# A Prime or Not a Prime? That is the Question

Vetle Tjora

Bachelor's thesis
2022:K15

Lund University

Faculty of Science
Centre for Mathematical Sciences
Mathematics

Centrum Scientiarum Mathematicarum

# A Prime or Not a Prime? That is the Question

Vetle V. Tjora

Bachelor's thesis
2021–2022

## Popular Scientific Summary

Among the integers, aside from maybe 0 and 1, the primes are no doubt the most interesting ones. Not only are they interesting in their own rights, but they can also be utilised to construct mathematical objects like rings, fields, groups and so on. Going outside of mathematics, primes can be used in computer science and play an essential role in cryptography; sensitive data online are kept safe because of primes. Primes even find their way into folklore and mythology. Just think of the Holy Trinity, or how three 7's means jackpot in Las Vegas, or Friday the 13th.

Unfortunately, it remains a difficult task to check if an integer is prime. There are no simple algorithms that immediately tells you if a number is prime or not. Of course, with some time at hand, anyone can figure out all the primes less than 100. With more time, one can do the same for the primes less than 1000. However, there is a limit to anyone's patience, and for large integers, even computers are not efficient enough.

However, there are ways to test if an integer is prime, aptly named primality tests. One such test is the Lucas–Lehmer test, a test that can check very large integers, but alas, only tests a small portion of the integers known as the Mersenne numbers. Luckily, one can generalise the Lucas–Lehmer test to test a larger part of the integers. This thesis will give a proof of both the Lucas–Lehmer test and a generalised version.

**Abstract**

In this survey, we shall prove the Lucas–Lehmer primality test used to find the Mersenne primes. A proof of the Law of Cubic Reciprocity will also be presented, which will be applied in the proof of a generalisation of the Lucas–Lehmer primality test.

# Contents

# 1 Introduction

This thesis consists of three sections. The first section introduces the ring $\mathbb{Z}[\sqrt{3}]$ with the intention of proving the Lucas–Lehmer primality test. The Lucas–Lehmer test is a test for the Mersenne numbers. The Mersenne numbers are the integers on the form $M_n = 2^n - 1$, for some integer $n$. When a Mersenne number is prime, it is called a Mersenne prime, and it is those primes that the Lucas–Lehmer test classifies. Because of its exponential nature, the Mersenne numbers increase fast for each $n$, and thus the Mersenne primes are few, and largest of them are impressively large primes.

The second section introduces the ring $\mathbb{Z}[\omega]$ and the cubic residue character. The section ends with proving the the law of cubic reciprocity which is later used in the last section of the thesis.

The final section generalises the Lucas–Lehmer test so that one can test more than just the Mersenne numbers. It cannot check all integers, but it is a significant improvement to the original test.

# 2 The Lucas–Lehmer Test

The following section of the thesis can be found in most elementary number theory literature. It will therefore not be referred to any specific literature until Section 3 of this thesis.

## 2.1 The Ring $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{3}]$

**Definition 2.1** We define

$$\mathbb{Q}[\sqrt{3}] = \left\{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \right\}.$$

**Proposition 2.2** $\mathbb{Q}[\sqrt{3}]$ is a ring.

*Proof* Since $\mathbb{Q}[\sqrt{3}]$ is a non-empty subset of $\mathbb{R}$, we only have to check that $\mathbb{Q}[\sqrt{3}]$ is closed under subtraction and multiplication to show that it is a subring of $\mathbb{R}$. Let $\alpha = a_1 + a_2\sqrt{3}$ and $\beta = b_1 + b_2\sqrt{3}$ be elements of $\mathbb{Q}[\sqrt{3}]$. Then

$$\begin{aligned} \alpha - \beta &= a_1 + a_2\sqrt{3} - (b_1 + b_2\sqrt{3}) = a_1 - b_1 + (a_2 - b_2)\sqrt{3} \in \mathbb{Q}[\sqrt{3}], \\ \alpha\beta &= (a_1 + a_2\sqrt{3})(b_1 + b_2\sqrt{3}) = a_1b_1 + 3a_2b_2 + (a_1b_2 + a_2b_1)\sqrt{3} \in \mathbb{Q}[\sqrt{3}], \end{aligned}$$

and so $\mathbb{Q}[\sqrt{3}]$ is closed under subtraction and multiplication and must be a ring. □

**Definition 2.3** If $\alpha = a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$, we define the conjugate of $\alpha$ as $\overline{\alpha} = a - b\sqrt{3}$, and the norm as

$$N(\alpha) = \alpha\overline{\alpha} = \left(a + b\sqrt{3}\right)\left(a - b\sqrt{3}\right) = a^2 - 3b^2.$$

**Proposition 2.4** If $\alpha$, $\beta \in \mathbb{Q}[\sqrt{3}]$, then $N(\alpha)N(\beta) = N(\alpha\beta)$.

*Proof* It is easily seen by direct computation. Let $\alpha = a_1 + a_2\sqrt{3}$ and $\beta = b_1 + b_2\sqrt{3}$. Then we get

$$\begin{aligned} N(\alpha)N(\beta) &= \left(a_1^2 - 3a_2^2\right)\left(b_1^2 - 3b_2^2\right) = (a_1b_1)^2 + (3a_2b_2)^2 - 3\,(a_1b_2)^2 - 3\,(a_2b_1)^2 \\ &= \left((a_1b_1)^2 + 6a_1a_2b_1b_2 + (3a_2b_2)^2\right) - 3\left((a_1b_2)^2 + 2a_1a_2b_1b_2 + (a_2b_1)^2\right) \\ &= (a_1b_1 + 3a_2b_2)^2 - 3\,(a_1b_2 + a_2b_1)^2 = N\left((a_1b_1 + 3a_2b_2) + (a_1b_2 + a_2b_1)\,\sqrt{3}\right) \\ &= N(\alpha\beta). \ \square \end{aligned}$$

**Definition 2.5** We define

$$\mathbb{Z}[\sqrt{3}\,] = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\right\}.$$

$\mathbb{Z}[\sqrt{3}\,]$ is essential in the proof of the Lucas–Lehmer test. Before we can state and prove the Lucas–Lehmer test however, we must first establish some properties of $\mathbb{Z}[\sqrt{3}\,]$. This includes, among other things, to show that $\mathbb{Z}[\sqrt{3}\,]$ is a ring, and classifying the units and the primes.

**Proposition 2.6** $\mathbb{Z}[\sqrt{3}\,]$ is a subring of $\mathbb{Q}[\sqrt{3}\,]$.

*Proof* The proof follows the exact same procedure as the proof of Proposition 2.2, just substitute $\mathbb{Q}[\sqrt{3}\,]$ with $\mathbb{Z}[\sqrt{3}\,]$, and $\mathbb{R}$ with $\mathbb{Q}[\sqrt{3}\,]$. $\square$

Notice that because $\mathbb{Z}[\sqrt{3}\,]$ is a subring of $\mathbb{Q}[\sqrt{3}\,]$, the norm $N$ as defined in Definition 2.3 and all its properties hold in $\mathbb{Z}[\sqrt{3}\,]$.

**Proposition 2.7** Let $\alpha$ be an element in $\mathbb{Z}[\sqrt{3}\,]$, then $\alpha = a + b\sqrt{3}$, $a, b \in \mathbb{Z}[\sqrt{3}\,]$, is a unique representation.

