lemma 4.5. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{P}$. Then,

$$(a + b)^n \equiv a^n + b^n \pmod{n}. \tag{4.5}$$

Proof. By the binomial theorem, we have

$$\begin{aligned} (a + b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^n b^{n-k} \\ &= a^n + b^n + n \sum_{k=1}^{n-1} \frac{(n-1)!}{k!(n-k)!} a^n b^{n-k}. \end{aligned}$$

Because $n \in \mathbb{P}$ and $k, (n-k) < n$, we have $\gcd(n, k!) = \gcd(n, (n-k)!) = 1$, for all $k \in [1, n-1]$. Thus,

$$n \sum_{k=1}^{n-1} \frac{(n-1)!}{k!(n-k)!} a^n b^{n-k} \equiv 0 \pmod{n},$$

and the lemma follows. □

Lemma 4.6. Let $n \geq 3$ be odd. Then,

$$2^n \equiv 8 \pmod{12}. \tag{4.6}$$

Proof. Clearly,

$$2^3 = 8 \equiv 8 \pmod{12}.$$

Assuming (4.6) is true for some odd $n = p$ where $p \geq 3$, it is also true for the next odd number $n = p + 2$, as

$$2^{p+2} = 4 \cdot 2^p \equiv 4 \cdot 8 = 32 \equiv 8 \pmod{12}.$$

Thus, by the principle of induction, the lemma is true. □

For the proof presented in the following of the Lucas–Lehmer primality test, the reader is expected to have a rudimentary knowledge of group and ring theory. To prove the sufficiency of the test, i.e. $s_{n-1} \equiv 0 \pmod{M_n} \implies M_n \in \mathbb{P}$, we use the results of Bruce [5] and his humorously named article *A Really Trivial Proof of the Lucas–Lehmer Test*. The necessity implication is maybe somewhat less "really trivial" and the proof we show follows the structure of Rödseth [28].

Proof of Theorem 4.1. $\implies$: We prove the implication using *reductio ad absurdum*. Given $s_{n-1} \equiv 0 \pmod{M_n}$, then by Lemma 4.3;

$$s_{n-1} = \omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}} \equiv 0 \pmod{M_n}.$$

Thus, $\omega^{2^{k-2}} + \bar{\omega}^{2^{k-2}} = kM_n$ for some $k \in \mathbb{Z}$. Rearranging and multiplying by $\omega^{2^{n-2}}$, we end up with

$$\begin{aligned} \left(\omega^{2^{n-2}}\right)^2 &= kM_n\omega^{2^{n-2}} - (\omega\bar{\omega})^{2^{n-2}} \\ \iff \quad \omega^{2^{n-1}} &= kM_n\omega^{2^{n-2}} - 1, \end{aligned} \tag{4.7}$$

where (4.7) follows from (4.4).

Now, assume M_n is composite. Let δ be the smallest prime factor for M_n. Because M_n is odd, it follows $\delta \geq 3$. Let $X \coloneqq \{a + \sqrt{3}b : a, b \in \mathbb{Z}_\delta\}$ and $X^* \coloneqq \{x \in X : x^{-1} \in X\}$, where $\mathbb{Z}_\delta = \{0, 1, \ldots, \delta - 1\}$ is the set of all integers modulo δ. It is clear that X under multiplication is associative, commutative, and has 1 as the identity element (of course $1 = 1 + \sqrt{3} \cdot 0 \in X$). In addition, it is closed, as for $a, b, c, d \in \mathbb{Z}_\delta$, we have

$$\begin{aligned} &(a + \sqrt{3}b)(c + \sqrt{3}d) \\ &\quad = [ac + 3bd \pmod{\delta}] + \sqrt{3}[ad + bc \pmod{\delta}] \in X. \end{aligned}$$

All these properties also apply to X^* and thus X^* is an Abelian group.

It is established that zero lacks an inverse for multiplication. This tells us $0 \notin X^*$, while on the other hand $0 = 0 + \sqrt{3} \cdot 0 \in X$. Thus,

$$|X^*| \leq |X| - 1 = \delta^2 - 1.$$

From our assumption, we have $M_n \equiv 0 \pmod{\delta}$. Moreover, $\omega \in X$ meaning

$$kM_n\omega^{2^{n-2}} = 0 \text{ in } X.$$

Then, by (4.7);

$$\omega^{2^{n-1}} = -1 \text{ in } X. \tag{4.8}$$

Squaring both sides results in

$$\omega^{2^n} = 1 \text{ in } X.$$

Thus, $\omega^{-1} = \omega^{2^n - 1}$ in X and $\omega \in X^*$. From Remark 3.7 we know that the order of ω divides 2^n. However, note from (4.8) that $\omega^{2^{n-1}} \neq 1$ in X. Therefore, by the reversed implication of the same remark, the order of ω cannot divide 2^{n-1} or, in fact, any smaller number (as 2^{n-1} would have be a multiple of it). This concludes that the order of ω equals 2^n.

It is known that the order of an element is at most the order of the group, so

$$2^n \leq |X^*| \leq \delta^2 - 1 < \delta^2. \tag{4.9}$$

But δ is the smallest prime factor of the composite M_n, so by Lemma 1.5;

$$\delta^2 \leq M_n = 2^n - 1. \tag{4.10}$$

Combining (4.9) and (4.10) we have $2^n < 2^n - 1$; an obvious contradiction. Hence, our assumption that $M_n \in \mathbb{P}^c$ is incorrect, so $M_n \in \mathbb{P}$, which is what we wanted to show.

$\impliedby$: We now let $M_n \in \mathbb{P}$ where $n \in \mathbb{P}_{\geq 3}$. From Lemma 4.6 we have

$$M_n = 2^n - 1 \equiv 8 - 1 = 7 \equiv -5 \pmod{12}.$$

Then, by Lemma A.4, we see $(3/M_n) = -1$, or written using Theorem A.2;

$$3^{\frac{M_n - 1}{2}} \equiv -1 \pmod{M_n}. \tag{4.11}$$

We know $2^n \equiv 1 \pmod{M_n}$. Therefore,

$$2 = 2 \cdot 1 \equiv 2 \cdot 2^n = 2^{n+1} = \left(2^{\frac{n+1}{2}}\right)^2 \pmod{M_n}$$

and we can conclude that 2 is a quadratic residue modulo M_n (as $2^{\frac{n+1}{2}}$ is an integer) and $(2/M_n) = 1$. Thus,

$$2^{\frac{M_n - 1}{2}} \equiv 1 \pmod{M_n}. \tag{4.12}$$

Now, using (4.11) and (4.12) we find

$$24^{\frac{M_n-1}{2}} = \left(2^{\frac{M_n-1}{2}}\right)^3 \cdot 3^{\frac{M_n-1}{2}} \equiv 1^3 \cdot (-1) = -1 \pmod{M_n}. \tag{4.13}$$

Let $\sigma \coloneqq 2\sqrt{3}$ so that

$$\frac{(6+\sigma)^2}{24} = \frac{(6+2\sqrt{3})^2}{24} = 2+\sqrt{3} = \omega. \tag{4.14}$$

Further, let $Y \coloneqq \{a+\sqrt{3}b : a,b \in \mathbb{Z}_{M_n}\}$. It is easily shown that Y fulfils the properties of a ring under multiplication and addition. We see

$$(6+\sigma)^{M_n} = 6+\sigma^{M_n} = 6+2^{M_n}\cdot 3^{\frac{M_n-1}{2}}\cdot\sqrt{3} = 6+2\cdot(-1)\cdot\sqrt{3} = 6-\sigma \text{ in } Y, \tag{4.15}$$

where we have used Lemma 4.5, Fermat's little theorem, and (4.11).

