The Lucas-Lehmer primality test

Anna Carolina Eichholz, 12206819

Innsbruck, Februar 2025

Masterarbeit

eingereicht an der Universität Innsbruck, Fakultät für Mathematik, Informatik und Physik zur Erlangung des akademischen Grades

Diplom-Ingenieurin/Diplom-Ingenieur (Dipl.-Ing./DI)

Masterstudium Mathematik

Betreuer*in:
Tobias Fritz
Fakultät für Mathematik

Contents

1 Introduction

The greatest known prime number today is a Mersenne prime number, that has been discovered with the help of the Lucas-Lehmer test, which is the subject of this master thesis. It is stated as follows:

Theorem 1.1 (Lucas-Lehmer-Test)**.** *Define the following sequence of numbers:*

$$S_1 = 4; \qquad S_k = S_{k-1}^2 - 2.$$

Then, for $p > 2$ prime, the following statements are equivalent:

1. *The Mersenne number $M_p = 2^p - 1$ is prime.*
2. *$M_p \mid S_{p-1}$.*

Let us start with a little remark. Looking at the test one recognises that we exclude $p = 2$. Although $M_2 = 3$ is obviously the smallest Mersenne prime it does not satisfy the Lucas-Lehmer test. We use several methods to prove the theorems and lemmas that do only work for odd primes. Therefore $p = 2$ is always excluded in the proofs of this master thesis.
The Lucas-Lehmer test is a really useful tool to determine wether a Mersenne number is prime or not. It seems really out of the blue, that we can test, if a number is prime, by testing if it divides another number. The goal is to get a better understanding of the test and its proofs. In order to get there we'll have a close look at several proofs of this theorem and later compare them. We will consider a rather long but elementary proof and afterwards different proofs that need some knowledge of algebraic number theory. Further we will present the GIMPS project, which found the latest Mersenne primes.
To get a first understanding of what we are dealing with, we define Mersenne numbers and perfect numbers and state their connection:

Definition 1.2. *A perfect number is an integer where the sum of all divisors (excluding itself) gives the number itself. So two easy examples are:*

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14.$$

Definition 1.3. *Let $p \in \mathbb{N}$ be a prime number. A Mersenne number is a number of the form:*

$$M_p = 2^p - 1.$$

It is called a Mersenne prime, if M_p is prime.

The next theorem, which we are going to state without a proof (for the proof we refer to [Sie88]), gives us a reason why we should be interested in Mersenne primes.

Theorem 1.4. *For an even number P to be perfect it is necessary and sufficicient, that $P = 2^{s-1}(2^s - 1)$ where $s \in \mathbb{N}$ and $2^s - 1$ is prime and therefore a Mersenne prime. In order for $2^s - 1$ to be prime, s has to be prime too.*

The following text can be understood by all people that have a basic knowledge in mathematics and especially in number theory and algebraic number theory. All number theoretical aspects that will be needed are stated and a reference for a proof is given.

2 Basics in number theory

As we will do a lot of modulo calculation in the next chapters we will often consider $M_p \pmod 2$ or $\pmod 3$. It is clear that $M_p \equiv 1 \pmod 2$. For the second one we need to do a little calculation:

Lemma 2.1. *For $l > 2$ odd it holds that*

$$M_l \equiv 1 \pmod 3,$$

where $M_l = 2^l - 1$ is a Mersenne number for l prime.

Proof. We can prove this fact by induction. First let $l = 3$. Then $M_3 = 7 \equiv 1$ mod 3. Suppose it holds for M_l. We show that it also holds for M_{l+2}.

$$M_{l+2} = 2^{l+2} - 1 = 4 \cdot 2^l - 1 \equiv 1 \cdot 2^l - 1 \equiv M_l \equiv 1 \pmod 3 \quad \square$$

The modulo calculation has a lot of properties that simplify its use. One that we will need later is the following, where one can find a proof in [A$^+$17]:

Lemma 2.2. *Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. When we have $a \equiv b \pmod m$ and $a \equiv b \pmod n$ then also $a \equiv b \pmod{lcm(m, n)}$, where lcm stands for the least common multiple.*

Let us now introduce the definition of two integers being coprime, that we will use afterwards.

Definition 2.3. *Two integers are said to be coprime, if the only positive integer, that divides them both is* 1.

In the following chapters we will make use of Fermat's little theorem, which we will therefore state here. One can find a proof in [SW24] on page 87.

Theorem 2.4 (Fermat)**.** *Let p be prime and $a \in \mathbb{Z}$ coprime to p. Then we have*

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

Further we will use Lagranges theorem of which one can find a proof in [KM21].

Lemma 2.5 (Lagrange)**.** *Let G be a finite group and $|G| = g$. Then the order of an element of G is at most g and further divides g.*

On another note we will deal with algebraic integers, which are defined in the following way:

Definition 2.6. *An algebraic number is a root of a polynomial in one variable with integer coefficients. An algebraic number which is a zero of a monic polynomial $f \in \mathbb{Z}[x]$ is called algebraic integer. Together they form the ring of algebraic integers R.*

In the following we will sometimes adapt the modulus calculation in $\mathbb{Z}$ to the ring of algebraic integers R. For $r, s \in R$ and $q \in \mathbb{N}$ we define modulo as follows:

$$r \equiv s \pmod{q} \Leftrightarrow r = s + kq \text{ for some } k \in R.$$

In fact for $r, s \in \mathbb{Z}$ this definition is equivalent to the one we already know for integers:

Theorem 2.7. *For $s, t \in \mathbb{Z}$ the following two statements are equivalent:*

1. $r \equiv s \pmod{q}$ *in* R.
2. $r \equiv s \pmod{q}$ *in* $\mathbb{Z}$.

Proof. 2. ⇒1. follows directly as we can injectively embed $\mathbb{Z}$ in the ring of algebraic integers.
For the other implication suppose $r \equiv s \pmod{q}$ holds in R. According to the definition we can find $k \in R$ such that $r = s + kq$. As $s, t, q \in \mathbb{Z}$ the only possiblity is for k to be in $\mathbb{Z}$ aswell and as a consequence $r \equiv s \pmod{q}$ holds in $\mathbb{Z}$ too. □

3 Quadratic residues

In order to show the Lucas-Lehmer test we will need the Legendre symbol, which we introduce in this chapter. To calculate it, a helpful tool is the quadratic reciprocity law, where one can find a proof in this chapter aswell. Further we will introduce the Jacobi symbol.

3.1 Legendre symbol

The Legendre symbol is a very important tool in number theory, that we will use in our proofs and will therefore define in this subsection. For the whole subsection we follow chapter 8 in [SW24], where one can also find the missing proofs.

Definition 3.1. *Let p be prime. a is a **quadratic residue** $\pmod p$ if there exists $x \in \mathbb{N}$ such that*

$$x^2 \equiv a \pmod p.$$

*If such x does not exist, a is a **quadratic-non-residue**.*

Definition 3.2. *The **Legendre symbol** tells us if a number is a quadratic residue $\pmod p$: For a coprime to p and p prime and odd we define:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue} \pmod p \\ -1, & \text{if } a \text{ is a non-quadratic residue} \pmod p. \end{cases}$$

There exist a lot of helpful lemmas to make calculating with the Legendre symbol easier. We will state the ones we will make use of:

Lemma 3.3. *Let $p > 2$ be a prime number and $a, b \in \mathbb{Z}$. Then:*

1. *If $a \equiv b \pmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Lemma 3.4. *Let $p > 2$ be prime and $a \in \mathbb{Z}$, then it holds that*

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

Lemma 3.5. *Let $p > 3$ be prime. Then the following holds:*

1. *$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$ and $\left(\frac{2}{p}\right) = -1 \Leftrightarrow p \equiv \pm 3 \pmod 8$.*

2. $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$ *and* $\left(\frac{-1}{p}\right) = -1 \Leftrightarrow p \equiv 3 \pmod 4$.

3. $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3$ *and* $\left(\frac{-3}{p}\right) = -1 \Leftrightarrow p \equiv 2 \pmod 3$.

Proof. We will only show the third part, as one can find really simple proofs of the other two in many books, for example the one we refered to at the start of the chapter. This proof follows the algebraic number theory lecture I had at the university of Cantabria in Spain.
For the proof, we need the following theorem:

Theorem 3.6. *Let $a, b, c \in \mathbb{Z}$ and $p > 2$ be a prime number, such that $p \nmid a$. Then*

$$ax^2 + bx + c \equiv 0 \pmod p$$

has $1 + \left(\frac{\delta}{p}\right)$ solutions $\pmod p$, where $\delta = b^2 - 4ac$.

Proof. To begin, we multiply the equation by $4a$ which is $\not\equiv 0 \pmod p$ because $p \nmid a$ and $4 \not\equiv 0 \pmod p$.