*Proof* Let $a + b\sqrt{3} = a' + b'\sqrt{3}$. Then $a + b\sqrt{3} - (a' + b'\sqrt{3}\,) = 0$, and so

$$(a - a'\,) + (b - b'\,)\sqrt{3} = 0.$$

Since $a$, $b$, $a'$ and $b'$ are all integers, this only holds if $a = a'$ and $b = b'$. $\square$

## 2.2 Units in $\mathbb{Z}[\sqrt{3}\,]$

**Theorem 2.8** The units in $\mathbb{Z}[\sqrt{3}\,]$ are

$$\pm\varepsilon^k,$$

where $\varepsilon = 2 + \sqrt{3}$ and $k \in \mathbb{Z}$.

*Proof* First, we prove that $\varepsilon$ is the smallest unit greater than 1. It is easily shown that $\varepsilon$ is a unit by noting that the norm of $\varepsilon$ is 1,

$$N(\varepsilon) = \varepsilon\bar{\varepsilon} = (2 + \sqrt{3}\,)(2 - \sqrt{3}\,) = 4 - 3 = 1.$$

Thus $\bar{\varepsilon} = \varepsilon^{-1}$ and so $\varepsilon$ is a unit. To see that it is the smallest unit, notice that for any unit $\eta$ in $\mathbb{Z}[\sqrt{3}\,]$, there must be an inverse $\eta^{-1}$ such that $\eta\eta^{-1} = 1$. Consequently, we attain

$$N(\eta)N(\eta^{-1}) = N(\eta\eta^{-1}) = N(1) = 1.$$

Since the norm is always an integer, the norm $N(\eta)$ of any unit $\eta$ must be equal to $\pm 1$. Assume $\eta = a + b\sqrt{3}$ is the smallest unit greater than 1, in $\mathbb{Z}[\sqrt{3}\,]$. If $a, b < 0$, then $\eta < 0$, so this cannot be the case. It is also clear that $a, b \neq 0$, because otherwise $N(\eta) = a^2$ or $3b^2$, and since $N(\eta) = \pm 1$, we must have $\eta = \pm 1$ which contradicts the assumption that $\eta > 1$. For the case $a < 0 < b$, assume $a = -c$ for some positive integer $c$. Then

$$1 < \eta = a + b\sqrt{3} = -c + b\sqrt{3} < c + b\sqrt{3},$$

but

$$c + b\sqrt{3} = -a + b\sqrt{3} = -\overline{\eta},$$

so

$$\overline{\eta} = -\left(c + b\sqrt{3}\right) < -1.$$

So $N(\eta) = \eta\overline{\eta} < -1$. If $b < 0 < a$ and $b = -c$ for some positive integer $c$,

$$1 < \eta = a + b\sqrt{3} = a - c\sqrt{3} < a + c\sqrt{3} = \overline{\eta},$$

thus $N(\eta) > 1$. We can conclude that $a, b > 0$. But in this case, the only possibility for $\eta$ such that $1 < \eta < \varepsilon$ is $\eta = 1 + \sqrt{3}$, but $N(1 + \sqrt{3}\,) = -2$, and therefore it cannot be a unit.

Take any unit $\eta > 1$ in $\mathbb{Z}[\sqrt{3}\,]$. Since $\varepsilon$ is the smallest positive unit greater than 1, $1 < \varepsilon \leq \eta$, and because $\varepsilon$ and $\eta$ are both real numbers, it follows that

$$\eta = \varepsilon^r,$$

for some real number $r \geq 1$. If we write $r = s + t$, where $s = \lfloor r \rfloor$ and $0 \leq t < 1$, we get

$$\eta = \varepsilon^{s+t},$$

and it follows that

$$\varepsilon^{-s}\eta = \varepsilon^t.$$

Since $\varepsilon^{-s}$ and $\eta$ are units, $\varepsilon^t$ must be one too. However,

$$1 \leq \varepsilon^t < \varepsilon,$$

and $\varepsilon$ is the smallest unit greater than 1. So we must have $\varepsilon^t = 1$, i.e. $t = 0$. Thus $\eta = \varepsilon^s$ for $s \in \mathbb{Z}_+$.

Now consider the units $0 < \eta < 1$. It should be clear that the inverse of $\eta$ must be greater than 1. So $\eta^{-1} = \varepsilon^k$ for some positive integer $k$. It immediately follows that

$$\eta = \varepsilon^{-k}.$$

For units $\eta < 0$, there must be an inverse $\eta^{-1} < 0$ such that $\eta\eta^{-1} = 1$. This implies

$$(-\eta)\left(-\eta^{-1}\right) = 1.$$

It follows that $-\eta$ is a positive unit, i.e. $-\eta = \varepsilon^k$ for an integer $k$. Therefore all negative units $\eta$ can be written in the form

$$-\varepsilon^k,$$

for $k \in \mathbb{Z}$. $\square$

## 2.3 Unique Factorisation in $\mathbb{Z}[\sqrt{3}\,]$

**Theorem 2.9** $\mathbb{Z}[\sqrt{3}\,]$ is a euclidean domain with respect to the norm $\alpha \mapsto |N(\alpha)|$. In particular, $\mathbb{Z}[\sqrt{3}\,]$ is a unique factorisation domain.

*Proof* For $z, w \in \mathbb{Z}[\sqrt{3}\,]$, we set

$$\frac{z}{w} = x + y\sqrt{3}, \quad x, y \in \mathbb{Q}.$$

Let $m$ and $n$ be the integers closest to $x$ and $y$, respectively, i.e.

$$|x - m|\,,\ |y - n| \leq \frac{1}{2},$$

and set $q = m + n\sqrt{3}$. Thus we get

$$\frac{z - qw}{w} = x + y\sqrt{3} - \left(m + n\sqrt{3}\right) = (x - m) + (y - n)\sqrt{3}.$$

Taking the norm on both sides gives

$$N\left(\frac{z - qw}{w}\right) = (x - m)^2 - 3\,(y - n)^2\,.$$

By our definition of $m$ and $n$ we get the following inequalities

$$(x - m)^2 - 3\,(y - n)^2 \leq \left(\frac{1}{2}\right)^2 - 3 \cdot 0^2 = \frac{1}{4},$$
$$(x - m)^2 - 3\,(y - n)^2 \geq 0^2 - 3\left(\frac{1}{2}\right)^2 = -\frac{3}{4},$$

and thus

$$-\frac{3}{4} \leq N\left(\frac{z - qw}{w}\right) \leq \frac{1}{4},$$

or more specifically

$$\left|N\left(\frac{z - qw}{w}\right)\right| < 1.$$

Consequently, for every $z, w \in \mathbb{Z}[\sqrt{3}\,]$, there is a $q \in \mathbb{Z}[\sqrt{3}\,]$ such that

$$|N(z - qw)| < |N(w)|\,.$$

As a result, we can use the Euclidean algorithm and $\mathbb{Z}[\sqrt{3}\,]$ must be a unique factorisation domain. □

Since primes and irreducibles are the same in unique factorisation domains, this thesis will solely refer to primes. This also holds later in the thesis when discussing the ring $\mathbb{Z}[\omega]$.

## 2.4 Primes in $\mathbb{Z}[\sqrt{3}]$

**Theorem 2.10** If $p > 0$ is a rational prime, i.e. a prime in $\mathbb{Z}$, then

(i) $p = 2$ or $3 \Rightarrow p$ ramifies in $\mathbb{Z}[\sqrt{3}]$,

(ii) $p \equiv \pm 5 \pmod{12} \Rightarrow p$ is prime in $\mathbb{Z}[\sqrt{3}]$.

(iii) $p \equiv \pm 1 \pmod{12} \Rightarrow p$ splits into conjugate primes in $\mathbb{Z}[\sqrt{3}]$,

*Proof* (i) It is easily checked that 2 and 3 ramify. To see this, all we have to do is see that

$$\left(1+\sqrt{3}\right)^2 = 1 + 2\sqrt{3} + 3 = 2\left(2+\sqrt{3}\right) = 2\varepsilon,$$

meanwhile $3 = \left(\sqrt{3}\right)^2$. Therefore, both 2 and 3 ramify in $\mathbb{Z}[\sqrt{3}]$.