Combining our results from (4.13)–(4.15), we get

$$\omega^{\frac{M_n+1}{2}} = \frac{(6+\sigma)^{M_n+1}}{24^{\frac{M_n+1}{2}}} = \frac{(6+\sigma)(6+\sigma)^{M_n}}{24\cdot 24^{\frac{M_n-1}{2}}} = \frac{(6+\sigma)(6-\sigma)}{24\cdot(-1)} = -1 \text{ in } Y.$$

Adding 1 and multiplying by $\bar{\omega}^{\frac{M_n+1}{4}}$ we end up with

$$\begin{aligned} 0 &= \omega^{\frac{M_n+1}{2}}\cdot\bar{\omega}^{\frac{M_n+1}{4}} + \bar{\omega}^{\frac{M_n+1}{4}} \\ &= \omega^{\frac{M_n+1}{4}}\cdot(\omega\bar{\omega})^{\frac{M_n+1}{4}} + \bar{\omega}^{\frac{M_n+1}{4}} \\ &= \omega^{\frac{M_n+1}{4}} + \bar{\omega}^{\frac{M_n+1}{4}} = \omega^{\frac{2^n-1+1}{4}} + \bar{\omega}^{\frac{2^n-1+1}{4}} \\ &= \omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}} = s_{n-1} \text{ in } Y. \end{aligned}$$

Since $s_{n-1} = 0$ in Y, we can write $s_{n-1} \equiv 0 \pmod{M_n}$; which is what we wanted. □

4.2 Fermat Primality Test

Our next test is—unlike e.g. the Lucas–Lehmer test—probabilistic. This means that it does not give a guaranteed answer as to whether or not a number is prime. However, the idea is that the probability that it is composite is incredibly small. To understand this, we present the following definition.

Definition 4.7. Let $n \in \mathbb{Z}_{\geq 2}$. If n satisfies a condition satisfied by all prime numbers, but not by most composite numbers, we call n a *probable prime*.

One of these conditions is the famous *Fermat's little theorem*, proposed by Pierre de Fermat in 1640.

Theorem 4.8 (Fermat's little theorem)**.** Let $n \in \mathbb{P}$ and $a \in \mathbb{N}$ such that $n \nmid a$. Then,

$$a^{n-1} \equiv 1 \pmod{n}. \tag{4.16}$$

Proof. See Section 4.2.1. □

Observe that Theorem 4.8 is not an equivalence relation, i.e. there exist composite numbers that fulfil (4.16). Though, they are in general rare, giving us the *Fermat primality test*.

Corollary 4.9 (Fermat primality test)**.** Let n be a potential prime and choose some $a \in I \subset \mathbb{N}$ such that $n \nmid a$. Then, if

$$a^{n-1} \equiv 1 \pmod{n},$$

n is a probable prime. Otherwise, n must be composite.

The idea behind Corollary 4.9 is that it is unlikely that the congruence holds for an arbitrarily chosen a if n is composite. The test is, however, not a guarantee of primality. Although it is a great indicator for further study of the suspected prime in question. Either by applying the Fermat primality test again for another value of a or using a completely different test, such as the Lucas–Lehmer test. Also, it works for all types of potential primes—not just Mersenne numbers.

When choosing I, there are key considerations to observe. For example, if $a = 1$ all values of n are classified as probable primes. Also, if n is odd—which of course is the case for all primes excluding 2—then the same holds for $a = n-1$, as

$$(n-1)^{n-1} \equiv (-1)^{n-1} = 1 \pmod{n}.$$

Therefore, these trivial cases are often omitted. Thus, a good candidate for I is $[2, n-2]$, as it excludes trivial cases and avoids multiples of n. It can also be appropriate to choose a low value for a, as it is faster to compute. If the tested number is composite, this means that we can comparatively quickly reject it.

Conceptual `Python` code of the Fermat primality test for Mersenne numbers and $I = [2, M_n - 2]$ can be found below. Note, however, this code is crazily slow for large n. In practice, something like, e.g. exponentiation by squaring combined with a fast Fourier transform, would be needed to make these computations within reasonable time.

```
from random import randint

def Fermat_primality_test(n):
    M_n = 2 ** n - 1
    a = randint(2, M_n - 2)

    if a ** (M_n - 1) % M_n == 1:
        return("Probable prime")

    else:
        return("Composite")
```

4.2.1 Proof of Fermat's Little Theorem

Fermat's little theorem can be proven in several ways using vastly different methods. Like his *last theorem*, Fermat never proved it himself; writing in a letter to a fellow mathematician "I would send you a demonstration of it, if I did not fear going on for too long" [23, p. 295]. The first proof of Fermat's little theorem was made by Leonhard Euler [27, p. 22]. The proof we choose to demonstrate is inspired by that of Ivory [19]. Let us start by introducing three necessary lemmas.

Lemma 4.10 (Euclid's lemma)**.** Let $n \mid \alpha\beta$ where $n \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{Z}$. Then, $n \mid \alpha$ or $n \mid \beta$.

Proof. Assume that $n \nmid \alpha$ and thus $\gcd(\alpha, n) = 1$. Then, using Bézout's identity;

$$\alpha x + ny = 1,$$

for some $x, y \in \mathbb{Z}$. Multiplying by β results in

$$\alpha\beta x + \beta n y = \beta.$$

It is clear that n divides both terms in the left-hand side. Thus, n must also divide their sum, i.e. $n \mid \beta$.

The other case follows by symmetry. □

Lemma 4.11. Let $a, x, y \in \mathbb{Z}$ and $n \in \mathbb{P}$ such that $\gcd(a, n) = 1$. Then,

$$x \equiv y \pmod{n} \quad \Longleftrightarrow \quad ax \equiv ay \pmod{n}. \tag{4.17}$$

Proof. $\Longrightarrow$: We know $x - y = kn$, for some $k \in \mathbb{Z}$. Then,

$$ax - ay = a(x - y) = akn \equiv 0 \pmod{n},$$

or equivalently $ax \equiv ay \pmod{n}$.