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p.$$

By adding and substracting b^2 and rearranging the sumands we obtain

$$(2ax + b)^2 \equiv b^2 - 4ac = \delta \pmod p.$$

Rewriting the last equation we obtain that the quadratic formula holds $\pmod p$ as we know it:

$$x \equiv \frac{-b \pm \sqrt{\delta}}{2a} \pmod p.$$

This can only have two integer solutions if δ is a square modulo p so just if $\left(\frac{\delta}{p}\right) = 1$. Obviously the equation has 1 solution if $\delta = 0$ or $\left(\frac{\delta}{p}\right) = 0$. □

Now we can prove the last part of the lemma.
By the theorem above $\left(\frac{-3}{p}\right) = 1$ is equivalent to

$$x^2 + x + 1 \equiv 0 \pmod p$$

having two solutions, as $\delta = 1 - 4 = -3$. Everything we will mention below is equivalent to these first statements. As 1 is no solution of the equation above by $p > 3$, the following equation has three solutions.

$$(x - 1)(x^2 + x + 1) \equiv 0 \pmod p.$$

This is just

$$x^3 - 1 \equiv 0 \pmod{p}.$$

Which again is equivalent to $x^3 \equiv 1 \pmod{p}$ having three solutions. As $x^{p-1} \equiv 1 \pmod{p}$ by Fermats little theorem 2.4, we should get

$$3 \mid p - 1$$

and that is just equivalent to

$$p \equiv 1 \pmod{3},$$

which we wanted to show. □

Because we will use it several times, we will show that 3 is always a quadratic-non-residue $\pmod{M_p}$:

Lemma 3.7. *Let M_p be a Mersenne prime. Then*

$$\left(\frac{3}{M_p}\right) = -1.$$

Proof. In order to use lemma 3.5 we convince ourselves of

$$M_p \equiv 3 \pmod{4} \text{ and } M_p \equiv 1 \pmod{3}$$

by lemma 2.1. The first congruence follows just by the definition of M_p. By lemma 3.3 we have

$$\left(\frac{3}{M_p}\right) = \left(\frac{-3}{M_p}\right)\left(\frac{-1}{M_p}\right) = 1 \cdot (-1) = -1.$$

We thus have proven that 3 is a quadratic non-residue modulo a Mersenne prime. □

The next lemma tells us that for an odd prime p there exist the same number of quadratic residues modulo p as quadratic non residues. One can find a proof in [SW24].

Lemma 3.8. *For $p > 2$ prime and $a \in \mathbb{Z}/p\mathbb{Z}$, $\left(\frac{a}{p}\right) = 1$ for exactly $\frac{p-1}{2}$ different a and the same is true for $\left(\frac{a}{p}\right) = -1$.*

3.2 The quadratic reciprocity law

In this subsection we will state the quadratic reciprocity law and also prove it. Therefore we will use the method of Gauss sums. As a reference take [Saw17].

Theorem 3.9 (quadratic reciprocity law)**.** *Let $p, q > 2$ be two different prime numbers, then the following holds:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

In this whole chapter p and q will be different odd primes.
Let's start with some preparations for the proof. First we define Gauss sums:

Definition 3.10. *For $a \in \mathbb{Z}$ we define the Gauss sum of a as*

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \left(e^{\frac{2\pi i}{p}}\right)^{aj}.$$

As a next step we show the following lemma:

Lemma 3.11. *We have $g_a = \left(\frac{a}{p}\right) g_1$.*

Proof. First suppose $a \equiv 0 \pmod{p}$. Then the second factor in the Gauss sum $\left(e^{\frac{2\pi i}{p}}\right)^{aj}$ is always 1. Therefore we have

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0.$$

The last equality holds because $\left(\frac{0}{p}\right) = 0$ and by lemma 3.8 we have the same number of 1's and -1's in the sum. On the other hand we also have $\left(\frac{a}{p}\right) g_1 = 0$ as $a \equiv 0 \pmod{p}$.
Now let $a \not\equiv 0 \pmod{p}$. Then we have

$$\left(\frac{a}{p}\right) g_a = \sum_{j=0}^{p-1} \left(\frac{aj}{p}\right) \left(e^{\frac{2\pi i}{p}}\right)^{aj} = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \left(e^{\frac{2\pi i}{p}}\right)^{k} = g_1.$$

We obtain the desired result by multiplying both sides with $\left(\frac{a}{p}\right)$. □

For the next lemma, we define the delta function:

Definition 3.12. *Let $x, y \in \mathbb{Z}$. For $p \in \mathbb{N}$ we define the delta function as follows:*

$$\delta_p(x,y) := \begin{cases} 1 \text{ if } x \equiv y \pmod p \\ 0 \text{ if } x \not\equiv y \pmod p. \end{cases}$$

Lemma 3.13. *We have*

$$\sum_{a=0}^{p-1} \left(e^{\frac{2\pi i}{p}}\right)^{a(x-y)} = p \cdot \delta_p(x,y).$$

Proof. For $x - y \equiv 0 \pmod p$ we have that $\left(e^{\frac{2\pi i}{p}}\right)^{a(x-y)} = 1$ for every a.

Now let $x - y \not\equiv 0 \pmod p$ then $\left(e^{\frac{2\pi i}{p}}\right)^{(x-y)} \neq 1$ and

$$\sum_{a=0}^{p-1} \left(e^{\frac{2\pi i}{p}}\right)^{a(x-y)} = \frac{\left(e^{\frac{2\pi i}{p}}\right)^{ap} - 1}{\left(e^{\frac{2\pi i}{p}}\right)^{a} - 1} = 0.$$

For the second last equality we used the following formula: Let $n \in \mathbb{N}$ and $x \in \mathbb{R}$ then

$$x^n - 1 = (x-1)(x^0 + x^1 + ... + x^{n-1}).$$

□

Lemma 3.14. *We have $g_1^2 = (-1)^{\frac{p-1}{2}} \cdot p$.*

Proof. To show the lemma, we will present two different ways of calculating $\sum_{a=0}^{p-1} g_a g_{-a}$. Making use of lemma 3.11 we obtain

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g_1^2 = \sum_{a=0}^{p-1} \left(\frac{a^2}{p}\right)\left(\frac{-1}{p}\right) g_1^2 = (p-1)\left(\frac{-1}{p}\right) g_1^2.$$

On the other hand we have

$$\begin{aligned} \sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{a=0}^{p-1} \left(\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \left(e^{\frac{2\pi i}{p}}\right)^{ax} \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \left(e^{\frac{2\pi i}{p}}\right)^{-ay} \right) \\ &= \sum_{a=0}^{p-1} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \left(e^{\frac{2\pi i}{p}}\right)^{a(x-y)} \\ &= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) p \cdot \delta(x,y) \\ &= \sum_{x=0}^{p-1} p \left(\frac{x^2}{p}\right) = (p-1)p. \end{aligned}$$

In the middle we used lemma 3.13.
Combining both we have

$$(p-1)p = (p-1)\left(\frac{-1}{p}\right) g_1^2$$

which leads to the statement we wanted to show by multiplying both sides by $\frac{1}{p-1}\left(\frac{-1}{p}\right)$. □

The next two lemmas use the modulo calculation in the ring of algebraic integers as explained in the last chapter.

Lemma 3.15. *We have* $g_1^q \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\cdot g_1 \pmod{q}$.

Proof. We use lemma 3.14 to get

$$\begin{aligned} g_1^q &= g_1^{q-1}\cdot g_1 = (g_1^2)^{\frac{q-1}{2}}\cdot g_1 = ((-1)^{\frac{p-1}{2}}\cdot p)^{\frac{q-1}{2}}\cdot g_1 \\ &\equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\cdot g_1 \pmod{q}. \end{aligned}$$

□

Lemma 3.16. *It holds that* $g_1^q = \left(\frac{q}{p}\right)\cdot g_1 \pmod{q}$.

Proof.

$$g_1^q = \left(\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(e^{\frac{2\pi i}{p}}\right)^j\right)^q \equiv \sum_{j=0}^{p-1}\left(\frac{j}{p}\right)^q\left(e^{\frac{2\pi i}{p}}\right)^{jq} \equiv g_q \equiv \left(\frac{q}{p}\right) g_1 \pmod{q}.$$

In the last step we used lemma 3.11. □

Now we have all the tools we need to prove the law of quadratic reciprocity:

Proof of the law of quadratic reciprocity. Combining lemma 3.15 and lemma 3.16 leads us to

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\cdot g_1 = \left(\frac{q}{p}\right)\cdot g_1.$$

In order to obtain the law of quadratic reciprocity we only have to multiply by $\left(\frac{p}{q}\right)$ and divide by g_1. By lemma 3.14 we know that $g_1^2 \neq 0$ and therefore also $g_1 \neq 0$. □

3.3 The Jacobi symbol

What if the denominator of the Legendre symbol is not prime? For this case we will introduce the Jacobi symbol, which unfortunately is not as helpful as the Legendre symbol. Why that is, we will discuss after having a look at the definition. For this subsection one might refer to chapter 8 in [SW24].

Definition 3.17. *Let $n > 2 \in \mathbb{N}$ be odd with prime factorization $n = p_1 \cdot \ldots \cdot p_k$. Then for every $a \in \mathbb{Z}$ the **Jacobi symbol** is defined as*

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_k}\right),$$

where $\left(\frac{a}{p_i}\right)$ are Legendre symbols.

Similar to the Legendre symbol, the Jacobi symbol has the following properties:

Lemma 3.18. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ odd. Then it holds that:*

1. *If $a \equiv b \pmod{n}$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*
2. *$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.*

As mentioned before one needs to pay attention with the Jacobi symbol, because it does not tell if a number is a quadratic residue $\pmod{n}$. Only if the Jacobi symbol equals to -1 we know that it is not a quadratic residue.