The cases (ii) and (iii) are less obvious. We start by noticing that $p$ cannot split into more than 2 non-units, for if $p = \pi_1\pi_2\cdots\pi_n$ where $n \geq 3$, then

$$p^2 = N(p) = N(\pi_1\pi_2\cdots\pi_n) = N(\pi_1)N(\pi_2)\cdots N(\pi_n).$$

If arranged such that $|N(\pi_1)| \geq |N(\pi_2)| \geq \cdots \geq |N(\pi_n)|$, we must have $|N(\pi_1)| = |N(\pi_2)| = p$ and $|N(\pi_i)| = 1$ for $3 \leq i \leq n$, i.e. $\pi_i$ must be a unit for $i \geq 3$. Now assume $p$ splits into $p = \pi\pi'$. Then $N(\pi) = N(\pi') = \pm p$. If $\pi = m + n\sqrt{3}$, we get

$$N(\pi) = m^2 - 3n^2 \equiv 0 \pmod{p}.$$

If $p \mid n$, $p$ must also divide $m$, and as a result $p \mid \pi$, but $\pi$ is prime, so this is impossible thus $p$ cannot divide $n$. Therefore we have

$$\begin{aligned} m^2 &\equiv 3n^2 \pmod{p}, \\ m^2 n^{-2} &\equiv 3 \pmod{p}, \\ \left(mn^{-1}\right)^2 &\equiv 3 \pmod{p}. \end{aligned}$$

Consequently, 3 is a quadratic residue of $p$, and $\left(\frac{3}{p}\right) = 1$.

Now consider case (ii), and assume that $p \equiv 5 \pmod{12}$. Then

$$p = 12k + 5 = 4(3k+1) + 1,$$

so $p \equiv 1 \pmod{4}$. It follows from quadratic reciprocity that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. Furthermore, $p = 3(4k+2) - 1$, so $p \equiv -1 \pmod{3}$, and so $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$. In a similar fashion, if $p \equiv -5 \pmod{12}$, we get $p \equiv -1 \pmod{4}$ and $p \equiv 1 \pmod{3}$, so

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

Thus $p$ cannot be split if $p \equiv \pm 5$.

Considering the last case (iii), we start by assuming $p \equiv 1 \pmod{12}$. By the same procedure as used for case (ii), we get $p \equiv 1 \pmod{3}$ and $p \equiv 1 \pmod{4}$. So it follows that

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

and for $p \equiv -1 \pmod{12}$,

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

Hence if $p \equiv \pm 1 \pmod{12}$ there exists an $a$ such that

$$\begin{aligned} & a^2 \equiv 3 \pmod{p} \\ \Rightarrow\ & p \mid a^2 - 3 = \left(a + \sqrt{3}\right)\left(a - \sqrt{3}\right). \end{aligned}$$

However, if $p$ does not split, $p$ must divide either $\left(a + \sqrt{3}\right)$ or $\left(a - \sqrt{3}\right)$. But if

$$\begin{aligned} & p \mid \left(a \pm \sqrt{3}\right) \\ \Rightarrow\ & p\alpha = a \pm \sqrt{3}, \text{ for some } \alpha = b + c\sqrt{3}, \end{aligned}$$

then $p\alpha = p\left(b + c\sqrt{3}\right) = pb + pc\sqrt{3} = a \pm \sqrt{3}$, and following from this, $pb = a$ and $pc = \pm 1$, but the latter is impossible unless $p = \pm 1$ which contradicts $p$ being a prime.

Since $p = \pm N(\pi) = \pm\pi\overline{\pi}$, this concludes the proof. □

## 2.5 The Lucas–Lehmer Test

Now we are ready to present the Lucas–Lehmer test and prove it:

**Theorem 2.11** If $p$ is an odd prime, then $P = 2^p - 1$ is a prime if and only if

$$\varepsilon^{2^{p-1}} \equiv -1 \pmod{P},$$

where

$$\varepsilon = 2 + \sqrt{3}.$$

*Proof* Suppose $P$ is prime. By the binomial theorem,

$$\varepsilon^P = \left(2 + \sqrt{3}\right)^P = \sum_{k=0}^{P} \binom{P}{k} 2^{P-k} \left(\sqrt{3}\right)^k.$$

However, for $k \neq 0$ and $k \neq P$,

$$\binom{P}{k} = \frac{P!}{(P-k)!k!} = P\frac{(P-1)!}{(P-k)!k!} \equiv 0 \pmod{P},$$

so

$$\varepsilon^P \equiv 2^P + \left(\sqrt{3}\right)^P \pmod{P}.$$

By Fermat's little theorem, we know that $2^P \equiv 2 \pmod{P}$. Furthermore,

$$\left(\sqrt{3}\right)^P = \sqrt{3} \cdot 3^{\frac{P-1}{2}} \equiv \sqrt{3}\left(\frac{3}{P}\right) \pmod{P},$$

by the definition of the Lagrange symbol. We can compute $\left(\frac{3}{P}\right)$ fairly easily by first noting that

$$P = 2^p - 1 = 4 \cdot 2^{p-2} - 1 \equiv -1 \pmod 4,$$

and

$$P = 2^p - 1 \equiv (-1)^p - 1 = -1 - 1 \equiv 1 \pmod 3.$$

Thence

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

The result of the previous computations becomes

$$\varepsilon^P \equiv 2 + \sqrt{3}\left(\frac{3}{P}\right) = 2 - \sqrt{3} = \varepsilon^{-1} \pmod P.$$

Multiplying by $\varepsilon$ on both sides gives us $\varepsilon^{P+1} \equiv 1 \pmod P$, and since $P + 1 = 2^p$, we can rewrite this as

$$\varepsilon^{2^p} = \left(\varepsilon^{2^{p-1}}\right)^2 \equiv 1 \pmod P,$$

in other words, $P \mid \left(\varepsilon^{2^{p-1}} + 1\right)\left(\varepsilon^{2^{p-1}} - 1\right)$. Since $P \equiv 3 \pmod 4$ and $P \equiv 1 \pmod 3$,

$$P \equiv -5 \pmod{12},$$

so by Theorem 2.10, $P$ must be prime in $\mathbb{Z}[\sqrt{3}\,]$. Since $P$ is a prime, $P$ must divide $\varepsilon^{2^{p-1}} + 1$ or $\varepsilon^{2^{p-1}} - 1$, i.e.

$$\varepsilon^{2^{p-1}} \equiv \pm 1 \pmod P.$$

To determine the correct sign, we note that $\left(1 + \sqrt{3}\right)^2 = 4 + 2\sqrt{3} = 2\varepsilon$. The second observation needed is that

$$\left(1 + \sqrt{3}\right)^P \equiv 1 - \sqrt{3} \pmod P,$$

which is seen by repeating the computation using the binomial theorem as before. Thirdly,

$$\begin{aligned} &\left(1 + \sqrt{3}\right)\left(1 - \sqrt{3}\right) = -2 \\ \Rightarrow \quad &1 - \sqrt{3} = -2\left(1 + \sqrt{3}\right)^{-1}. \end{aligned}$$

Therefore

$$\left(1 + \sqrt{3}\right)^P \equiv 1 - \sqrt{3} = -2\left(1 + \sqrt{3}\right)^{-1} \pmod P.$$