$\Longleftarrow$: From Lemma 4.10, we know that n must divide a or $x - y$. But $\gcd(a, n) = 1$ so n cannot divide a. Therefore, n must divide $x - y$ which is the same as $x \equiv y \pmod{n}$. □

Lemma 4.12. Let $a \in \mathbb{Z}_{\geq 1}$ and $n \in \mathbb{P}$ such that $\gcd(a, n) = 1$. Then, the set of remainders when dividing $a, 2a, \ldots, (n-1)a$ by n equals $\{1, 2, \ldots, (n-1)\}$.

Proof. First, we know that none of $a, 2a, \ldots, (n-1)a$ can be congruent to zero modulo n as per our assumptions and Lemma 4.10. This means all remainders have to be in $[1, n-1]$. Now, we show that all remainders are distinct. Let

$$ka \equiv \ell a \pmod{n},$$

for some $k, \ell \in [1, n-1]$. Then, by Lemma 4.11;

$$k \equiv \ell \pmod{n},$$

which can only be true if $k = \ell$. □

We now possess the necessary components to complete the proof of Fermat's little theorem.

Proof of Theorem 4.8. Using Lemma 4.12 and the variables as defined in it, we get

$$a \cdot 2a \cdots (n-1)a \equiv 1 \cdot 2 \cdots (n-1) \pmod{n},$$

which is equivalent to

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

Now, by conjuring Lemma 4.11, we have

$$a^{n-1} \equiv 1 \pmod{n};$$

the theorem. □

5 Great Internet Mersenne Prime Search

The *Great Internet Mersenne Prime Search*, more commonly known as simply GIMPS, is the leading platform for discovering new Mersenne primes. Founded in 1996 by George Woltman, it has been responsible for finding all new Mersenne primes since then; a total of 18 as of writing this thesis.

The idea behind GIMPS is that users download a free piece of software called `Prime95` or `mprime`. The user then chooses what test to perform and is assigned an appropriate PEMN. For example, users can search for factors, verify previous tests using the Lucas–Lehmer primality test, or test completely new PEMNs using the Fermat primality test. The Fermat primality test was implemented in 2018 to replace the Lucas–Lehmer test which had been used since the start. The reason behind this is that the Fermat test is faster, more reliable, and has a lower chance of missing a new prime. Six years later, the first Mersenne prime using Fermat's primality test was discovered. Note, however, GIMPS classifies the official date of discovery for when the test was confirmed using a Lucas–Lehmer test, as the Fermat test technically only discovered a probable prime.

In 2024, GIMPS had more than 270,000 users working on close to 3 million computers. To incentivise people to use their programme, GIMPS offers a cash reward of $3,000 for each new Mersenne prime discovered. For primes with more than 100 million digits (the smallest such Mersenne number being $M_{332,192,857}$) the reward is $150,000. For more information on the Great Internet Mersenne Prime Search, we refer to their website: `https://www.mersenne.org/`.

6 Personal Contributions

Alongside writing this thesis, I have myself used GIMPS on two computers to contribute to finding

new Mersenne primes. The type of test I focused on was verifying previously made Lucas–Lehmer primality tests. The reason for opting to verify—rather than undertaking the more glamorous task of testing unknown Mersenne numbers—is mainly because it is much faster. When verifying, we work with numbers M_n where $n \approx 75,000,000$ (which takes 1–2 weeks), while for new numbers we must go to $n > 125,000,000$ (which usually takes over a month). Not only can we test more numbers this way, but we also decrease the potential loss of a computer failure which is not negligible.

I completed 12 Lucas–Lehmer tests. All results returned the same conclusion as in the first attempt, i.e. negative for new Mersenne primes. The findings are summarised in Table B.1. There, we find a hyperlink to the number's page on GIMPS's website for further details. The pages can also be accessed at `https://www.mersenne.ca/exponent/n` where `n` is replaced with the prime exponent of the Mersenne number in question.

While performing the Lucas–Lehmer tests (which were supposed to be the main focus of this section), I was assigned a total of 188 certifications of recently completed Fermat primality tests. This usually happened several times a day, the most of which was ten tests in 24 hours. These certifications require approximately 150–500,000 iterations (compare this to $n \approx 75,000,000$ for Lucas–Lehmer) and were usually completed in an hour. The results are presented in Table B.2. Thanks to this, I was able to complete many more tests than originally planned. However, as with the previous tests, all Mersenne numbers checked were determined to be composite.

The "probability" of finding a Mersenne prime among those listed in Tables B.1 and B.2 can be estimated using Equation (2.30) (assuming that Wagstaff's conjecture holds). Let $\mathcal{N}$ be the set of exponents for the 200 Mersenne numbers we tested. Assuming we obtain no further information knowing the initial tests were unsuccessful, the probability of discovering at least one prime is the complement to all Mersenne numbers being composite, i.e.

$$1 - \prod_{n \in \mathcal{N}} \left(1 - \frac{e^\gamma}{\log 2} \cdot \frac{\log a_n n}{n}\right) \approx 0.0092\ \%. \tag{6.1}$$

Therefore, it should not come as a surprise that I did not discover a new prime. (In reality, the probability is much, much smaller as there is a slim chance any of the original tests failed to begin with.)

Finally, I was also assigned 28 Fermat primality tests on already proven composite PEMNs. These tests were not performed on the number itself, but on its *cofactor*. Let $\delta_1, \delta_2, \ldots, \delta_N$ be the known prime factors for the composite M_n. Then, $M_n/(\prod_{k=1}^{N} \delta_k)$ is known as the cofactor for M_n. It is of interest to determine if the cofactor is prime, as this would mean the number is fully factorised. Otherwise, further factorisation is needed (cf. the discussion to Theorem 3.16). The results of these certifications were that all of the tested cofactors were composite, which aligned with the original results. They can be seen in Table B.3.

Although I have not discovered any new primes, I have at least contributed to adding knowledge about what Mersenne numbers are *not* prime. Moreover, as shown in Table C.1, the ranks of the 49th, 50th, 51st, and 52nd Mersenne primes are not certain. This means that there could be Mersenne primes that are missed between them. And by doing these verifications in Table B.1, I have taken some small steps to find out if this is the case. However, the journey towards this is far from over and GIMPS [17] predicts that at this current rate, it will take until the year 3200 to settle whether the 52nd Mersenne prime is indeed the 52nd.

A Notes on Quadratic Residues

The following material is not central to the thesis but is necessary to complete some of the proofs, which serves as motivation for this appendix.

Definition A.1. Let $p \in \mathbb{P}_{\geq 3}$ and $a, b \in \mathbb{Z}$ such that $\gcd(a, p) = 1$ and $a \equiv b^2 \pmod{p}$. Then, a is called a *quadratic residue* modulo p.

In his study of quadratic residues, Adrien-Marie Legendre introduced the following notation:

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{else.} \end{cases} \tag{A.1}$$

A general formula for (a/p) was derived by Leonhard Euler.