4 Elementary proof

Let us first discuss a proof for the correctness of the Lucas-Lehmer-Test, that only relies on very elementary facts. One can refer to this proof in [Sie88] in chapter 10.

Before we can start the proof, we will introduce some facts, which we will use in the proof afterwards.
We start by setting $a := 1 + \sqrt{3}$ and $\bar{a} := 1 - \sqrt{3}$. With this we define the following sequences:

$$u_n := \frac{a^n - \bar{a}^n}{a - \bar{a}} \text{ and } v_n := a^n + \bar{a}^n.$$

We state some equations for these two sequences, that can easily be checked by calculating:

$$\begin{aligned}
2u_{k+l} &= u_k v_l + v_k u_l && (4.1)\\
(-2)^{l+1} u_{k-l} &= u_l v_k - u_k v_l \text{ for } k > l && (4.2)\\
u_{2k} &= u_k v_k && (4.3)\\
v_{2k} &= v_k^2 + (-2)^{k+1} && (4.4)\\
v_k^2 - 12u_k^2 &= (-2)^{k+2} && (4.5)\\
2v_{k+1} &= v_k v_1 + 12 u_k u_1. && (4.6)
\end{aligned}$$

Proof. We start with (4.1):

$$\begin{aligned}
u_k v_l + v_k u_l &= \frac{a^k - \bar{a}^k}{a - \bar{a}}(a^l + \bar{a}^l) + (a^k + \bar{a}^k)\frac{a^l - \bar{a}^l}{a - \bar{a}}\\
&= \frac{1}{a - \bar{a}}(a^{k+l} - \bar{a}^{k+l} - b^k a^l + a^k \bar{a}^l + a^{k+l} - \bar{a}^{k+l} + b^k a^l - a^k \bar{a}^l)\\
&= 2\frac{a^{k+l} - \bar{a}^{k+l}}{a - \bar{a}} = 2u_{k+l}.
\end{aligned}$$

Next we show (4.2):

$$\begin{aligned}
u_l v_k - u_k v_l &= \frac{1}{a - \bar{a}}(a^{k+l} - a^k \bar{a}^l + a^l \bar{a}^k - \bar{a}^{k+l} - a^{k+l} + a^l \bar{a}^k - a^k \bar{a}^l + \bar{a}^{k+l})\\
&= \frac{2}{a - \bar{a}}(a^l \bar{a}^k - a^k \bar{a}^l) = 2(a\bar{a})^l \frac{\bar{a}^{k-l} - a^{k-l}}{a - \bar{a}}\\
&= 2(-2)^l(-1)\frac{a^{k-l} - \bar{a}^{k-l}}{a - \bar{a}} = (-2)^{l+1} u_{k-l}.
\end{aligned}$$

The other statements are shown in a similar way and are therefore left to the reader. □

As a next step we will use the equations above to prove some lemmas, which we will use to prove the Lucas-Lehmer-test.

Lemma 4.1. *If we define $w(q)$ to be the smallest m (if it exists) such that $q|u_m$, then for $q > 2$ prime the following statements are equivalent:*

1. $q \mid u_n$.
2. $w(q) \mid n$.

Proof. We start by showing that 2.⇒1. holds. Suppose $w(q) \mid n$ and take $k \in \mathbb{N}$ such that $w(q) \cdot k = n$. On the other hand we know $q \mid u_{w(q)}$. Further we can inductively show that $q \mid u_{k \cdot w(q)}$. First by considering (4.1) with $k = l = w(q)$, we already now that q divides the right hand side, therefore $q \mid 2u_{2w(q)}$. As $q \nmid 2$ we have $q \mid u_{2w(q)}$. Next we apply (4.1) to $k = w(q)$ and $l = 2w(q)$ to obtain $q \mid 2u_{3w(q)}$. Again it follows that $q \mid u_{3w(q)}$ as $q \nmid 2$. We can repeat this procedure until we get the desired result.
Now for the other implication. Let $q \mid u_n$. Then obviously $n \geq w(q)$. Further there exists $t \geq 1$ and $0 \leq r < w(q)$ such that $n = tw(q)+r$. If we now define $S := \{m \in \mathbb{N} \text{ such that } q \mid u_m\}$, it is clear that $n, w(q) \in S$. For the first implication we already showed that $tw(q) \in S$ holds. We get $n - tw(q) \in S$ by aplying (4.2) with $k = n$ and $l = tw(q)$. But with what we were looking for we just have $r = n - tw(q) \in S$. Because $w(q)$ is the smallest element in S and $r < w(q)$ we have $r = 0$. This is equivalent to $w(q) \mid n$ which we wanted to show. □

The next lemmas give us a variety of multiples of a prime number. The lemmas build on each other and in the actual proof in the end we will arrive at a contradiction with the help of combined multiples of the prime number.

Lemma 4.2. *Let q be a prime number and $q \equiv 7 \pmod{12}$, then it holds that $q \mid (3^{\frac{q-1}{2}} + 1)$. As a special case, this holds for every Mersenne prime $q = M_p$, where $p > 2$ prime.*

Proof. By lemma 3.4 we have $3^{\frac{q-1}{2}} \equiv \left(\frac{3}{q}\right) \pmod{q}$ and we can make use of the Legendre symbol. First we notice that $q \equiv 1 \pmod 3$ and therefore by lemma 3.3 we have $\left(\frac{q}{3}\right) = \left(\frac{1}{3}\right) = 1$. On the other hand by theorem 3.9 we have $\left(\frac{3}{q}\right) = \left(\frac{q}{3}\right)\left(\frac{3}{q}\right) = -1$ because $q \equiv 3 \pmod 4$. As a consequence $3^{\frac{q-1}{2}} + 1 \equiv -1 + 1 \equiv 0 \pmod{q}$. We thus have shown the first part.
Special case: As $q \equiv -1 \equiv 7 \pmod 8$ and by lemma 2.1 $q \equiv 1 \equiv 7 \pmod 3$ also $q \equiv 7 \pmod{24}$ by theorem 2.2. □

Lemma 4.3. *Let $q > 3$ be a prime number. Then the following holds:*

1. $q \mid \left(u_q - 3^{\frac{q-1}{2}}\right)$.
2. $q \mid (v_q - 2)$.
3. *For $q = 2^p - 1$ a Mersenne prime it holds that $q \mid (v_{2^p} + 4)$.*

Proof. We start with the first statement.

$$\begin{aligned}
u_q &= \frac{1}{2\sqrt{3}}\left(\sum_{j=0}^{q}\binom{q}{j}\sqrt{3}^j - \sum_{j=0}^{n}\binom{q}{j}(-1)^j\sqrt{3}^j\right) \\
&= \frac{1}{2\sqrt{3}}\left(\sum_{j=1,2\nmid j}^{q}\binom{q}{j}2\sqrt{3}^j\right) = \sum_{j=1,2\nmid j}^{q}\binom{q}{j}3^{\frac{j-1}{2}} = \sum_{k=0}^{\frac{q-1}{2}}\binom{q}{2k+1}3^k \\
&= 3^{\frac{q-1}{2}} + \sum_{k=0}^{\frac{q-3}{2}}\binom{q}{2k+1}3^k
\end{aligned}$$

Now we can easily see that

$$u_q - 3^{\frac{q-1}{2}} = \sum_{k=0}^{\frac{q-3}{2}}\binom{q}{2k+1}3^k \equiv 0 \pmod q.$$

For the second part we have

$$v_q = \sum_{j=0,2\mid j}^{q}\binom{q}{j}2\sqrt{3}^j = 2\sum_{k=0}^{\frac{q-1}{2}}\binom{q}{2k}3^k = 2 + \sum_{k=1}^{\frac{q-1}{2}}\binom{q}{2k}3^k.$$

Again, it is easy to see that $v_q - 2 \equiv 0 \pmod q$.
For the last part we have

$$2v_{2^p} = 2v_{q+1} = v_q v_1 + 12u_q u_1 = 2v_q + 12u_q$$

by (4.6). We can rewrite this as

$$v_{2^p} = v_q + 6u_q = v_q - 2 + 6(u_q + 1) - 4$$

or equivalently

$$v_{2^p} + 4 = v_q - 2 + 6(u_q + 1). \tag{4.7}$$

We use lemma 4.2 and the first part of the lemma for

$$q \mid ((u_q - 3^{\frac{q-1}{2}}) + (3^{\frac{q-1}{2}} + 1)) = u_q + 1.$$

By the last result and the second part of the lemma we have

$$q \mid (v_q - 2 + 6(u_q + 1))$$

and by (4.7) we get

$$q \mid (v_{2^p} + 4). \qquad \Box$$

Lemma 4.4. *Let $q > 3$ be a Mersenne prime number then $w(q) \leq q + 1$.*

Proof. As $u_1 = 1$ and $v_1 = 2$ we use (4.1) and (4.2) to obtain

$$2u_{q+1} = u_q v_1 + u_1 v_q = 2u_q + v_q$$

and

$$-4u_{q-1} = u_q v_1 - u_1 v_q = 2u_q - v_q.$$

If we multiply both equations together, we obtain

$$-8u_{q+1}u_{q-1} = 4u_q^2 - v_q^2.$$

On the other hand by Fermat's little theorem 2.4 we have $3^{q-1} \equiv 1 \pmod{q}$ which is equivalent to

$$q \mid (3^{q-1} - 1). \tag{4.8}$$

By lemma 4.3 we obtain

$$q \mid (u_q^2 - 3^{q-1}) \text{ and } q \mid (v_q^2 - 4). \tag{4.9}$$

If we now combine (4.8) and (4.9) we get

$$q \mid (u_q^2 - 3^{q-1} + 3^{q-1} - 1) = u_q^2 - 1,$$

$$q \mid (4(u_q^2 - 1) - (v_q^2 - 4)) = 4u_q^2 - v_q^2 = -8u_{q+1}u_{q-1}.$$

The last equalitiy is just what we showed at the start of the proof. From this we conclude, that q has to divide u_{q+1} or u_{q-1} and therefore we have shown that $w(q) \leq q + 1$. □

A tool that is very common in the proofs of the Lucas-Lehmer test is to express the sequence S_n by some other sequence. The next lemma gives us such an expression and we will see others in later chapters.