Multiplying both sides by $1 + \sqrt{3}$, we obtain

$$\left(1 + \sqrt{3}\right)^{P+1} = \left(1 + \sqrt{3}\right)^{2^p} = \left(\left(1 + \sqrt{3}\right)^2\right)^{2^{p-1}} = (2\varepsilon)^{2^{p-1}} \equiv -2 \pmod P. \qquad (1)$$

We need to rid ourselves of the powers of 2. By Euler's criterion,

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

Since $p$ is an odd prime, $P = 2^p - 1 \equiv -1 \pmod 8$, and consequently,

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

Thus

$$\begin{aligned} 2^{\frac{P+1}{2}} &\equiv 2 \pmod{P} \\ \Rightarrow \quad 2^{2^{p-1}} &\equiv 2 \pmod{P}, \end{aligned}$$

and (1) can be simplified to our desired result

$$\varepsilon^{2^{p-1}} \equiv -1 \pmod{P}.$$

To prove the converse, we assume that $\varepsilon^{2^{p-1}} \equiv -1 \pmod P$ and that $P$ is not prime. Then $P$ must have prime factor $Q \leq \sqrt{P}$, and

$$\varepsilon^{2^{p-1}} \equiv -1 \pmod{Q}.$$

Squaring both sides of the congruence, we get

$$\varepsilon^{2^p} \equiv 1 \pmod{Q}.$$

From this we see that the order of $\varepsilon \pmod Q$ must divide $2^p$, i.e. the order must be a power of 2. If we assume the order is $2^k < 2^p$, we can set a non-negative integer $n = p - k - 1$, and we get

$$1 = 1^{2^n} \equiv \left(\varepsilon^{2^k}\right)^{2^n} = \varepsilon^{2^{(k+n)}} = \varepsilon^{2^{p-1}} \equiv -1 \pmod{Q}.$$

But this is a contradiction, so the order of $\varepsilon$ must be $2^p \pmod Q$. If we consider the quotient ring

$$A = \mathbb{Z}[\sqrt{3}]/(Q) = \left\{ \left[ m + n\sqrt{3} \right] \mid 0 \leq m, n < Q \right\},$$

we see it must have $Q^2$ elements. And because $0 \in A$ is not a unit, the set $A^\times$ of units in $A$ has less than $Q^2$ elements. By Lagrange's theorem, any unit in $A$ must have order less than $Q^2$. However, the order of $\varepsilon \pmod Q$ is $2^p$, and

$$2^p = P + 1 \geq Q^2 + 1.$$

This is a contradiction and we conclude that $P$ must be prime. □

## 2.6 Recursive Lucas–Lehmer

To tailor the Lucas–Lehmer test for a computer, it is practical to define the test recursively.

**Theorem 2.12** Let $s_i$ be defined by

$$s_i = s_{i-1}^2 - 2, \quad s_0 = 4,$$

and let $p$ be an odd prime. Then

$$P = 2^p - 1 \text{ is prime}$$

if and only if

$$P \mid s_{p-2}.$$

*Proof* Set

$$s_i = \varepsilon^{2^i} + \varepsilon^{-2^i}.$$

We know that $P$ is prime if and only if

$$\varepsilon^{2^{p-1}} \equiv -1 \pmod{P}.$$

By moving everything to the left-hand side and multiplying by $\varepsilon^{-2^{p-2}}$, we get the equivalent statement

$$\varepsilon^{2^{p-2}} + \varepsilon^{-2^{p-2}} \equiv 0 \pmod{P},$$

which is the same as saying

$$P \mid s_{p-2}.$$

We can easily see that

$$s_0 = \varepsilon^1 + \varepsilon^{-1} = 2 + \sqrt{3} + 2 - \sqrt{3} = 4.$$

Lastly, we need to do some simple algebraic manipulations to define $s_i$ recursively,

$$\begin{aligned} s_{i-1}^2 &= \varepsilon^{2^i} + 2 + \varepsilon^{-2^i} = s_i + 2 \\ \Rightarrow \quad s_i &= s_{i-1}^2 - 2. \end{aligned}$$

Note that since $s_0 = 4$, $s_i \in \mathbb{Z}$ for all $i$, and we are done. □

# 3 Cubic Residue

Whilst to prove the Lucas–Lehmer test, one uses quadratic reciprocity and the ring $\mathbb{Z}[\sqrt{3}]$, to prove the generalised version, we will be using cubic reciprocity and $\mathbb{Z}[\omega]$. We will introduce $\mathbb{Z}[\omega]$ first as this ring is used to define the cubic reciprocity character.

The following section follows §1–4 of Chapter 9 in [3] unless otherwise specified.

## 3.1 The Ring $\mathbb{Z}[\omega]$

**Definition 3.1** Let $\omega$ be the complex number

$$\omega = \frac{-1 + \sqrt{-3}}{2}.$$

**Proposition 3.2** $\omega^2 = \omega^{-1} = \bar{\omega} = -1 - \omega$, where $\bar{\omega}$ is the complex conjugate. Additionally, $\omega^3 = 1$.

*Proof* By simple algebra, we see that

$$\omega^2 = \left(\frac{-1+\sqrt{-3}}{2}\right)^2 = \frac{1-2\sqrt{-3}-3}{4} = \frac{-1-\sqrt{-3}}{2} = \bar{\omega},$$

which additionally can be rewritten in following way

$$\omega^2 = \frac{-1-\sqrt{-3}}{2} = -1 + \frac{1-\sqrt{-3}}{2} = -1 - \omega.$$

Furthermore,

$$\omega\bar{\omega} = \omega\omega^2 = \omega\left(-1-\omega\right) = -\omega - \omega^2 = -\omega - \left(-1-\omega\right) = 1.$$

Thus $\omega^2 = \bar{\omega} = \omega^{-1}$ and $\omega^3 = 1$. □

**Definition 3.3** Similarly to $\mathbb{Z}[\sqrt{3}\,]$, we define $\mathbb{Z}[\omega]$ as

$$\mathbb{Z}[\omega] = \left\{a + b\omega \mid a, b \in \mathbb{Z}\right\}.$$

**Proposition 3.4** $\mathbb{Z}[\omega]$ is a ring.

*Proof* Since $\mathbb{Z}[\omega]$ is a non-empty subset of the complex numbers, we only have to show that $\mathbb{Z}[\omega]$ is closed under subtraction and multiplication to prove that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$. Let $\alpha = a_1 + a_2\omega$ and $\beta = b_1 + b_2\omega$ be elements of $\mathbb{Z}[\omega]$. Then

$$\alpha - \beta = a_1 + a_2\omega - (b_1 + b_2\omega) = a_1 - b_1 + (a_2 - b_2)\omega \in \mathbb{Z}[\omega],$$

so $\mathbb{Z}[\omega]$ is closed under subtraction. Furthermore,

$$\begin{aligned}\alpha\beta &= (a_1 + a_2\omega)(b_1 + b_2\omega) = a_1b_1 + (a_1b_2 + a_2b_1)\omega + a_2b_2\omega^2 \\ &= a_1b_1 + (a_1b_2 + a_2b_1)\omega + a_2b_2(-1-\omega) \\ &= a_1b_1 - a_2b_2 + (a_1b_2 + a_2b_1 - a_2b_2)\omega \in \mathbb{Z}[\omega],\end{aligned}$$

which shows that $\mathbb{Z}[\omega]$ is closed under multiplication too. Thus $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$, and more generally a ring. □