Theorem A.2 (Euler's criterion)**.** Let $p \in \mathbb{P}_{\geq 3}$ and $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$. Then,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}. \tag{A.2}$$

Interesting cases for us is $a = 2$ and $a = 3$ which has certain useful properties.

Lemma A.3. Let $p \in \mathbb{P}_{\geq 3}$. Then,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}, \end{cases} \tag{A.3}$$

Lemma A.4. Let $p \in \mathbb{P}_{\geq 5}$. Then,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}, \end{cases} \tag{A.4}$$

As it is out of the objective for this thesis, we refrain from proving Theorem A.2 and Lemmas A.3–A.4. Instead, for proofs and further reading on the subject, we refer to [6, Ch. 9] for the interested reader.

B Results from Primality Tests

Table B.1: Results from verifying Lucas–Lehmer primality tests.

M_n	Result	Original test	Completion date	URL
$M_{70,849,997}$	Composite	*Anonymous* (2017)	2024-10-09	1
$M_{70,984,063}$	Composite	Curtis Cooper (2015)	2024-10-22	2
$M_{70,977,163}$	Composite	"Templar" (2015)	2024-10-16	3
$M_{71,315,693}$	Composite	"arnaud" (2017)	2024-09-26	4
$M_{71,342,833}$	Composite	"Xolotl" (2017)	2024-10-02	5
$M_{73,574,629}$	Composite	Dave Ward (2016)	2024-05-26	6
$M_{75,631,121}$	Composite	Curtis Cooper (2017)	2024-08-29	7
$M_{75,646,411}$	Composite	Åke Tilander (2017)	2024-09-01	8
$M_{75,672,353}$	Composite	"Chappy" (2016)	2024-08-25	9
$M_{76,640,953}$	Composite	Steppen Herring (2017)	2024-09-09	10
$M_{77,038,583}$	Composite	*Anonymous* (2016)	2024-10-09	11
$M_{77,940,739}$	Composite	*Anonymous* (2018)	2024-09-18	12

Table B.2: Results from certifying Fermat primality tests.

M_n	Result	Original test	Completion date	URL
$M_{70,980,863}$	Composite	"k0r3" (2024)	2024-10-12	1
$M_{71,192,861}$	Composite	Luke Durant (2024)	2024-10-20	2
$M_{71,261,831}$	Composite	Luke Durant (2024)	2024-10-20	3
$M_{71,274,971}$	Composite	Luke Durant (2024)	2024-10-20	4
$M_{71,566,249}$	Composite	Luke Durant (2024)	2024-10-20	5
$M_{71,628,451}$	Composite	Luke Durant (2024)	2024-10-21	6
$M_{72,194,839}$	Composite	Luke Durant (2024)	2024-10-22	7
$M_{74,332,933}$	Composite	Luke Durant (2024)	2024-10-16	8
$M_{74,301,631}$	Composite	Luke Durant (2024)	2024-10-17	9
$M_{74,601,587}$	Composite	Luke Durant (2024)	2024-10-22	10
$M_{74,900,873}$	Composite	Luke Durant (2024)	2024-10-15	11
$M_{75,203,741}$	Composite	Luke Durant (2024)	2024-10-15	12
$M_{75,221,383}$	Composite	Luke Durant (2024)	2024-10-19	13
$M_{75,318,011}$	Composite	Luke Durant (2024)	2024-10-15	14
$M_{75,718,961}$	Composite	Luke Durant (2024)	2024-10-16	15
$M_{75,770,621}$	Composite	Luke Durant (2024)	2024-10-19	16
$M_{75,836,963}$	Composite	Luke Durant (2024)	2024-10-16	17
$M_{75,914,281}$	Composite	Luke Durant (2024)	2024-10-20	18
$M_{75,942,821}$	Composite	Luke Durant (2024)	2024-10-16	19
$M_{75,936,437}$	Composite	Luke Durant (2024)	2024-10-17	20
$M_{76,057,483}$	Composite	Luke Durant (2024)	2024-10-16	21
$M_{76,072,049}$	Composite	Luke Durant (2024)	2024-10-18	22
$M_{76,101,283}$	Composite	Luke Durant (2024)	2024-10-19	23
$M_{76,303,001}$	Composite	Luke Durant (2024)	2024-10-16	24
$M_{76,350,871}$	Composite	Luke Durant (2024)	2024-10-18	25
$M_{76,501,081}$	Composite	Luke Durant (2024)	2024-10-18	26
$M_{76,501,493}$	Composite	Luke Durant (2024)	2024-10-18	27
$M_{76,533,241}$	Composite	Luke Durant (2024)	2024-10-16	28
$M_{76,567,147}$	Composite	Luke Durant (2024)	2024-10-17	29
$M_{76,668,169}$	Composite	Luke Durant (2024)	2024-10-20	30
$M_{76,694,557}$	Composite	Luke Durant (2024)	2024-10-19	31
$M_{76,830,959}$	Composite	Luke Durant (2024)	2024-10-17	32
$M_{76,979,527}$	Composite	Luke Durant (2024)	2024-10-19	33
$M_{77,029,679}$	Composite	Luke Durant (2024)	2024-10-19	34

Table B.2: Results from certifying Fermat primality tests.