Lemma 4.5. $2^{2^{k-1}}S_k = v_{2^k}$, *where* S_k *is the sequence, we defined in the Lucas-Lehmer test.*

Proof. We show it by induction. For $k = 1$ we have $2S_1 = 8 = v_2$. Next we calculate:

$$2^{2^k}S_{k+1} = 2^{2^k}S_k^2 - 2^{2^k+1} = (2^{2^{k-1}}S_k)^2 - 2^{2^k+1} \overset{induction}{=} v_{2^k}^2 + (-2)^{2^k+1} = v_{2^{k+1}},$$

where we have used (4.4) in the last equation. □

Theorem 4.6. *Let* $q = 7 \pmod 8$ *be a prime number. Then*

$$q \mid M_{\frac{q-1}{2}}.$$

Note: This theorem holds for all Mersenne prime numbers, where $p > 2$.

Proof. This is a direct consequence of lemma 3.4 and 3.5 because it holds that $M_{\frac{q-1}{2}} = 2^{\frac{q-1}{2}} - 1 \equiv \left(\frac{2}{q}\right) - 1 = 0 \pmod q$. □

Now that we have done all the preliminary work we will prove the Lucas-Lehmer test.

Proof. For the first implication we suppose $M_p \mid S_{p-1}$ and the goal is to show that M_p is prime.
Suppose M_p is not prime and there exists a prime divisor q of M_p. $q > 3$ because $2, 3 \nmid M_p$. The first one is obvious and the second we have shown in lemma 2.1.
By lemma 4.5 we know $M_p \mid v_{2^{p-1}}$ and also

$$M_p \mid u_{2^p} = u_{2^{p-1}}v_{2^{p-1}}$$

because of (4.3). Using lemma 4.1, we obtain $w(q) \mid 2^p$. Suppose $w(q) \mid 2^{p-1}$. Again by lemma 4.1 we would have $q \mid u_{2^{p-1}}$. Combining different multiples of q leads us to

$$q \mid (v_{2^{p-1}}^2 - 12u_{2^{p-1}}^2) = 2^{2^{p-1}+2},$$

where the last equality follows by (4.5). This is a contradiction, because $q \neq 2$. Therefore we have shown that $w(q) = 2^p$. If we combine this with lemma 4.4 we obtain

$$M_p = 2^p - 1 = w(q) - 1 \leq q + 1 - 1 = q,$$

which shows that M_p must be prime.
Now for the other implication. Suppose M_p is prime. Take $q := M_p = 2^p - 1$, where $p > 2$ is prime. By theorem 4.6 we know

$$q \mid M_{\frac{2^p-1-1}{2}} = 2^{2^{p-1}-1} - 1. \tag{4.10}$$

Next we use (4.4) to obtain

$$v_{2^p} = v_{2^{p-1}}^2 - 4 \cdot 2^{2^{p-1}-1}$$

and also

$$v_{2^p} - v_{2^{p-1}}^2 + 4 = -4(2^{2^{p-1}-1} - 1).$$

Combining this formula and (4.10) gives us

$$q \mid (v_{2^p} - v_{2^{p-1}}^2 + 4).$$

By this and part three of lemma 4.3 we can see that

$$q \mid v_{2^{p-1}}^2$$

must hold. We can get rid of the square, because q is prime. To conclude we use lemma 4.5, that states $v_{2^{p-1}} = 2^{2^{p-2}} S_{p-1}$. As $q > 2$ and prime, we can see now that $q = M_p \mid S_{p-1}$. □

5 Recap of algebraic number theory

For the next proofs we need some properties of algebraic number theory, which we will treat in this chapter.
A really handy tool is the Chinese remainder theorem. As a reference for the proof please refer to chapter 6 in [Bax22].

Theorem 5.1 (Chinese remainder theorem)**.** *Let R be a commutative ring with identity element. Let $I_1, ..., I_n$ be pairwise coprime ideals of R. Then*

$$R/(I_1...I_n) \simeq R/(I_1) \times \cdots \times R/(I_n).$$

Next we talk about how a prime number can be factorized in $\mathbb{Z}[\sqrt{w}]$ (a reference for the definiton and theorem is [Sch07]). For simplification we will restrict ourselves to the cases $w \equiv 2, 3 \pmod 4$.

Definition 5.2. *Let $p \in \mathbb{Z}$ be prime. Take $w \in \mathbb{Z}$ squarefree and further $w \equiv 2, 3 \pmod 4$. Let $(p) := p\mathbb{Z}[\sqrt{w}]$ be the ideal generated by p in $\mathbb{Z}[\sqrt{w}]$, then we say that*

1. *p ramifies in $\mathbb{Z}[\sqrt{w}]$ if and only if $(p) = P^2$ for P a prime ideal in $\mathbb{Z}[\sqrt{w}]$.*

2. *p splits in $\mathbb{Z}[\sqrt{w}]$ if and only if $(p) = P_1 \cdot P_2$ for P_1 and P_2 being different prime ideals in $\mathbb{Z}[\sqrt{w}]$.*

3. *p inerts in $\mathbb{Z}[\sqrt{w}]$ if and only if (p) is prime in $\mathbb{Z}[\sqrt{w}]$.*

In order to determine which case we have, the following theorem will help us:

Theorem 5.3. *As in the definition above we take $2 < p \in \mathbb{N}$ to be a prime and $w \in \mathbb{Z}$ be squarefree. Then the following holds:*

1. *p ramifies in $\mathbb{Z}[\sqrt{w}] \Leftrightarrow \left(\frac{w}{p}\right) = 0$.*

2. *p splits in $\mathbb{Z}[\sqrt{w}] \Leftrightarrow \left(\frac{w}{p}\right) = 1$.*

3. *p inerts in $\mathbb{Z}[\sqrt{w}] \Leftrightarrow \left(\frac{w}{p}\right) = -1$.*

6 Proofs using algebraic number theory

Over the years matematicians have found different aproaches to prove the correctness of the Lucas-Lehmer test. In this chapter we will have a look at some of them. The proofs by Rosen, Bruce and Rödseth appeared in a short period of time. They each tried to come up with an even more elegant method to prove the Lucas-Lehmer test. We will treat the proofs in the order of publication. Not totally cronological we will work on a paper by Tao, that gives an explanation of the ideas behind Bruce's and Rosen's proof.

6.1 Proof by Rosen

The first proof we are going to have a closer look at is the one that was published by Rosen in 1988 [Ros88]. To prepare the proof, we start by defining:

$$\tau = \frac{1+\sqrt{3}}{\sqrt{2}}\ ,\ \bar{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}\ ,\ \omega = \tau^2 = 2+\sqrt{3} \text{ and } \bar{\omega} = \bar{\tau}^2 = 2-\sqrt{3}.$$

Lemma 6.1. *Using the definitions above, we get the following alternative representation for the sequence S_k in the Lucas-Lehmer test:*

$$S_k = \omega^{2^{k-1}} + \bar{\omega}^{2^{k-1}}.$$

Proof. We can easily prove this by induction. Firstly

$$S_1 = 4 = 2+\sqrt{3}+2-\sqrt{3} = \omega + \bar{\omega}.$$

Next

$$S_{k+1} = S_k^2 - 2 = (\omega^{2^{k-1}} + \bar{\omega}^{2^{k-1}})^2 - 2 = \omega^{2^k} + \bar{\omega}^{2^k} + 2\omega^{2^{k-1}}\bar{\omega}^{2^{k-1}} - 2 = \omega^{2^k} + \bar{\omega}^{2^k},$$

where we used the fact, that obviously $\omega\bar{\omega} = 1$. □

The next lemma gives us a tool to show the second implication of the Lucas-Lehmer test.

Lemma 6.2. *If M_p is prime, then $\tau^{M_p+1} \equiv -1 \pmod{M_p}$.*

As explained in chapter 2 this congruence is understood to be in the ring of algebraic integers. Obviously $\sqrt{2}$ and $\sqrt{3}$ are algebraic integers. Also τ is an algebraic integer, because it is a zero of the polynom $x^4 - 4x^2 + 1$.