**Definition 3.5** We denote the norm of $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ as

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2.$$

**Proposition 3.6** $N(\alpha) \geq 0$ with equality if and only if $\alpha = 0$, for $\alpha \in \mathbb{Z}[\omega]$.

*Proof* Let

$$\alpha = a + b\omega = \left(a - \frac{b}{2}\right) + \frac{\sqrt{3}}{2}bi,$$

then the square of the complex modulus of $\alpha$ is equal to $N(\alpha)$,

$$|\alpha|^2 = \left(a - \frac{b}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}b\right)^2 = a^2 - ab + b^2 = N(\alpha).$$

So $N(\alpha) \geq 0$ with equality if and only if $\alpha = 0$. □

**Proposition 3.7** For $\alpha\beta \in \mathbb{Z}[\omega]$, $N(\alpha)N(\beta) = N(\alpha\beta)$.

*Proof* By direct computation, one can see that $N(\alpha)N(\beta) = N(\alpha\beta)$ in $\mathbb{Z}[\omega]$. □

Note that the complex conjugate of any element $\alpha$ can be written as

$$\bar{\alpha} = a + b\bar{\omega} = a + b(-1-\omega) = a - b + (-b)\omega \in \mathbb{Z}[\omega],$$

and so it follows:

**Proposition 3.8** If $\alpha \in \mathbb{Z}[\omega]$, then $\bar{\alpha} \in \mathbb{Z}[\omega]$.

**Proposition 3.9** $\mathbb{Z}[\omega]$ is a Euclidean domain.

*Proof* Let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ and $\beta$ be a non-zero element of $\mathbb{Z}[\omega]$. Then

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{\alpha\bar{\beta}}{N(\beta)}.$$

Because $\alpha\bar{\beta} \in \mathbb{Z}[\omega]$ and $N(\beta) \in \mathbb{Z}$, we can write

$$\frac{\alpha}{\beta} = r + s\omega, \text{ for } r, s \in \mathbb{Q}.$$

Let $m$ and $n$ be the closest integers to $r$ and $s$, respectively, then

$$|r-m|, \ |s-n| \leq \frac{1}{2}.$$

For $\gamma = m + n\omega$,

$$\begin{aligned} N\left(\frac{\alpha}{\beta} - \gamma\right) &= N((r-m) + (s-n)\,\omega) \\ &= (r-m)^2 - (r-m)(s-n) + (s-n)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1. \end{aligned}$$

Finally, set $\rho = \alpha - \beta\gamma$, and take the norm

$$N(\rho) = N(\alpha - \beta\gamma) = N\left(\left(\frac{\alpha}{\beta} - \gamma\right)\beta\right) = N\left(\frac{\alpha}{\beta} - \gamma\right)N(\beta) < N(\beta). \ \square$$

## 3.2 The Units in $\mathbb{Z}[\omega]$

**Proposition 3.10** The units in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega$ and $\pm\omega^2$.

*Proof* First, we shall show that $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ is a unit if and only if $N(\alpha) = 1$. Suppose that $N(\alpha) = \alpha\bar{\alpha} = 1$. Then the inverse of $\alpha$ is $\alpha^{-1} = \bar{\alpha}$, and so $\alpha$ must be a unit.

Conversely, if $\alpha$ has an inverse $\beta$ such that $\alpha\beta = 1$, then $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. It follows that $N(\alpha) = 1$ as the norm is non-negative. Therefore, if $\alpha = a + b\omega$ is a unit, then

$$N(\alpha) = a^2 - ab + b^2 = 1.$$

Multiplying both sides by 4, and rewriting $4a^2 - 4ab + b^2$ as $(2a - b)^2$, we get

$$4N(\alpha) = (2a - b)^2 + 3b^2 = 4.$$

The equation has integer solutions only if $|b| \leq 1$. If $b = -1$,

$$(2a + 1)^2 = 1, \text{ so } a = 0 \text{ or } a = -1.$$

If $b = 0$,

$$(2a)^2 = 4, \text{ so } a = \pm 1.$$

Lastly, if $b = 1$,

$$(2a - 1)^2 = 1, \text{ so } a = 0 \text{ or } a = 1.$$

The six solutions gives

$$\begin{aligned} 0 - \omega &= -\omega, \\ -1 - \omega &= \omega^2, \\ 1 + 0\omega &= 1, \\ -1 + 0\omega &= -1, \\ 0 + \omega &= \omega, \\ 1 + \omega &= -\omega^2. \end{aligned}$$

□

## 3.3 The Primes in $\mathbb{Z}[\omega]$

**Lemma 3.11** If $\pi$ is a prime, then $N(\pi) = p$ or $p^2$, where $p$ is a rational prime. In the first case, $\pi$ is not an associate to any rational prime, whilst in the second case $p$ and $\pi$ are associates.

*Proof* If $\pi$ is prime, then it is not a unit, so $N(\pi) = \pi\overline{\pi} = n > 1$. Since $n > 1$, and it is an integer, $n$ must be a product of rational primes. Therefore, $\pi \mid p_1 p_2 \cdots p_k$, and $\pi$ must divide one of the prime factors $p_i$, which we call $p$, i.e. there exists a $\gamma$ such that $\pi\gamma = p$, for some prime factor $p$ of $N(\pi)$. Thus we get

$$N(\pi)N(\gamma) = N(\pi\gamma) = N(p) = p^2.$$

Since $N(\pi) > 1$, we are left with two possibilities, either $N(\pi) = p^2$ and $N(\gamma) = 1$, or $N(\pi) = N(\gamma) = p$. If $N(\gamma) = 1$, $\gamma$ must be a unit, and $\pi$ is an associate of $p = \pi\gamma$.

If $N(\pi) = p$ and associate to a rational prime $q$, such that $\pi = q\alpha$ for some unit $\alpha$, we get

$$p = N(\pi) = N(q\alpha) = N(q)N(\alpha) = N(q) = q^2.$$

This cannot be, so $\pi$ cannot be an associate to a rational prime if $N(\pi) = p$. □

**Lemma 3.12** If $N(\pi) = p$ for some rational prime $p$, $\pi$ is prime in $\mathbb{Z}[\omega]$.

*Proof* Assume $\pi$ is not a prime. Then $\pi$ can be written as a product of two non-units, $\pi = \alpha\beta$ where $N(\alpha), N(\beta) > 1$. But then

$$p = N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta),$$

which contradicts $p$ being a rational prime. □

**Lemma 3.13** Let $p$ be a rational prime. If $p \equiv 1 \pmod 3$, $p$ splits in $\mathbb{Z}[\omega]$, i.e. $p$ can be written as $p = N(\pi) = \pi\bar{\pi}$, where $\pi$ and $\bar{\pi}$ are primes in $\mathbb{Z}[\omega]$. If $p \equiv 2 \pmod 3$, then $p$ is a prime in $\mathbb{Z}[\omega]$ and

*Proof* If $p$ is not a prime in $\mathbb{Z}[\omega]$, then $p$ is a product of two non-units, $p = \pi\gamma$. So

$$p^2 = N(p) = N(\pi\gamma) = N(\pi)N(\gamma),$$

and it follows that $N(\pi) = p$. We set $\pi = a + b\omega$, and get $p = N(\pi) = a^2 - ab + b^2$, or

$$4p = (2a - b)^2 + 3b^2,$$

which leaves us with the congruence

$$p \equiv (2a - b)^2 \pmod 3.$$

Since $1^2 \equiv 2^2 \equiv 1 \pmod 3$, we can conclude that $p \equiv 1 \pmod 3$, unless $p \mid 3$, and therefore if $p \equiv 2 \pmod 3$, $p$ must be prime in $\mathbb{Z}[\omega]$.