M_n	Result	Original test	Completion date	URL
$M_{77,117,951}$	Composite	Luke Durant (2024)	2024-10-17	35
$M_{77,953,229}$	Composite	Luke Durant (2024)	2024-10-22	36
$M_{78,234,451}$	Composite	Luke Durant (2024)	2024-10-19	37
$M_{78,380,779}$	Composite	Luke Durant (2024)	2024-10-20	38
$M_{78,452,119}$	Composite	Luke Durant (2024)	2024-10-20	39
$M_{82,799,723}$	Composite	Luke Durant (2024)	2024-10-18	40
$M_{82,813,337}$	Composite	Luke Durant (2024)	2024-10-16	41
$M_{82,862,837}$	Composite	Luke Durant (2024)	2024-10-14	42
$M_{82,922,911}$	Composite	Luke Durant (2024)	2024-10-15	43
$M_{82,993,739}$	Composite	Luke Durant (2024)	2024-10-16	44
$M_{126,494,129}$	Composite	Luke Durant (2024)	2024-08-28	45
$M_{126,863,981}$	Composite	Luke Durant (2024)	2024-09-10	46
$M_{127,780,021}$	Composite	Luke Durant (2024)	2024-08-28	47
$M_{128,089,867}$	Composite	Luke Durant (2024)	2024-08-30	48
$M_{129,126,157}$	Composite	Luke Durant (2024)	2024-08-29	49
$M_{129,548,869}$	Composite	Luke Durant (2024)	2024-09-03	50
$M_{129,568,757}$	Composite	Luke Durant (2024)	2024-08-27	51
$M_{129,599,797}$	Composite	Luke Durant (2024)	2024-08-28	52
$M_{129,604,373}$	Composite	Luke Durant (2024)	2024-08-27	53
$M_{129,616,681}$	Composite	Luke Durant (2024)	2024-08-27	54
$M_{129,653,527}$	Composite	Luke Durant (2024)	2024-08-28	55
$M_{129,785,627}$	Composite	Luke Durant (2024)	2024-08-29	56
$M_{129,796,697}$	Composite	Luke Durant (2024)	2024-08-30	57
$M_{129,816,509}$	Composite	Luke Durant (2024)	2024-08-30	58
$M_{129,907,249}$	Composite	Luke Durant (2024)	2024-08-31	59
$M_{129,929,717}$	Composite	Luke Durant (2024)	2024-09-20	60
$M_{130,029,443}$	Composite	Luke Durant (2024)	2024-09-24	61
$M_{130,264,033}$	Composite	Luke Durant (2024)	2024-09-03	62
$M_{130,285,031}$	Composite	Luke Durant (2024)	2024-09-04	63
$M_{130,365,329}$	Composite	Luke Durant (2024)	2024-09-04	64
$M_{130,414,589}$	Composite	Luke Durant (2024)	2024-09-06	65
$M_{130,432,649}$	Composite	Luke Durant (2024)	2024-09-24	66
$M_{130,449,691}$	Composite	Luke Durant (2024)	2024-09-05	67
$M_{130,487,899}$	Composite	Luke Durant (2024)	2024-09-05	68
$M_{130,512,461}$	Composite	Luke Durant (2024)	2024-09-05	69
$M_{130,572,653}$	Composite	Luke Durant (2024)	2024-09-07	70
$M_{130,577,581}$	Composite	Luke Durant (2024)	2024-09-06	71
$M_{130,598,003}$	Composite	Luke Durant (2024)	2024-09-06	72
$M_{130,606,639}$	Composite	Luke Durant (2024)	2024-09-08	73
$M_{130,689,719}$	Composite	Luke Durant (2024)	2024-09-07	74
$M_{130,725,653}$	Composite	Luke Durant (2024)	2024-09-07	75
$M_{130,742,107}$	Composite	Luke Durant (2024)	2024-09-26	76
$M_{130,770,421}$	Composite	Luke Durant (2024)	2024-09-08	77
$M_{130,792,213}$	Composite	Luke Durant (2024)	2024-09-26	78
$M_{130,824,983}$	Composite	Luke Durant (2024)	2024-09-07	79
$M_{130,912,729}$	Composite	Luke Durant (2024)	2024-09-30	80
$M_{130,961,717}$	Composite	Luke Durant (2024)	2024-09-08	81
$M_{131,255,837}$	Composite	Luke Durant (2024)	2024-09-09	82
$M_{131,430,197}$	Composite	Luke Durant (2024)	2024-09-10	83
$M_{131,503,037}$	Composite	Luke Durant (2024)	2024-09-10	84
$M_{131,566,867}$	Composite	Luke Durant (2024)	2024-09-28	85
$M_{131,708,729}$	Composite	Luke Durant (2024)	2024-09-23	86
$M_{131,810,827}$	Composite	Luke Durant (2024)	2024-09-20	87
$M_{131,877,539}$	Composite	Luke Durant (2024)	2024-10-01	88

Table B.2: Results from certifying Fermat primality tests.

M_n	Result	Original test	Completion date	URL
$M_{131,922,559}$	Composite	Luke Durant (2024)	2024-09-16	89
$M_{131,946,743}$	Composite	Chun Sung Soo (2024)	2024-09-24	90
$M_{132,043,151}$	Composite	Luke Durant (2024)	2024-10-06	91
$M_{132,043,151}$	Composite	Luke Durant (2024)	2024-10-06	92
$M_{132,061,961}$	Composite	Luke Durant (2024)	2024-10-14	93
$M_{132,131,723}$	Composite	Luke Durant (2024)	2024-09-19	94
$M_{132,350,521}$	Composite	Luke Durant (2024)	2024-09-21	95
$M_{132,369,703}$	Composite	Luke Durant (2024)	2024-09-20	96
$M_{132,417,871}$	Composite	Luke Durant (2024)	2024-09-23	97
$M_{132,501,671}$	Composite	Luke Durant (2024)	2024-09-22	98
$M_{132,507,281}$	Composite	Luke Durant (2024)	2024-09-21	99
$M_{132,507,667}$	Composite	Luke Durant (2024)	2024-10-04	100
$M_{132,532,627}$	Composite	Luke Durant (2024)	2024-09-21	101
$M_{132,539,339}$	Composite	Luke Durant (2024)	2024-09-22	102
$M_{132,584,981}$	Composite	Luke Durant (2024)	2024-09-22	103
$M_{132,628,393}$	Composite	Luke Durant (2024)	2024-09-22	104
$M_{132,633,569}$	Composite	Luke Durant (2024)	2024-09-22	105
$M_{132,645,281}$	Composite	Luke Durant (2024)	2024-09-22	106
$M_{132,723,229}$	Composite	Luke Durant (2024)	2024-09-22	107
$M_{132,743,761}$	Composite	Luke Durant (2024)	2024-09-22	108
$M_{132,761,723}$	Composite	Luke Durant (2024)	2024-09-23	109
$M_{133,079,203}$	Composite	Luke Durant (2024)	2024-09-24	110
$M_{133,080,173}$	Composite	Luke Durant (2024)	2024-09-24	111
$M_{133,128,461}$	Composite	Luke Durant (2024)	2024-09-25	112
$M_{133,175,489}$	Composite	Luke Durant (2024)	2024-09-25	113
$M_{133,273,883}$	Composite	Luke Durant (2024)	2024-09-26	114
$M_{133,382,191}$	Composite	Luke Durant (2024)	2024-09-26	115
$M_{133,422,803}$	Composite	Luke Durant (2024)	2024-10-11	116
$M_{133,430,887}$	Composite	Luke Durant (2024)	2024-10-08	117
$M_{133,487,477}$	Composite	Luke Durant (2024)	2024-09-29	118
$M_{133,554,143}$	Composite	Luke Durant (2024)	2024-09-27	119
$M_{133,583,033}$	Composite	Luke Durant (2024)	2024-09-27	120
$M_{133,586,581}$	Composite	Luke Durant (2024)	2024-09-27	121
$M_{133,622,561}$	Composite	Luke Durant (2024)	2024-10-11	122
$M_{133,628,153}$	Composite	Luke Durant (2024)	2024-09-27	123
$M_{133,664,413}$	Composite	Luke Durant (2024)	2024-09-27	124
$M_{133,737,077}$	Composite	Luke Durant (2024)	2024-09-27	125
$M_{133,769,021}$	Composite	Luke Durant (2024)	2024-09-28	126
$M_{133,818,779}$	Composite	Luke Durant (2024)	2024-09-28	127
$M_{133,852,181}$	Composite	Luke Durant (2024)	2024-09-29	128
$M_{133,864,327}$	Composite	Luke Durant (2024)	2024-09-25	129
$M_{133,894,517}$	Composite	Luke Durant (2024)	2024-09-28	130
$M_{133,918,633}$	Composite	Luke Durant (2024)	2024-10-09	131
$M_{134,035,589}$	Composite	Luke Durant (2024)	2024-10-04	132
$M_{134,045,189}$	Composite	Luke Durant (2024)	2024-10-04	133
$M_{134,056,877}$	Composite	Luke Durant (2024)	2024-10-04	134
$M_{134,155,919}$	Composite	Luke Durant (2024)	2024-10-05	135
$M_{134,168,953}$	Composite	Luke Durant (2024)	2024-10-04	136
$M_{134,210,327}$	Composite	Luke Durant (2024)	2024-09-29	137
$M_{134,218,289}$	Composite	Luke Durant (2024)	2024-09-29	138
$M_{134,218,307}$	Composite	Luke Durant (2024)	2024-09-29	139
$M_{134,295,737}$	Composite	Luke Durant (2024)	2024-09-30	140
$M_{134,377,993}$	Composite	Luke Durant (2024)	2024-09-30	141
$M_{134,440,547}$	Composite	Luke Durant (2024)	2024-09-30	142