Proof.

$$\begin{aligned}\tau &= \frac{1+\sqrt{3}}{\sqrt{2}} \\ \tau\sqrt{2} &= 1+\sqrt{3} \\ (\tau\sqrt{2})^{M_p} &= (1+\sqrt{3})^{M_p}.\end{aligned}$$

In the next step we use our modified definition of modulus in order to cancel out every term that is a product of M_p, for example $M_p\sqrt{3}$.

$$\tau^{M_p} 2^{\frac{M_p-1}{2}}\sqrt{2} \equiv 1 + 3^{\frac{M_p-1}{2}}\sqrt{3} \pmod{M_p}.$$

In the last row we recognize two Legendre symbols using lemma 3.4:

$$\tau^{M_p}\left(\frac{2}{M_p}\right)\sqrt{2} \equiv 1 + \left(\frac{3}{M_p}\right)\sqrt{3} \pmod{M_p}.$$

As $M_p \equiv -1 \pmod 8$ and by aplying lemma 3.5 and lemma 3.7 we have

$$\tau^{M_p}\sqrt{2} \equiv 1 - \sqrt{3} \pmod{M_p}.$$

We can now divide by $\sqrt{2}$ as it is not a zero divisor to obtain $\bar{\tau}$ on the right side:

$$\tau^{M_p} \equiv \bar{\tau} \pmod{M_p}.$$

If we multiply both sides by τ we get the desired result:

$$\tau^{M_p+1} \equiv -1 \pmod{M_p}.$$

□

Now we have the tools we need for the proof of the Lucas-Lehmer test.

Proof. For the first implication suppose $S_{p-1} \equiv 0 \pmod{M_p}$ and the goal is to show that M_p is prime. By lemma 6.1

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}.$$

Rearranging the terms and multiplying both sides by $\omega^{2^{p-2}}$ leads us to

$$\omega^{2^{p-1}} \equiv -1 \pmod{M_p} \text{ and } \omega^{2^p} \equiv 1 \pmod{M_p}, \tag{6.1}$$

where we made use of the fact that $\omega\bar{\omega} = 1$.
Next suppose there exists a prime divisor q of M_p. We will be working in the

ring $O = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}$ such that $a, b \in \mathbb{Z}\}$. By (6.1) we see that the order of the coset of ω in $(O/qO)^*$ is 2^p. According to theorem 5.3 q either ramifies, splits or inerts in O. As $3 \nmid q$, q does not ramify. Now suppose q splits in O. Then we would have

$$(O/qO) = \mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}] = \mathbb{Z}[x]/(x^2 - 3, q) = \mathbb{F}_q[x]/(x^2 - 3),$$

where $\mathbb{F}_q$ is just another notation for $\mathbb{Z}/q\mathbb{Z}$.
As 3 is a square in $\mathbb{F}_p$ by theorem 5.3 we set $3 = a^2 \pmod{q}$ to get

$$\begin{aligned}(O/qO) &= \mathbb{F}_q[x]/(x^2 - 3) = \mathbb{F}_q[x]/(x^2 - a^2) = \mathbb{F}_q[x]/(x + a)(x - a)\\ &\simeq \mathbb{F}_q[x]/(x + a) \times \mathbb{F}_q[x]/(x - a) = \mathbb{F}_q \times \mathbb{F}_q\end{aligned}$$

by the Chinese remainder theorem 5.1. Further the same holds for the ring of units:

$$(O/qO)^* \simeq (\mathbb{Z}/q\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*.$$

As a consequence the order of the element ω in $(O/qO)^*$ divides the order of the group $(\mathbb{Z}/q\mathbb{Z})^*$ which on the other hand is equal to $q - 1$ by the last isomorphism. Speaking in a formula we have $2^p \mid q - 1$ by Lagranges theorem 2.5 or in other words $q = 1 + 2^p k$, $k \geq 1$. But this leads to a contradiction, as $q \geq 2^p + 1 > M_p$ is not possible.
Therefore q must inert and as a consequence be prime in O. Then (O/qO) is a field and $(O/qO)^*$ has $q^2 - 1$ elements and we have $2^p \mid q^2 - 1 = (q-1)(q+1)$. To conclude we look at two different cases. First suppose $q \equiv 1 \pmod{4}$. As $q + 1 \equiv 2 \pmod{4}$ this term can only provide one factor 2 and $q - 1$ has to provide the other $p - 1$, meaning $2^{p-1} \mid q - 1$. So there exists $k \in \mathbb{N}$ such that $q - 1 = k2^{p-1}$. As $2q \geq 2 + 2^p > M_p$, q cannot be a prime divisor of M_p.
In the second step we treat the case $q \equiv 3 \pmod{4}$. With the same explanation as in the first case, we obtain $2^{p-1} \mid q + 1$ or equivalently $q + 1 = k2^{p-1}$ for some $k \in \mathbb{N}$. $k \neq 1$ because $q = 2^{p-1} - 1 \mid M_p = 2^p - 1$ is not possible. So let $k = 2$. Then $q = 2^p - 1 = M_p$ and we have shown that M_p must be prime.
Now for the other implication. Let M_p be prime. The goal is to show that $M_p \mid S_{p-1}$. By lemma 6.2 we start with the fact that

$$\tau^{M_p+1} \equiv -1 \pmod{M_p}.$$

Or also:

$$\tau^{2^p} + 1 \equiv 0 \pmod{M_p}.$$

Because we chose τ such that $\tau^2 = \omega$ we have:

$$\omega^{2^{p-1}} + 1 \equiv 0 \pmod{M_p}.$$

In the next step we multiply both sides by $\bar{\omega}^{2^{p-2}}$ to obtain

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}.$$

The left hand side is just S_{p-1} by lemma 6.1 and we have thus proven the implication. □

6.2 Proof by Bruce

Not completely different, but simplifying the most technical part of Rosen's proof is the one that Bruce gives in 1993 [Bru93]. He only gives an alternative proof of the first implication and uses the same lemma to start with.

Proof of Lucas-Lehmer tests first implication. Suppose $M_p \mid S_{p-1}$. The goal is to show that M_p is prime. So with lemma 6.1

$$M_p \mid S_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}}.$$

Therefore

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}.$$

As a consequence there exists $R \in \mathbb{N}$ such that

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

Multiplying both sides by $\omega^{2^{p-2}}$ and using once again $\omega\bar{\omega} = 1$ we obtain

$$\omega^{2^{p-1}} = RM_p\omega^{2^{p-2}} - 1. \tag{6.2}$$

If we now assume that M_p is not prime, then there exists a prime divisor q with $q^2 \leq M_p$. Obviously $q \neq 2$.
Now for the group theory: We will use the following really trivial lemma:

Lemma 6.3. *Let O be a monoid (a set with an associative binary operation and an identity element). Then the set O^* of invertible elements in O forms a group.*

Define Z_q as the set of all integers modulo q and

$$O := \{a + b\sqrt{3} : a, b \in Z_q\}$$

with addition and multiplication. By lemma 6.3 O^*, all invertible elements of O with respect to multiplication, is a group. Because O has q^2 elements and 0 is not invertible, O^* has at most $q^2 - 1$ elements. Next, by lemma 2.5

the order of each element of O^* is at most $q^2 - 1$.
Looking at $\omega = 2 + \sqrt{3}$, it is an element of X. Further, as we assumed $q \mid M_p$ we have $M_p = 0$ in O. So in O the equation (6.2) becomes

$$\omega^{2^{p-1}} \equiv -1 \pmod{q}.$$

Squaring the equation we obtain

$$\omega^{2^p} \equiv 1 \pmod{q}.$$

Therefore the order of ω in O^* is 2^p. Using lemma 2.5 we get a contradiction:

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

We have shown that M_p must be prime. □

6.3 Explanation by Tao

After having worked through the last two proofs, the intuition of the authors might not be very clear. In his proof [Tao08], Tao explained how to get the idea to work in the ring $\mathbb{Z}[\sqrt{3}]$ and use the element $\omega = 2 + \sqrt{3}$ to prove the Lucas-Lehmer test.

Let us start by using Fermat's little theorem 2.4. Fermats little theorem gives us a necessary condition for a number to be prime. If we take any a coprime to n (usually for simplicity one uses $a = 2$ or $a = 3$) and we have $a^{n-1} \neq 1 \pmod{n}$ then n can't be prime. Note that the reverse is not true. For example $8^{9-1} = 1 \pmod{9}$ but 9 is obviously not prime.
As a "generalization" of Fermats little theorem, let's have a look at Euler's theorem. The proof can be found in [SW24] on page 91.

Theorem 6.4 (Euler)**.** *Let $n \in \mathbb{N}$ and a again coprime to n. Then*

$$a^{\phi(n)} = 1 \pmod{n},$$

where $\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$.

Combining Lagrange's lemma 2.5 and Fermat's little theorem gives us the following result:
If n is prime, then $ord_n(a) := ord_{(\mathbb{Z}/n\mathbb{Z})^*}(a) \mid n - 1$.
On the other hand we can deduce a strict inequality for n not prime by Euler's theorem: For n not prime we have $ord_n(a) < n - 1$.
So our new goal to show that n is prime, is to find a coprime to n such that

$ord_n(a) = n - 1$. When n is really large (around 10^{10^7}) it is extremely hard to calculate the order of an element, so we'll make use of the following trick: Suppose we can find a k and a a coprime to n such that

$$a^{2^k} = -1 \pmod n \text{ and } a^{2^{k+1}} = 1 \pmod n. \tag{6.3}$$

Then we would have $ord_n(a) = 2^{k+1}$. This is a lot easier to calculate, than having to consider every power of a. At first sight this only helps us to identify Fermat primes, so numbers of the form $2^k + 1$, but we will show in the next step how to use this.