If $p \equiv 1 \pmod 3$, then $p = 3m + 1$. Since $p$ is odd, $m$ must be even, and either divisible by 4 or not, so we can write $m$ as

$$m = 4n \quad \text{or} \quad m = 4n + 2,$$

respectively. If we first assume that $m = 4n$, we get

$$p = 3m + 1 = 12n + 1 \equiv 1 \pmod{12},$$

and

$$(-1)^{\frac{p-1}{2}} = (-1)^{6n} = 1.$$

Using this and Theorem 9.10 from [3] it follows that

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

If $m$ is not divisible by 4, $m = 4n + 2$ and

$$p = 3m + 1 = 12n + 7 \equiv -5 \pmod{12},$$

and

$$(-1)^{\frac{p-1}{2}} = (-1)^{6n+3} = (-1)^{3(2n+1)} = -1.$$

By utilising the same theorem, it follows that

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

Thus there exists an $a$ such that $a^2 \equiv -3 \pmod p$. Equivalently, there is a $b \in \mathbb{Z}$ such that $bp = \left(a + \sqrt{-3}\right)\left(a - \sqrt{-3}\right)$. By the definition of $\omega$, we can write $\sqrt{-3} = 1 + 2\omega$, and under the assumption that $p$ is prime in $\mathbb{Z}[\omega]$, either of the conditions,

$$p \mid (a + 1 + 2\omega) \quad \text{or} \quad p \mid (a - 1 - 2\omega),$$

must be fulfilled, but $p \nmid 2\omega$ since $p$ is odd, and thus $p$ cannot be prime in $\mathbb{Z}[\omega]$. Therefore, $p$ must be the product of two non-units $p = \pi\gamma$, and

$$p^2 = N(p) = N(\pi)N(\gamma).$$

So we must have $N(\pi) = N(\bar{\pi}) = \pi\bar{\pi} = p$, and hence $\pi$ and $\bar{\pi}$ must be primes. □

For the special case of $p = 3$, note that

$$N(1-\omega) = (1-\omega)(1-\bar{\omega}) = 1 - (\omega + \bar{\omega}) + \omega\bar{\omega} = 3,$$

so $(1-\omega)$ is a prime, whilst 3, on the other hand, is not a prime in $\mathbb{Z}[\omega]$.

The following theorem is not explicitly stated in [3], but it is not difficult to see by combining the previous three lemmas, as can be seen in the proof. However, the theorem is written out here for the convenience of the reader.

**Theorem 3.14** Let $\pi \in \mathbb{Z}[\omega]$, then $\pi$ is prime if and only if

(i) $\pi = \gamma p$, where $\gamma$ is a unit and $p$ is a rational prime such that $p \equiv 2 \pmod 3$,

(ii) or $N(\pi) = p$ for some rational prime $p$.

*Proof* If $\pi$ is prime, then by Lemma 3.11 $N(\pi) = p$ or $p^2$, for a rational prime $p$. If $N(\pi) = p$, then it is the case (ii). If $N(\pi) = p^2$,

$$N(\pi) = p^2 = N(p).$$

It follows that $\pi$ and $p$ are associates which is case (i).

To prove the converse, consider both cases separately. In case (i), $\pi = p \equiv 2 \pmod 3$ for some rational prime $p$. By Lemma 3.13, $\pi$ must be prime. Case (ii) follows directly from Lemma 3.12. □

## 3.4 Primary Primes and the Quotient Ring $D/\pi D$

**Definition 3.15** Let $\alpha \in \mathbb{Z}[\omega]$. We call $\alpha$ *primary* if $\alpha \equiv 2 \pmod 3$.

**Proposition 3.16** Let $\alpha = a_1 + a_2\omega$, then $\alpha$ is primary if and only if $a_1 \equiv 2 \pmod 3$ and $a_2 \equiv 0 \pmod 3$.

*Proof* If $\alpha$ is primary, then $\alpha = 2 + 3\beta$ for some $\beta \in \mathbb{Z}[\omega]$. If $\beta = b_1 + b_2\omega$, then $a_1 = 2 + 3b_1$ and $a_2 = 3b_2\omega$. So $a_1 \equiv 2 \pmod 3$ and $a_2 \equiv 0 \pmod 3$. □

To make notation more readable, we shall start referring to $\mathbb{Z}[\omega]$ as $D$ from now on.

**Theorem 3.17** $D/\pi D$ is a field with $N(\pi)$ elements when $\pi$ is prime.

*Proof* For $D/\pi D$ to be a field, every non-zero element must have a multiplicative inverse. If $\alpha \in D$ is relatively prime to $\pi$, i.e. $\alpha \not\equiv 0 \pmod \pi$, then there exist $\beta, \gamma \in D$ such that

$$\alpha\beta + \gamma\pi = 1$$

as $\mathbb{Z}[\omega]$ is a Euclidean domain. So $\alpha\beta \equiv 1 \pmod \pi$ and it follows that $\alpha$ is a unit in $D/\pi D$, which must therefore be a field.

To prove that $D/\pi D$ has $N(\pi)$ elements, we must consider three cases. First, assume $\pi = q$ is a rational prime congruent to 2 (mod 3). Since $\pi = q$ is an integer, $N(q) = q^2$. We shall show that

$$\{a + b\omega \mid 0 \le a, b < q\}$$

is a complete set of coset representatives. Then $D/qD$ must have $N(q) = q^2$ elements. Take an element $\mu = m + n\omega$ in $D$. For some $a, b, s, t \in D$, and $0 \leq a, b < q$,

$$\mu = (qs + a) + (qt + b)\,\omega.$$

Thus $\mu \equiv a + b\omega \pmod{q}$. Now assume $a + b\omega \equiv a' + b'\omega \pmod{q}$ for $0 \leq a, a', b, b' < q$. Then

$$(a - a') + (b - b')\,\omega = q\gamma,$$

for some $\gamma \in D$. Said in another way,

$$\frac{a - a'}{q} + \frac{b - b'}{q}\omega \in D,$$

which is only possible if $a = a'$ and $b = b'$.

If $\pi$ is not a rational prime, then $N(\pi) = \pi\overline{\pi} = p$ for some rational prime $p \equiv 1 \pmod{3}$ by Lemma 3.13, assuming $\pi \neq 1 - \omega$. We want to prove that

$$\{0, 1, 2, \ldots, p - 1\}$$

is a complete set of coset representatives. Without loss of generality, set $\pi = a + b\omega$ with $a \geq 0$, and assume that $p \mid b$, so that $b = kp$. Then

$$p = N(\pi) = a^2 - ab + b^2 = a^2 - akp + k^2p^2.$$

However, if $a \geq kp$,

$$p = a^2 - akp + k^2p^2 = a\,(a - kp) + k^2p^2 > p.$$

If $kp > a$, we get

$$p = a^2 - akp + k^2p^2 = a^2 + kp\,(kp - a) > p.$$

Both are obvious contradictions, so $p$ cannot divide $b$. If $\mu = m + n\omega$, there is an integer $c$ such that $cb \equiv n \pmod{p}$. This means that $\mu - c\pi \equiv m - ca \pmod{p}$, which implies that $\mu \equiv m - ca \pmod{\pi}$. Thus any $\mu \in D$ is congruent to an integer modulo $\pi$. Furthermore, any integer $l$, can be written as $l = sp + r$ for $0 \leq r < p$, so $l \equiv r \pmod{p}$. It immediately follows that $l \equiv r \pmod{\pi}$, so any element of $D$ is congruent to a positive integer less than $p$ modulo $\pi$. Finally, if $r \equiv r' \pmod{\pi}$ for $0 \leq r, r' < p$, then $r - r' = \gamma\pi$ and

$$N(r - r') = (r - r')^2 = N(\gamma)p.$$

Thus $p \mid (r - r')$, which only holds if $r = r'$.