Table B.2: Results from certifying Fermat primality tests.

M_n	Result	Original test	Completion date	URL
$M_{134,466,799}$	Composite	Luke Durant (2024)	2024-09-30	143
$M_{134,642,953}$	Composite	Luke Durant (2024)	2024-10-01	144
$M_{134,689,171}$	Composite	Luke Durant (2024)	2024-10-02	145
$M_{134,726,833}$	Composite	Luke Durant (2024)	2024-10-02	146
$M_{134,760,097}$	Composite	Luke Durant (2024)	2024-10-15	147
$M_{134,783,273}$	Composite	Luke Durant (2024)	2024-10-13	148
$M_{134,786,837}$	Composite	Luke Durant (2024)	2024-10-05	149
$M_{134,797,511}$	Composite	Luke Durant (2024)	2024-10-02	150
$M_{134,802,419}$	Composite	Luke Durant (2024)	2024-10-02	151
$M_{134,859,343}$	Composite	Luke Durant (2024)	2024-10-03	152
$M_{134,901,719}$	Composite	Luke Durant (2024)	2024-10-03	153
$M_{134,937,787}$	Composite	Luke Durant (2024)	2024-10-03	154
$M_{134,960,717}$	Composite	Luke Durant (2024)	2024-10-03	155
$M_{135,014,069}$	Composite	Luke Durant (2024)	2024-10-05	156
$M_{135,029,537}$	Composite	Luke Durant (2024)	2024-10-05	157
$M_{135,189,493}$	Composite	Luke Durant (2024)	2024-10-06	158
$M_{135,319,417}$	Composite	Luke Durant (2024)	2024-10-06	159
$M_{135,391,049}$	Composite	Luke Durant (2024)	2024-10-07	160
$M_{135,471,733}$	Composite	Luke Durant (2024)	2024-10-07	161
$M_{135,547,891}$	Composite	Luke Durant (2024)	2024-10-07	162
$M_{135,616,483}$	Composite	Luke Durant (2024)	2024-10-08	163
$M_{135,643,639}$	Composite	Luke Durant (2024)	2024-10-08	164
$M_{135,819,797}$	Composite	Luke Durant (2024)	2024-10-09	165
$M_{135,826,547}$	Composite	Luke Durant (2024)	2024-10-09	166
$M_{135,948,559}$	Composite	Luke Durant (2024)	2024-10-09	167
$M_{136,056,077}$	Composite	Luke Durant (2024)	2024-10-10	168
$M_{136,134,931}$	Composite	Luke Durant (2024)	2024-10-10	169
$M_{136,154,167}$	Composite	Luke Durant (2024)	2024-10-10	170
$M_{136,172,809}$	Composite	Luke Durant (2024)	2024-10-12	171
$M_{136,215,689}$	Composite	Luke Durant (2024)	2024-10-10	172
$M_{136,283,041}$	Composite	Luke Durant (2024)	2024-10-11	173
$M_{136,462,691}$	Composite	Luke Durant (2024)	2024-10-12	174
$M_{136,476,127}$	Composite	Luke Durant (2024)	2024-10-12	175
$M_{136,545,407}$	Composite	Luke Durant (2024)	2024-10-12	176
$M_{136,582,769}$	Composite	Luke Durant (2024)	2024-10-12	177
$M_{136,625,527}$	Composite	Luke Durant (2024)	2024-10-14	178
$M_{136,655,557}$	Composite	Luke Durant (2024)	2024-10-12	179
$M_{136,795,517}$	Composite	Luke Durant (2024)	2024-10-13	180
$M_{136,802,629}$	Composite	Luke Durant (2024)	2024-10-13	181
$M_{136,893,787}$	Composite	Luke Durant (2024)	2024-10-13	182
$M_{136,966,409}$	Composite	Luke Durant (2024)	2024-10-14	183
$M_{137,025,289}$	Composite	Luke Durant (2024)	2024-10-14	184
$M_{137,148,071}$	Composite	Luke Durant (2024)	2024-10-17	185
$M_{146,794,913}$	Composite	"MathEnthousiast" (2024)	2024-09-25	186
$M_{148,364,323}$	Composite	Curtis Cooper (2024)	2024-09-29	187
$M_{164,353,429}$	Composite	Curtis Cooper (2024)	2024-09-23	188

Table B.3: Results from certifying Fermat primality tests on cofactors. The number of known prime factors for M_n is denoted by N.