Our goal is to show the following lemma, which is almost the Lucas-Lehmer test:

Lemma 6.5. *Let N be a Mersenne number. Then the two following statements are equivalent:*

1. *N is prime.*
2. *$(2+\sqrt{3})^{(\frac{N+1}{2})} = -1$ in $\mathbb{F}_N[\sqrt{3}]$.*

Proof. We did show 2. ⇒ 1. in the proof by Bruce.

Note that the proof of the first implication could be done a lot faster, but the goal of this proof is to explain how to arrive at the statement of the lemma. So let N be prime. We observe that $N+1 \mid N^2 - 1$. That is the reason we will be working in $\mathbb{F}^*_{N^2}$ which contains $N^2 - 1$ elements as N is prime. The goal now is to look at $\mathbb{F}_{N^2}$ as a quadratic extension so to speak $\mathbb{F}[\sqrt{k}]$. For them to be equivalent, k should be a quadratic-non-residue $\pmod N$. If we consider $k = 2$ obviously it is coprime to N, but 2 is a quadratic residue $\pmod N$, as we mentioned in lemma 3.5 that $(\frac{2}{N}) = 1$ for $N = -1 \pmod 8$, which is the case.

We now consider $k = 3$. k and N are again coprime and this time k is also a quadratic non-residue as we have shown in lemma 3.7.

So let's work in $\mathbb{F}_N[\sqrt{3}]$. In order to make use of (6.3) we are looking for an element of order $N+1$, which is a power of 2. So in a formula: Find a such that $a^{(N+1)/2} = -1$ in $\mathbb{F}_N[\sqrt{3}]$. To do so, let's start with an element of $\mathbb{F}_N[\sqrt{3}]$: $c + b\sqrt{3}$. We have $c^N = c$ in $\mathbb{F}_N[\sqrt{3}]$ by Fermats little theorem 2.4 and $(\sqrt{3})^N = -\sqrt{3}$ because

$$(\sqrt{3})^N = \sqrt{3} \cdot (\sqrt{3}^2)^{\frac{N-1}{2}} = \sqrt{3} \cdot 3^{\frac{N-1}{2}} = \sqrt{3} \cdot \left(\frac{3}{N}\right) = -\sqrt{3}.$$

In this calculation we used lemma 3.4 and lemma 3.7. As a result we have

$$(c + b\sqrt{3})^N = c - b\sqrt{3}.$$

Multiplying both sides by $c + b\sqrt{3}$ gives us

$$(c + b\sqrt{3})^{N+1} = c^2 - 3b^2.$$

We can now rewrite this as

$$(c^2 + 3b^2 + 2cb\sqrt{3})^{(\frac{N+1}{2})} = c^2 - 3b^2.$$

Choosing $c = b = 1$ we get

$$(4 + 2\sqrt{3})^{(\frac{N+1}{2})} = -2. \tag{6.4}$$

On the other hand as 2 is a quadratic residue $\pmod N$ we have

$$2^{\frac{N-1}{2}} = 1.$$

and equivalentely:

$$2^{\frac{N+1}{2}} = 2. \tag{6.5}$$

Dividing (6.4) by (6.5) let's us find the element we were looking for:

$$(2 + \sqrt{3})^{(\frac{N+1}{2})} = -1.$$

As a result we have shown the lemma. □

We have therefore shown a way to check, if a Mersenne number is prime, which we can easily connect to the form of the Lucas-Lehmer test we know. By lemma 6.1 our goal is to show that the following two statements are equivalent:

1. $(2 + \sqrt{3})^{(\frac{N+1}{2})} = -1$ in $\mathbb{F}_N[\sqrt{3}]$.
2. $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod N$.

This equivalency is easy to show. The proof are just the last few lines of the proof by Rosen.

6.4 Proof by Rödseth

Knowing the aproaches of Bruce and Rosen, Rödseth came up with a different idea of how to prove the Lucas-Lehmer test in 1994. In fact, he even showed a more general result, of which the Lucas-Lehmer test is just a special case [Rö94].

Theorem 6.6. *Let $n, h \in \mathbb{N}$ with h an odd number and further $0 < h < 2^{n+1} - 1$. Set $N = h \cdot 2^n - 1$. Further we take some $P \in \mathbb{N}$ such that*

$$\left(\frac{P-2}{N}\right) = 1 \text{ and } \left(\frac{P+2}{N}\right) = -1 \tag{6.6}$$

holds. Next we define the following two sequences:

$$V_0 = 2 \ , \ V_1 = P \ , \ V_{i+1} = PV_i - V_{i-1};$$

$$S_1 = V_h \ , \ S_{i+1} = S_i^2 - 2.$$

Then the two following statements are equivalent:

1. *N is prime.*
2. *$S_{n-1} \equiv 0 \pmod{N}$.*

Before discussing the proof let us check, that the Lucas-Lehmer test is actually a special case of the theorem above. We set $h = 1$ and $P = 4$ and check (6.6):

$$\left(\frac{2}{N}\right) = 1$$

because of lemma 3.5 and for the other equation we use lemma 3.3, again lemma 3.5 and lemma 3.7 to obtain

$$\left(\frac{6}{N}\right) = \left(\frac{2}{N}\right)\left(\frac{3}{N}\right) = 1 \cdot (-1) = -1.$$

Now let's have a look at the proof given by Rödseth:

Proof. Define $D := (P-2)(P+2)$, then $\left(\frac{D}{N}\right) = -1$ holds and further there exists a prime divisor p of N (if N itself is prime it would be $N = p$, which is our goal to show) such that $\left(\frac{D}{p}\right) = -1$. For this we used the definition of the Jacobi symbol introduced earlier. In the following we work in the field $\mathbb{F}_{p^2}$. Because we can also represent $\mathbb{F}_{p^2}$ as $\mathbb{F}_p[x]/(x^2 - D)$ we find $\omega \in \mathbb{F}_{p^2}$ such that $\omega^2 = D$. Now we define $\alpha = \frac{(P+2+\omega)^2}{4(P+2)}$ with inverse $\alpha^{-1} = \frac{(P+2-\omega)^2}{4(P+2)}$. With that we have an alternative representation of V_i (in the prime field of $\mathbb{F}_{p^2}$): $V_i \equiv \alpha^i + \alpha^{-i}$. We show this by induction. First take $i = 1$. Then

$$\begin{aligned} \alpha + \alpha^{-1} &\equiv \frac{(P+2+\omega)^2 + (P+2-\omega)^2}{4(P+2)} \equiv \frac{2P^2 + 8 + 2D + 8P}{4(P+2)} \\ &\equiv \frac{P^2 + 4 + P^2 - 4 + 4P}{2(P+2)} \equiv \frac{2(P^2 + 2P)}{2(P+2)} \equiv P = V_1. \end{aligned}$$

And now for the induction step:

$\alpha^{i+1} + \alpha^{-(i+1)} \equiv (\alpha^i + \alpha^{-i})(\alpha + \alpha^{-1}) - (\alpha^i \alpha^{-1} + \alpha^{-i}\alpha) \equiv V_i P - V_{i-1} \equiv V_{i+1}$.

Next we can also show

$$S_i \equiv \alpha^{h \cdot 2^{i-1}} + \alpha^{-h \cdot 2^{i-1}} \tag{6.7}$$

in $\mathbb{F}_{p^2}$ by induction. Our next goal is to show, that the following holds:

$$\alpha^{\frac{p+1}{2}} = \left(\frac{P+2}{p}\right). \tag{6.8}$$

Let us start with the left hand side of the equation:

$$\alpha^{\frac{p+1}{2}} = \left(\frac{(P+2+\omega)^2}{4(P+2)}\right)^{\frac{p+1}{2}} = \frac{(P+2+\omega)^{p+1}}{(4(P+2))^{\frac{p+1}{2}}}.$$

In the next step we simplify the numerator:

$$(P+2+\omega)^p \equiv (P^p + 2^p + \omega^p) \text{ in } \mathbb{F}_{p^2}.$$

Let us calculate ω^p.

$$\omega^p = \omega \cdot \left(\omega^2\right)^{\frac{p-1}{2}} = \omega \cdot D^{\frac{p-1}{2}} = \omega \left(\frac{D}{p}\right) = -\omega.$$

Here we used lemma 3.4 and the fact that $\left(\frac{D}{p}\right) = -1$. By this calculation and Fermats little theorem 2.4 we have

$$(P+2+\omega)^p \equiv (P+2-\omega) \pmod{p}.$$

This leads to

$$\begin{aligned}
\alpha^{\frac{p+1}{2}} &\equiv \frac{(P+2+\omega)(P+2-\omega)}{2^{p+1}(P+2)^{\frac{p+1}{2}}} \equiv \frac{(P+2)^2-\omega^2}{4(P+2)} \cdot \frac{1}{(P+2)^{\frac{p-1}{2}}} \\
&\equiv \frac{(P+2)^2 - D}{4(P+2)} \cdot \frac{1}{\left(\frac{P+2}{p}\right)} \equiv \frac{P^2+4+4P-P^2+4}{4(P+2)} \cdot \left(\frac{P+2}{p}\right) \\
&\equiv \frac{4(P+2)}{4(P+2)} \cdot \left(\frac{P+2}{p}\right) \equiv \left(\frac{P+2}{p}\right) \pmod{p},
\end{aligned}$$

which we wanted to show. We used lemma 3.4 again.
Now we can start to show the first implication. Suppose $S_{n-1} \equiv 0 \pmod{N}$.