The last case is $\pi = 1 - \omega$. In this case, $D/\pi D$ has 3 elements. For any $\mu = m + n\omega$ we have

$$\mu \equiv m + n\omega + n\,(1 - \omega) \equiv m + n \pmod{1 - \omega}.$$

So any element of $D$ can be written as an integer modulus $\pi$. The rest of the proof follows the proof of the previous case with $p = 3$ and $\pi = 1 - \omega$. □

By using this result, we can prove an analogue to Fermat's little theorem:

**Corollary 3.18** If $\pi$ is prime and $\pi \nmid \alpha$, then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

*Proof* If $G$ is a multiplicative group with $n$ elements, then $\alpha^n = 1$ for all $\alpha \in G$. Apply this to $(D/\pi D)^*$. □

**Proposition 3.19** For a prime $\pi$ such that $N(\pi) \neq 3$, $[1], [\omega]$ and $[\omega^2]$ are all distinct congruence classes modulo $\pi$.

*Proof* If $1 \equiv \omega \pmod{\pi}$, then

$$\pi \mid (1-\omega).$$

However, $\pi$ and $1-\omega$ are both prime, so they must be associates, and it follows that

$$N(\pi) = N(1-\omega) = 3,$$

which is a contradiction. If $1 \equiv \omega^2 \pmod{\pi}$, then

$$\pi \mid \left(1-\omega^2\right),$$

in other words,

$$\pi \mid (1-\omega)(1+\omega),$$

but $(1+\omega) = -\omega^2$, which is a unit, so again we get the contradiction

$$\pi \mid (1-\omega).$$

Lastly, if $\omega \equiv \omega^2 \pmod{\pi}$, then $\pi$ divides $\omega - \omega^2 = \omega(1-\omega)$, but $\omega$ being a unit, we end up with the same contradiction as the previous two cases. □

The offered proof of the following theorem deviates from the proof of the theorem in [3], and the proof offered here is due to the author.

**Theorem 3.20** If $\pi$ is a prime such that $N(\pi) = p \equiv 1 \pmod{3}$, then $\pi$ has a unique primary associate.

*Proof* If $\pi = a + b\omega$ is not primary and $p \equiv 1 \pmod{3}$, we have 5 different cases,

(i) $a \equiv 0$ and $b \equiv 1 \pmod{3}$,

(ii) $a \equiv 0$ and $b \equiv 2 \pmod{3}$,

(iii) $a \equiv 1$ and $b \equiv 0 \pmod{3}$,

(iv) $a \equiv 1$ and $b \equiv 1 \pmod{3}$,

(v) $a \equiv 2$ and $b \equiv 2 \pmod{3}$.

The remaining four possibilities make $p \equiv 0 \pmod 3$ or $\pi \equiv 2 \pmod 3$. Going through all the cases, we can see that the primary associates are $-\omega^2\pi$, $\omega^2\pi$, $-\pi$, $\omega\pi$ and $-\omega\pi$, respectively. So every $\pi$ has a primary associate.

It remains to show that the primary associate is unique. Assume that $\pi = a + b\omega$ is primary, i.e. $a \equiv 2$ and $b \equiv 0 \pmod 3$. Then its associates are

$$\begin{aligned}
\pi = a + b\omega &\equiv 2 \pmod 3,\\
\omega\pi = -b + (a-b)\,\omega &\equiv 2\omega \pmod 3,\\
\omega^2\pi = -a + b - a\omega &\equiv 1 + \omega \pmod 3,\\
-\pi &\equiv -2 \equiv 1 \pmod 3,\\
-\omega\pi &\equiv -2\omega \equiv \omega \pmod 3,\\
-\omega^2\pi &\equiv -(1+\omega) \equiv 2 + 2\omega \pmod 3.
\end{aligned}$$

We see that among its associates, only $\pi$ is primary. □

## 3.5 The Cubic Character

**Theorem 3.21** Let $\pi$ be prime. If $N(\pi) \neq 3$ and $\pi \nmid \alpha$, then

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod \pi,$$

for a unique $m = 0, 1$ or $2$.

*Proof* First we show that $3 \mid (N(\pi) - 1)$. By Lemma 3.13, if $\pi = q$ is a rational prime not equal to 3, then $q \equiv 2 \pmod 3$, thus

$$N(\pi) = N(q) = q^2 \equiv 2^2 \equiv 1 \pmod 3.$$

If $\pi$ is not a rational prime, then $N(\pi) = p$, where $p \equiv 1 \pmod 3$. Thus $3 \mid (N(\pi) - 1)$.

Now by Corollary 3.18,

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi.$$

However,

$$\alpha^{N(\pi)-1} - 1 = \left(\alpha^{\frac{N(\pi)-1}{3}} - 1\right)\left(\alpha^{\frac{N(\pi)-1}{3}} - \omega\right)\left(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2\right).$$

The reader can check that this holds if they so wish. It follows that $\pi$ must divide at least one of the factors since it is prime. If, however, $\pi$ divides two or more factors, it must divide the difference, but this contradicts Proposition 3.19. □

From this, we can now define the cubic residue character:

**Definition 3.22** Let $\pi$ be a prime in $D$ such that $N(\pi) \neq 3$, and $\alpha \in D$. Then

(i) $\chi_\pi(\alpha) = 0$ if $\pi \mid \alpha$,

(ii) $\alpha^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(\alpha) \pmod \pi$, where $\chi_\pi(\alpha) = 1$, $\omega$ or $\omega^2$.

**Theorem 3.23** If $\pi$ is a prime in $D$ such that $N(\pi) \neq 3$, and $\pi \nmid \alpha$ for $\alpha \in D$, then

$$\chi_\pi(\alpha) = 1,$$

if and only if $\alpha$ is a cubic residue, i.e. $x^3 \equiv \alpha \pmod \pi$ has a solution.

*Proof* Since $(D/\pi D)^*$ is a cyclic group, choose a generator $[\gamma]$ such that $[\alpha] = [\gamma]^a$ and $[x] = [\gamma]^y$ for some $a, y \in \mathbb{Z}$. Then the equation $[x]^3 = [\alpha]$ becomes

$$[\gamma]^{3y} = [\gamma]^a,$$

which is equivalent to solving

$$3y \equiv a \pmod{N(\pi) - 1},$$

because $(D/\pi D)^*$ has $N(\pi) - 1$ elements by Theorem 3.17. In other words, $x^3 \equiv \alpha \pmod{\pi}$ is solvable if and only if

$$3y - (N(\pi) - 1)\, z = a$$

has a solution. The linear Diophantine equation has a solution if and only if the greatest common divisor of 3 and $N(\pi) - 1$, i.e. 3 divides $a$. Thus we have shown that $\alpha$ is a cubic residue if and only if $3 \mid a$.

Now assume that $\alpha \equiv \gamma^a \pmod{\pi}$, where $a$ is a multiple of 3, i.e. $a = 3a'$. Then

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv (\gamma^a)^{\frac{N(\pi)-1}{3}} \equiv \left(\gamma^{\frac{N(\pi)-1}{3}}\right)^a \pmod{\pi}.$$

However, since $\pi \nmid \alpha$, $\pi$ cannot divide $\gamma$ either, so by Theorem 3.21,

$$\left(\gamma^{\frac{N(\pi)-1}{3}}\right)^a \equiv (\omega^m)^a \equiv \omega^{3ma'} \equiv \left(\omega^3\right)^{ma'} \equiv 1 \pmod{\pi},$$

where $m = 0$, 1 or 2.