M_n	N	Result	Original test	Completion date	URL
$M_{311,539}$	1	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-08-28	1
$M_{311,561}$	1	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-08-28	2
$M_{311,569}$	4	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-08-28	3
$M_{311,609}$	1	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-08-28	4
$M_{315,899}$	2	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-08-30	5
$M_{379,177}$	1	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	6
$M_{379,273}$	3	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	7
$M_{379,277}$	2	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	8
$M_{379,283}$	2	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	9
$M_{405,719}$	2	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	10
$M_{405,731}$	4	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	11
$M_{405,749}$	1	Composite cofactor	"kkmrkkblmbrbk" (2024)	2024-10-01	12
$M_{699,719}$	3	Composite cofactor	"timc995" (2024)	2024-09-24	13
$M_{4,687,919}$	1	Composite cofactor	"feather" (2024)	2024-10-12	14
$M_{16,895,609}$	3	Composite cofactor	"Feritin" (2024)	2024-10-11	15
$M_{17,017,727}$	1	Composite cofactor	Luke Durant (2024)	2024-08-27	16
$M_{17,024,587}$	1	Composite cofactor	Luke Durant (2024)	2024-08-27	17
$M_{17,034,103}$	1	Composite cofactor	Luke Durant (2024)	2024-08-28	18
$M_{17,042,539}$	2	Composite cofactor	Luke Durant (2024)	2024-08-30	19
$M_{17,090,699}$	2	Composite cofactor	Luke Durant (2024)	2024-09-06	20
$M_{17,124,911}$	1	Composite cofactor	"XZT" (2024)	2024-09-08	21
$M_{17,152,781}$	1	Composite cofactor	"Perig" (2024)	2024-09-11	22
$M_{17,212,991}$	1	Composite cofactor	Luke Durant (2024)	2024-09-19	23
$M_{17,261,029}$	1	Composite cofactor	"dnova" (2024)	2024-10-03	24
$M_{17,311,391}$	3	Composite cofactor	Luke Durant (2024)	2024-10-19	25
$M_{17,319,329}$	4	Composite cofactor	Luke Durant (2024)	2024-10-22	26
$M_{17,322,233}$	2	Composite cofactor	Alvin Bunk (2024)	2024-10-19	27
$M_{18,937,241}$	2	Composite cofactor	Jason Lynch (2024)	2024-09-02	28

C List of Known Mersenne Primes

Table C.1: The 52 known Mersenne prime numbers [18]. The rank after 48 is not verified as denoted by *. The lowest unverified Mersenne number is $M_{70,578,077}$ and the lowest untested Mersenne number is $M_{124,817,431}$ as of 20 November 2024 [17].

Rank	M_n	Digits	Discovered	Discoverer
1	M_2	1	*c.* 500 BC	*Unkown*
2	M_3	1	*c.* 500 BC	*Unkown*
3	M_5	2	*c.* 275 BC	*Unkown*
4	M_7	3	*c.* 275 BC	*Unkown*
5	M_{13}	4	1456	*Unkown*
6	M_{17}	6	1588	Pietro Cataldi
7	M_{19}	6	1588	Pietro Cataldi
8	M_{31}	10	1772	Leonhard Euler
9	M_{61}	19	1883	Ivan Mikheevich Pervushin
10	M_{89}	27	1911	R. E. Powers
11	M_{107}	33	1914	R. E. Powers
12	M_{127}	39	1876	Édouard Lucas
13	M_{521}	157	1952	Raphael M. Robinson
14	M_{607}	183	1952	Raphael M. Robinson

Table C.1: The 52 known Mersenne prime numbers [18]. The rank after 48 is not verified as denoted by *. The lowest unverified Mersenne number is $M_{70,578,077}$ and the lowest untested Mersenne number is $M_{124,817,431}$ as of 20 November 2024 [17].

Rank	M_n	Digits	Discovered	Discoverer
15	$M_{1,279}$	386	1952	Raphael M. Robinson
16	$M_{2,203}$	664	1952	Raphael M. Robinson
17	$M_{2,281}$	687	1952	Raphael M. Robinson
18	$M_{3,217}$	969	1957	Hans Riesel
19	$M_{4,253}$	1,281	1961	Alexander Hurwitz
20	$M_{4,423}$	1,332	1961	Alexander Hurwitz
21	$M_{9,689}$	2,917	1963	Donald B. Gillies
22	$M_{9,941}$	2,993	1963	Donald B. Gillies
23	$M_{11,213}$	3,376	1963	Donald B. Gillies
24	$M_{19,937}$	6,002	1971	Bryant Tuckerman
25	$M_{21,701}$	6,533	1978	Landon Curt Noll & Laura Nickel
26	$M_{23,209}$	6,987	1979	Landon Curt Noll
27	$M_{44,497}$	13,395	1979	Harry Lewis Nelson & David Slowinski
28	$M_{86,243}$	25,962	1982	David Slowinski
29	$M_{110,503}$	33,265	1988	Walter Colquitt & Luke Welsh
30	$M_{132,049}$	39,751	1983	David Slowinski
31	$M_{216,091}$	60,050	1985	David Slowinski
32	$M_{756,839}$	227,832	1992	David Slowinski & Paul Gage
33	$M_{859,433}$	258,716	1994	David Slowinski & Paul Gage
34	$M_{1,257,787}$	378,632	1996	David Slowinski & Paul Gage
35	$M_{1,398,269}$	420,921	1996	Joel Armengaud / GIMPS
36	$M_{2,976,221}$	895,932	1997	Gordon Spence / GIMPS
37	$M_{3,021,377}$	909,526	1998	Roland Clarkson / GIMPS
38	$M_{6,972,593}$	2,098,960	1999	Nayan Hajratwala / GIMPS
39	$M_{13,466,917}$	4,053,946	2001	Michael Cameron / GIMPS
40	$M_{20,996,011}$	6,320,430	2003	Michael Shafer / GIMPS
41	$M_{24,036,583}$	7,235,733	2004	Josh Findley / GIMPS
42	$M_{25,964,951}$	7,816,230	2005	Martin Nowak / GIMPS
43	$M_{30,402,457}$	9,152,052	2005	Curtis Cooper & Steven Boone / GIMPS
44	$M_{32,582,657}$	9,808,358	2006	Curtis Cooper & Steven Boone / GIMPS
45	$M_{37,156,667}$	11,185,272	2008	Hans-Michael Elvenich / GIMPS
46	$M_{42,643,801}$	12,837,064	2009	Odd M. Strindmo / GIMPS
47	$M_{43,112,609}$	12,978,189	2008	Edson Smith / GIMPS
48	$M_{57,885,161}$	17,425,170	2013	Curtis Cooper / GIMPS
49*	$M_{74,207,281}$	22,338,618	2016	Curtis Cooper / GIMPS
50*	$M_{77,232,917}$	23,249,425	2017	Jon Pace / GIMPS
51*	$M_{82,589,933}$	24,862,048	2018	Patrick Laroche / GIMPS
52*	$M_{136,279,841}$	41,024,320	2024	Luke Durant / GIMPS

References

[1] Agrawal, M., Kayal, N. and Saxena, N., "PRIMES is in P", *Annals of Mathematics*, vol. 160, no. 2, pp. 781–793, 2004.

[2] Andersson, H. and Djehiche, B., *An Introduction to Martingale Theory*. Stockholm: Department of Mathematics, 1997.

[3] Bateman, P. T., Selfridge, J. L. and Wagstaff, S. S. Jr., "The Editor's Corner: The New Mersenne Conjecture", *The American Mathematical Monthly*, vol. 96, no. 2, pp. 125–128, 1989.

[4] Biggs, N. L., *Discrete Mathematics*, 2nd ed. Oxford: Oxford University Press, 2003.

[5] Bruce, J. W., "A Really Trivial Proof of the Lucas–Lehmer Test", *The American Mathematical Monthly*, vol. 100, no. 4, pp. 370–371, 1993.