By the Chinese remainder theorem 5.1 the same equation is true in $\mathbb{F}_{p^2}$. In the following proof all is understood to take place in $\mathbb{F}_{p^2}$ as it is already the case in the paragraphs above. By (6.7) we have

$$S_{n-1} = \alpha^{h\cdot 2^{n-2}} + \alpha^{-h\cdot 2^{n-2}} \equiv 0.$$

Multiplying by $\alpha^{h\cdot 2^{n-2}}$ we obtain

$$\alpha^{h\cdot 2^{n-1}} + 1 \equiv 0.$$

Or also $\alpha^{h\cdot 2^{n-1}} \equiv -1$. As a consequence we know that the multiplicative order of α divides $h \cdot 2^n$.
Suppose $2^n \nmid ord(\alpha)$. So $ord(\alpha) = m$ where $m \mid h \cdot 2^{n-1}$. Choose o such that $mo = h \cdot 2^{n-1}$. Then $\alpha^m \equiv 1$ but also $\alpha^{mo} \equiv 1^o = 1$. This is a contradiction to $\alpha^{h\cdot 2^{n-1}} \equiv -1$. Therefore $2^n \mid ord(\alpha)$. Further by (6.8) we have

$$\alpha^{p+1} = \left(\alpha^{\frac{p+1}{2}}\right)^2 = \left(\frac{P+2}{p}\right)^2 = 1.$$

This means that $ord(\alpha) = k \cdot 2^n \mid p+1$.
So $p+1$ has to be of the form $p+1 = 2^n \cdot k$ and obviously $p = 2^n \cdot k - 1$.
Let's do a little recap. We have $N = h \cdot 2^n - 1$ and want to show that N is prime. The goal is to use contradiction. Therefore we supposed that there exists p prime that divides N. Let us write $N = p \cdot q$ for some $q \in \mathbb{N}$ or also

$$N = h2^n - 1 = pq = (2^n \cdot k - 1)q.$$

Now we consider the equation $\pmod{2^n}$:

$$-1 \equiv N = p \cdot q \equiv -q \pmod{2^n}.$$

In other words we have $q = m2^n + 1$ for some $m \in \mathbb{Z}$. Suppose $N \neq p$. Then $q > 1$ and also $m \geq 1$. Let us first consider the case $m = k = 1$. Then we would have $h = 2^n$ which is a contradiction to h being odd. But on the other hand if $k \geq 2$ or $m \geq 2$ one gets that $h \geq 2^{n+1} - 1$ which again contradicts an assumption of the theorem.
Now for the other implication. Let $N = h \cdot 2^n - 1$ be prime. By (6.8) we have

$$\alpha^{\frac{N+1}{2}} = \left(\frac{P+2}{N}\right) = -1 \text{ in } \mathbb{F}_{N^2}.$$

The second equality simply holds by assumption. Multiplying by $\alpha^{-\frac{N+1}{4}}$ we get

$$\alpha^{\frac{N+1}{4}} = -\alpha^{-\frac{N+1}{4}}$$

or aswell

$$\alpha^{\frac{h2^n}{4}} + \alpha^{-\frac{h2^n}{4}} = \alpha^{h2^{n-2}} + \alpha^{-h2^{n-2}} = 0.$$

By (6.7) we recognise S_{n-1} on the left hand side and can finish the proof. □

7 Comparison of the proofs

In this section we want to analyze and compare the proofs we explained in the last chapters. Starting with the elementary one of Sierpinski [Sie88] it is for sure the one using the least complicated theory. To understand the proof one needs some knowledge in basic number theory, for example the Legendre symbol, the modulus calculation and the notion of a divisor. On the downside the proof does not seem straightforward at all. It would be really difficult to recreate it from scratch and one cannot see the intuition of the author.

Bruce [Bru93] breaks down his proof to elementary facts too. He bases his ideas on some elementary group theory. Besides that one needs an understanding of the ring $\mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$. As simple as that one might ask why we looked at the first proof, because this requires a similar knowledge. But thats not totally true. Bruce only shows one implication and refers to the other one in Rosen's paper. Again the proof of this implication needs the Legendre symbol, as in Sierpinski's proof, but one also needs to understand how to define modulo on another ring than $\mathbb{Z}$. This is not as trivial as it might seem (as we explained in chapter 2). On the other hand one might argue that the implication Bruce shows is the one we are actually interested in and therefore the more important part of the theorem. His implication is enough to convince ourselves, that one can use the Lucas-Lehmer test to show that a Mersenne number is prime. We only need the other implication in order to know that every Mersenne number that violates the Lucas Lehmer test is in fact not prime.

As already mentioned in the last paragraph, the next proof we want to investigate is the one by Rosen [Ros88]. We already discussed the second implication. And for the first implication let us have a look at a quote by Bruce [Bru93]: "In this article we show that it is possible to simplify Rosen's proof of the sufficiency of the test a little to eliminate any mention of algebraic numbers or questions concerning splittings of primes." With that sentence he already explained the main difference of his proof and the one Rosen gave. One thing to add is the use of the Chinese remainder theorem, that Bruce does not need. Second his argumentation of the contradiction is based on looking at different cases of $q \pmod 4$, which is a really common tool in number theory. Further he archieves another contradiction by considering the order of an element. This part is pretty similar to one in the proof by Rödseth, only that Rödseths argumentation gets more difficult because of the additional factor h he uses.

In the proof given by Tao [Tao08] we observe a lot of similarities with the other proofs. For example in our explanation we already skipped some parts

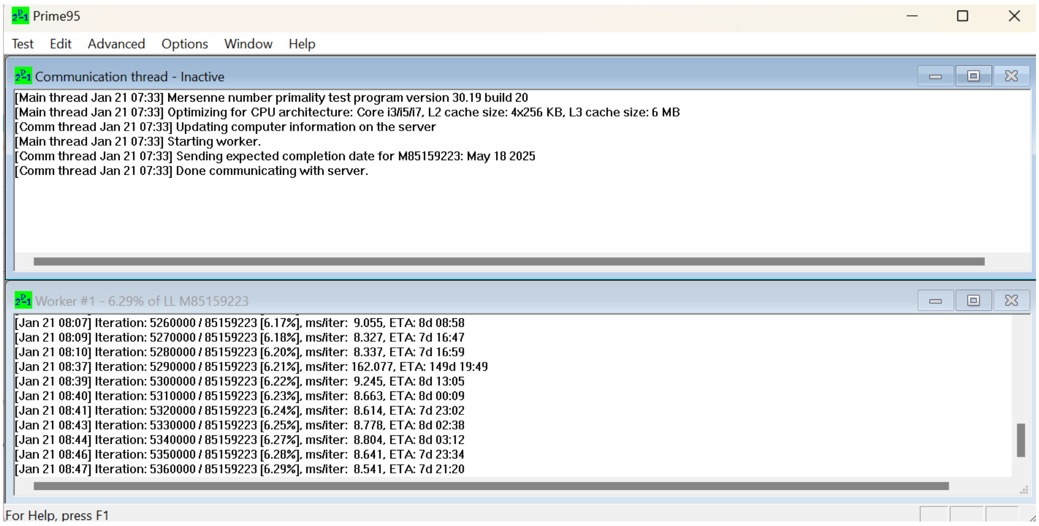
that are similar to parts of the proofs by Rosen and Bruce. Further Tao suggests to work in the field $\mathbb{F}_{N^2}$ which - assuming N is prime - is similar to Rödseths idea of working in $\mathbb{F}_{p^2}$. In contrast to the other proofs Tao explains where the ideas for the proofs originate. That this is exactly his goal becomes very clear from the quote in his paper: "the proofs are sometimes presented in a way that involves pulling a lot of rabbits out of hats, giving the argument a magical feel rather than a natural one. In this post, I will try to explain the basic ideas that make the primality test work, seeking a proof which is perhaps less elementary and a little longer than some of the proofs in the literature, but is perhaps a bit better motivated."
At last we want to discuss the proof given by Rödseth [Rö94]. First we have a look at a quote from his paper: "However, both Western and Rosen overlook the fact that it is not necessary to consider non-rational primes in O_r." That is true, but as in the other proofs the reader does not get an explanation of the intuition behind the proof. How should one know to chose α like this? Let us also mention that Rödseth shows an even more general theorem than the Lucas Lehmer test. One can discuss if this gives us a great advantage. As the sequence S_i already grows really fast in the standard version of the Lucas Lehmer test the computational effort for the generalized version will be even larger, as one needs to compute the sequence V_i first and the starting value of the S_i sequence is higher. For the computation of V_i Rödseth presents a very fast method using the following equalities:

$$V_{2i} = V_i^2 - 2,\ V_{2i+1} = V_i V_{i+1} - P.$$

One thing that still needs to be said is that all proofs considered in this thesis rely on the idea of finding a contradiction to N having a nontrivial prime divisor. But every author presents a different method of how to get to that point. Further one can find several other proofs in literature, which are more or less similar to the ones considered here. For example the proof by Western [Wes32] mentioned already above is one that Rosen improved. According to Rödseth Brewer's [Bre51] and Bruce's proofs have a lot in common and his proof follows the ideas presented by Riesel [Rie69].