[6] Burton, D. M., *Elementary Number Theory*, 7th ed. New York: McGraw-Hill, 2011.

[7] Caldwell, C. "Mersenne Primes: History, Theorems and Lists." (2021), [Online]. Available: `https://t5k.org/mersenne/` (visited on 01/09/2024).

[8] Caldwell, C. "The New Mersenne Prime Conjecture." (2021), [Online]. Available: `https://t5k.org/mersenne/NewMersenneConjecture.html` (visited on 21/09/2024).

[9] Catalan, E., *Nouvelle Correspondance Mathématique*. Brussels: Royal Academy of Belgium, 1876, vol. 2.

[10] Crandall, R., Dilcher, K. and Pomerance, C., "A Search for Wieferich and Wilson Primes", *Mathematics of Computation*, vol. 66, no. 217, pp. 433–449, 1997.

[11] Edington, W. "Mersenne Number Proofs." (2014), [Online]. Available: `https://web.archive.org/web/20141014102940/http://www.garlic.com/~wedgingt/mersenne.html` (visited on 27/08/2024).

[12] Egusquiza Castillo, L., *The Discrete Fourier Transform: Some Properties and Applications*. Stockholm: Department of Mathematics, 2024.

[13] Euclid, *Elements, Book IX*, Translated by Heath, Sir T. L. and published in *Euclid's Elements*. Santa Fe: Green Lion Press, pp. 211–236, 2017.

[14] Euler, L., "De numeris amicibilibus", *Commentationes arithmeticae*, vol. 2, pp. 627–636, 1849.

[15] Gillies, D. B., "Three New Mersenne Primes and a Statistical Theory", *Mathematics of Computation*, vol. 18, no. 85, pp. 93–97, 1964.

[16] Good, I. J., "Conjectures Concerning the Mersenne Numbers", *Mathematics of Computation*, vol. 9, no. 51, pp. 120–121, 1955.

[17] Great Internet Mersenne Prime Search. "GIMPS Milestones Report." (2024), [Online]. Available: `https://www.mersenne.org/report_milestones/` (visited on 20/11/2024).

[18] Great Internet Mersenne Prime Search. "List of Known Mersenne Prime Numbers." (2024), [Online]. Available: `https://www.mersenne.org/primes/` (visited on 21/10/2024).

[19] Ivory, J., "Demonstration of a Theorem Respecting Prime Numbers", *New Series of the Mathematical Repository*, vol. 1, no. 2, pp. 6–8, 1806.

[20] James, G., Witten, D., Hastie, T. and Tibshirani, R., *An Introduction to Statistical Learning*, 2nd ed. New York: Springer, 2021.

[21] Levenius, L. G. (Ed.) "M136279841." (2024), [Online]. Available: `https://www.dropbox.com/scl/fi/08ppv42gzb0nq4matws9q/M136279841.pdf?rlkey=bw0h40vlix5e6rq7mb4mw2u4h&st=3p83f8fd&dl=0` (visited on 26/10/2024).

[22] Ligh, S. and Neal, L., "A Note on Mersenne Numbers", *Mathematics Magazine*, vol. 47, no. 4, pp. 231–233, 1974.

[23] Mahoney, M. S., *The Mathematical Career of Pierre de Fermat*, 2nd ed. Princeton: Princeton University Press, 1994.

[24] Mersenne, M., *Cogitata Physico Mathematica*. Paris: Præfatio Generalis, 1644.

[25] "New Mersenne Conjecture." (2021), [Online]. Available: `http://www.hoegge.dk/mersenne/NMC.html#unknown` (visited on 21/09/2024).

[26] Ochem, P. and Rao, M., "Odd Perfect Numbers are Greater than 10^{1500}", *Mathematics of Computation*, vol. 81, no. 279, pp. 1869–1877, 2012.

[27] Ribenboim, P., *The New Book of Prime Number Records*, 3rd ed. New York: Springer, 1996.

[28] Rödseth, Ö. J., "A Note on Primality Tests for $N = h \cdot 2^n - 1$", *BIT Numerical Mathematics*, vol. 34, no. 3, pp. 451–454, 1994.

[29] Wagstaff, S. S. Jr., "Divisors of Mersenne Numbers", *Mathematics of Computation*, vol. 40, no. 161, pp. 385–397, 1983.

[30] Wikipedia. "Mersenne prime." (2024), [Online]. Available: `https://en.wikipedia.org/wiki/Mersenne_prime` (visited on 15/09/2024).

[31] Williams, H. C. and Shallit, J. O., "Factoring Integers Before Computers", *Proceedings of Symposia in Applied Mathematics*, vol. 48, pp. 481–531, 1994.

Corrigendum for *Mersenne Primes and the Quest to Find Them*

Leo G. Levenius

1st December 2024

Incomplete Proof of Theorem 3.8

On page 10, the proof of Equation (3.2) is only presented for prime divisors, while no such restriction is made in the theorem. For the proof to be thorough, the following must be added.

Proof of Theorem 3.8 (continuation). In order to show that (3.2) holds for $\delta \in \mathbb{P}^c$, let $\delta = \delta_1\delta_2$ where $\delta_1, \delta_2 \in \mathbb{P}_{\geq 7}$ (iterate if there are more prime factors). Assuming that δ divides M_n, it thus follows that $\delta_1 \mid M_n$ and $\delta_2 \mid M_n$. Then, we know

$$\delta_1 = 2nk_1 + 1 \quad \text{and} \quad \delta_2 = 2nk_2 + 1,$$

where $k_i \equiv 0$ or $k_i \equiv -n \pmod 4$ for $i \in \{1, 2\}$. Therefore,

$$\delta = \delta_1\delta_2 = (2nk_1 + 1)(2nk_2 + 1) = 4n^2k_1k_2 + 2nk_1 + 2nk_2 + 1 = 2n(2nk_1k_2 + k_1 + k_2) + 1.$$

Now, let $k = 2nk_1k_2 + k_1 + k_2$ and we get the sought after formula. To show that k fulfils the desired condition, we need to consider a few scenarios: If $k_1 \equiv k_2 \equiv 0 \pmod 4$ we trivially get $k \equiv 0 \pmod 4$. If $k_i \equiv 0$ and $k_j \equiv -n \pmod 4$ for $i, j \in \{1, 2\}$ where $i \neq j$, then $k \equiv -n \pmod 4$. For the final case $k_1 \equiv k_2 \equiv -n \pmod 4$, observe that n is odd and therefore $n = 2m + 1$ for some $m \in \mathbb{Z}_{\geq 1}$. Hence,

$$k = 2nk_1k_2 + k_1 + k_2 \equiv 2n^3 - 2n = 2n(n + 1)(n - 1) = 4(2m + 1)(2m + 2)m \equiv 0 \pmod 4.$$

Thus, $k \equiv 0$ or $k \equiv -n \pmod 4$ and we are done. □