8 The Great Internet Mersenne Prime Search project

Now that we have considered the theoretical part of the Lucas-Lehmer test, we will look at an application in this chapter.
As one notices really fast trying to do the calculation, the sequence S_p increases very rapidly. Therefore it is already computationally expensive to check $M_p \mid S_{p-1}$ for $p > 10$. In chapter 10.3 of [Sie88] there is an explanation how to simplify the calculation, such that it can be implemented.
Speaking of implementation, the GIMPS project [gim] (the Great Internet Mersenne Prime Search) is a project where everyone can contribute with a computer to help find the next prime number. On the website they explain briefly what they do: "If no factor is found after an appropriate amount of effort, the Mersenne number is tested with a PRP (Probable Prime) test. If that says composite, the candidate is not a Mersenne Prime. In the (rare) case that PRP says probably prime, the number is re-tested with Lucas-Lehmer test to verify primality." An important information about this quote is, that the GIMPS project does not only rely on the Lucas-Lehmer test. In order to save computation capacity, it only applies the Lucas-Lehmer test to numbers that have passed the PRP test. An explanation of how to implement such PRP tests and also how to test factors with minimal effort can be found in chapter 8 of [Coh93]. A PRP test uses calculations that are a lot faster than the Lucas-Lehmer test and if the outcome is "not prime" the considered number is not prime, so we are only left to apply the Lucas-Lehmer test to the few numbers that do not pass the PRP test. The PRP test finds numbers that are prime with a very high probability.
Your computer can help in one of these steps for a specific number. As easy as this might sound, every little step takes a long time. This is, because the numbers that are investigated today are really large. As an example of this, the latest Mersenne prime, the 52^{nd} Mersenne prime number, that has been discovered is $2^{136279841} - 1$ and has 41.024.320 digits. On the website of GIMPS one can find a document that contains the whole number. This number is also a perfect example of how long these calculations take. It was verified on October 21^{st} 2024 and the last discovery of a Mersenne prime was almost 6 years before that in 2018. I joined the project to get a better idea of it. First of all, downloading the software is fast and easy to understand. But to get significant results is not that easy. The computations that are part of the GIMPS project still need a really high effort, even after being split up. As an example one can see the process of calculating my laptop is doing: In the first window it says: "Sending expected completion date for M85159223:


Prime95
Test Edit Advanced Options Window Help
Communication thread - Inactive

```
[Main thread Jan 21 07:33] Mersenne number primality test program version 30.19 build 20
[Main thread Jan 21 07:33] Optimizing for CPU architecture: Core i3/i5/i7, L2 cache size: 4x256 KB, L3 cache size: 6 MB
[Comm thread Jan 21 07:33] Updating computer information on the server
[Main thread Jan 21 07:33] Starting worker.
[Comm thread Jan 21 07:33] Sending expected completion date for M85159223: May 18 2025
[Comm thread Jan 21 07:33] Done communicating with server.
```

```
[Jan 21 08:07] Iteration: 5260000 / 85159223 [6.17%], ms/iter:  9.055, ETA: 8d 08:58
[Jan 21 08:09] Iteration: 5270000 / 85159223 [6.18%], ms/iter:  8.327, ETA: 7d 16:47
[Jan 21 08:10] Iteration: 5280000 / 85159223 [6.20%], ms/iter:  8.337, ETA: 7d 16:59
[Jan 21 08:37] Iteration: 5290000 / 85159223 [6.21%], ms/iter: 162.077, ETA: 149d 19:49
[Jan 21 08:39] Iteration: 5300000 / 85159223 [6.22%], ms/iter:  9.245, ETA: 8d 13:05
[Jan 21 08:40] Iteration: 5310000 / 85159223 [6.23%], ms/iter:  8.663, ETA: 8d 00:09
[Jan 21 08:41] Iteration: 5320000 / 85159223 [6.24%], ms/iter:  8.614, ETA: 7d 23:02
[Jan 21 08:43] Iteration: 5330000 / 85159223 [6.25%], ms/iter:  8.778, ETA: 8d 02:38
[Jan 21 08:44] Iteration: 5340000 / 85159223 [6.27%], ms/iter:  8.804, ETA: 8d 03:12
[Jan 21 08:46] Iteration: 5350000 / 85159223 [6.28%], ms/iter:  8.641, ETA: 7d 23:34
[Jan 21 08:47] Iteration: 5360000 / 85159223 [6.29%], ms/iter:  8.541, ETA: 7d 21:20
```

May 18 2025". In the second window one sees the progress and notices that every iteration or 0.01% of the calculation take around $1-3$ minutes. So as a result my laptop is really slow in making progress. On the website they present which user succeded in finishing which calculation and one can see high differences in time. So computers with high computational capacity are a lot more likely to discover a new Mersenne prime and contribute much more to the project, than a laptop like mine.

9 Conclusion

To conclude, in this master thesis one gets an overview of the most important methods of proving the Lucas-Lehmer test. When working with the proofs one gets a good understanding of different aproaches to prove numbertheoretical statements. The methods such as the Legendre symbol, working in some helpful field or ring, considering special elements and its orders, the notion of a prime splitting/ inerting or ramifying in $\mathbb{Z}[\sqrt{\omega}]$ and using Fermats little theorem, are also handy components for other proofs in number theory. Further as Tao showed in his paper the knowledge of different proofs might help to combine them and find a more intuitive one.

In number theory there are still a lot of open problems and conjectures about prime numbers, which are easier to understand if one knows more about the existing proofs and theorems. One open problem that is closely related to the subject of this text is the question of wether there exist infinitely many Mersenne prime numbers. Scientists have tried to find an answer to that question for decades. Maybe this collection of different proofs of the Lucas-Lehmer test helps to get an idea to proof an open problem. In this master thesis we discussed a lot of different tools to prove numbertheoretical statements. There are often many different ways to aproach a proof and often proofs are not straightforward.

As we saw in the last chapter, the Lucas-Lehmer test has a practical aplication. Thanks to the Lucas-Lehmer test, scientists where able to design the GIMPS project. With its help modern computers were able to identify several Mersenne prime numbers and the search is not over yet. Who knows when the GIMPS project will anounce the next discovery of a Mersenne prime. Nevertheless as exponents are growing larger the research on Mersenne primes is significantly slowing down. One possibility to gain more speed again would be to improve the computing capacity of computers. Also helpful would be if future research may focus on improving the scalability of the test or developing alternative methods that can complement or expand upon the Lucas-Lehmer test for even larger numbers. Another direction of research would be to consider different types of primes. Mersenne primes are the highest known primes up to today, but maybe it is possible to find some sort of test similar to the Lucas-Lehmer test, that helps to find other prime numbers.

In conclusion, the Lucas-Lehmer test is an indispensable tool in modern number theory, and while it has certain limitations, it remains at the forefront of computational prime testing.

References

[A$^+$17] T. Arens et al. *Ergänzungen und Vertiefungen zu Arens et al., Mathematik.* Springer Spektrum Berlin, Heidelberg, 2017.

[Bax22] Christian Baxa. Algebraic number theory. ”`https://www.mat.univie.ac.at/~baxa/ws2223.html`”, 2022.

[Bre51] B.W. Brewer. Tests for primality. *Duke Math. J., 18, pp. 757-763.*, 1951.

[Bru93] J.W. Bruce. A really trivial proof of the Lucas-Lehmer Test. *Taylor and Francis, The American Mathematical Monthly, Vol. 100, No. 4, pp. 370-371*, 1993.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer Berlin, Heidelberg, 1993.

[gim] Great Internet Mersenne Prime Search. ”`https://www.mersenne.org/`.

[KM21] C. Karpfinger and K. Meyberg. *Algebra: Gruppen-Ringe-Körper.* Springer Spektrum Berlin, Heidelberg, 2021.

[Rie69] H. Riesel. Lucasian criteria for the primality of $n = h \cdot 2^n - 1$. *Math. Comp., 23, pp. 869-875.*, 1969.

[Ros88] M. I. Rosen. A Proof of the Lucas-Lehmer Test. *Taylor and Francis, The American Mathematical Monthly, Vol. 95, No. 9, pp. 855-856*, 1988.

[Rö94] Ö. J. Rödseth. A note on primality tests for $n = h \cdot 2^n - 1$. *Department of Mathematics, University of Bergen, All´egt. 55, N-5007 Bergen, Norway*, 1994.

[Saw17] A. Sawicki. ”`https://www.math.uni-duesseldorf.de/~bogopolski/pdfs2/Seminar_Zahlentheorie/ZT_03.pdf`, 2017.

[Sch07] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie.* Springer-Verlag Berlin Heidelberg, 2007.

[Sie88] W. Sierpinski. *Elementary Theory of Numbers.* polish scientific publishers, 1988.

[SW24] G. Stroth and R. Waldecker. *Elementare Algebra und Zahlentheorie.* Birkhäuser Cham, 2024.

[Tao08] T. Tao. The Lucas-Lehmer test for Mersenne primes. *Expository Mathematics*, 2008.

[Wes32] A. E. Western. On Lucas's and Pepin's test on the primeness of Mersenne's numbers. *Journal of the London Mathematical Society, Volume s1-7, Issue 2, Pages 130–137*, 1932.