Conversely, assume that $3 \nmid a$. Again,

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv (\omega^m)^a \pmod{\pi}.$$

However, because $[\gamma]$ is a generator, the order of $\gamma \pmod{\pi}$ is $N(\pi) - 1$, and it follows that $\gamma^{\frac{N(\pi)-1}{3}} \neq 1$, i.e. $m \neq 0$. Furthermore, the order of $\omega \pmod{\pi}$ is 3 by Proposition 3.2, so if $\omega^{ma} \equiv 1$, $ma$ must be a multiple of 3, but this is not the case. □

**Definition 3.24** A mapping $\chi$ from $\mathbb{Z}_p^*$ to some set $S \subseteq \mathbb{C}^*$ is said to be a *multiplicative character* on $\mathbb{Z}_p$ if

$$\chi(ab) = \chi(a)(b),$$

for all $a, b \in \mathbb{Z}_p^*$. If $\chi^3 = 1$, we call $\chi$ a *cubic character*.

## 3.6 The Law of Cubic Reciprocity

The law of cubic reciprocity will be introduced in the near future, but for the proof of said law, we need the notion of *Gauss sums* and the *Jacobi sum*. The author will provide the necessary statements and proofs regarding these sums, but if the reader should want to know more than strictly necessary for the purposes of this thesis, they can look through Chapter 8 of [3], where many of the following lemmas also can be found.

**Definition 3.25** Let $\chi$ be a multiplicative character on $\mathbb{Z}_p$ and $\zeta = e^{\frac{2\pi i}{p}}$. If $a$ is an integer such that $0 \leq a < p$, then the *Gauss sum* is defined as

$$g_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}.$$

When $a = 1$ we denote $g_a(\chi) = g_1(\chi) = \sum \chi(t)\zeta^t$ as $g(\chi)$.

**Definition 3.26** If $\chi$ and $\lambda$ are multiplicative characters on $\mathbb{Z}_p$, then the *Jacobi sum* is defined as

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b),$$

for $a, b \in \mathbb{Z}_p^*$.

The law of cubic reciprocity states that:

**Theorem 3.27** Let $\pi_1$ and $\pi_2$ be distinct primary primes, and let $\pi_1, \pi_2 \neq 3$. Then

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

Before proving the theorem, we shall need some lemmas and notions. If $\pi$ is a prime such that $N(\pi) = p$, where $p$ is a rational prime, then in the proof of Theorem 3.17 we have shown that $\{1, 2, \ldots, p-1\}$ is a complete set of coset representatives. This provides an explicit isomorphism between $D/\pi D$ and $\mathbb{Z}_p$ that can be treated as an identification

**Proposition 3.28** If $N(\pi) = p \neq 3$, then the cubic residue character $\chi_\pi$ is a cubic character on $\mathbb{Z}_p$.

*Proof* First we must prove that $\chi_\pi(ab) = \chi_\pi(a)\chi_\pi(b)$ for all $a, b \in \mathbb{Z}_p^*$,

$$\chi_\pi(ab) \equiv (ab)^{\frac{N(\pi)-1}{3}} \equiv a^{\frac{N(\pi)-1}{3}} b^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(a)\chi_\pi(b) \pmod{\pi}.$$

Since 1, $\omega$ and $\omega^2$ are distinct $\pmod{\pi}$, it follows that $\chi_\pi(ab) = \chi_\pi(a)\chi_\pi(b)$.

If $a \equiv b \pmod{p}$,

$$\chi_\pi(a) \equiv a^{\frac{N(\pi)-1}{3}} \equiv b^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(b) \pmod{\pi},$$

which implies that $\chi_\pi(a) = \chi_\pi(b)$, so $\chi_\pi$ is well-defined on $\mathbb{Z}_p^*$.

By Corollary 3.18,

$$\chi_\pi(a)^3 \equiv \left(a^{\frac{N(\pi)-1}{3}}\right)^3 = a^{N(\pi)-1} \equiv 1 \pmod{\pi},$$

showing that $\chi_\pi$ is cubic. □

**Lemma 3.29** $J(\chi_\pi, \chi_\pi)$ is primary in $D$.

*Proof* By definition

$$g(\chi_\pi)^3 = \left(\sum_{t=0}^{p-1} \chi_\pi(t)\zeta^t\right)^3 \equiv \sum_{t=0}^{p-1} \chi_\pi(t)^3\zeta^{3t} \pmod{3}.$$

The congruence holds for any cubed sum of a sequence, and can be proved by induction. Now since $\chi_\pi(0) = 0$ and $\chi_\pi(t)^3 = 1$ for $t \neq 0$, we get

$$g(\chi_\pi)^3 \equiv \sum_{t=1}^{p-1} \zeta^{3t} = -1 \pmod{3},$$

because $\sum_{t=0}^{p-1} \zeta^{3t} = 0$. The corollary to Proposition 8.3.3 in [3] states that if $\chi$ is a cubic character, then $g(\chi)^3 = pJ(\chi,\chi)$. Thus

$$g(\chi_\pi)^3 = pJ(\chi_\pi,\chi_\pi) \equiv J(\chi_\pi,\chi_\pi) \pmod 3,$$

since $p \equiv 1 \pmod 3$. Additionally, $J(\chi_\pi,\chi_\pi)$ must be in $D$ since it is a sum of products of elements of $D$, so we get

$$J(\chi_\pi,\chi_\pi) \equiv -1 \pmod 3,$$

which is to say that $J(\chi_\pi,\chi_\pi)$ is primary. □

**Lemma 3.30** Let $\pi$ be a prime such that $N(\pi) \neq 3$ and $\alpha \in D$. Then

(i) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha^2) = \chi_\pi(\alpha)^2$,

(ii) $\overline{\chi_\pi(\alpha)} = \chi_{\bar\pi}(\bar\alpha)$.

*Proof* To prove (i), notice that $\chi_\pi(\alpha)$ is equal to 1, $\omega$ or $\omega^2$. The square of each of them is equal to its complex conjugate, and it follows that $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha^2) = \chi_\pi(\alpha)^2$ by Proposition 3.28.

For (ii), we have

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(\alpha) \pmod \pi.$$

So

$$\bar\alpha^{\frac{N(\pi)-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\bar\pi},$$

and since $N(\pi) = N(\bar\pi)$, we get the desired result

$$\overline{\chi_\pi(\alpha)} = \chi_{\bar\pi}(\bar\alpha). \square$$

**Corollary 3.31** If $n \in \mathbb{Z}$ and $q$ is a rational primary prime, then $\chi_q(n) = 1$.

*Proof* Any rational integer is equal to its complex conjugate, so

$$\chi_q(n) = \chi_{\bar q}(\bar n) = \overline{\chi_q(n)} = \chi_q(n)^2.$$

Since $\omega \neq \omega^2$ and $\omega^2 \neq \omega^4$, we must have $\chi_q(n) = 1$. □

**Lemma 3.32** $J(\chi_\pi,\chi_\pi) = \pi$.

*Proof* The corollary to Theorem 1 in Chapter 8 of [3] states that if $\chi$ and $\lambda$ are multiplicative characters such that $\chi$, $\lambda$ and $\chi\lambda$ are not equal to $\varepsilon$, where $\varepsilon$ is the multiplicative character such that $\varepsilon(x) = 1$ for all $x$, then $|J(\chi,\lambda)| = \sqrt{p}$. It follows that $|J(\chi_\pi,\chi_\pi)| = \sqrt{p}$, where $p = N(\pi) = \pi\bar\pi$. So

$$J(\chi_\pi,\chi_\pi)\overline{J(\chi_\pi,\chi_\pi)} = |J(\chi_\pi,\chi_\pi)|^2 = p = \pi\bar\pi.$$

Since $\pi$ and $\bar\pi$ are primes, $J(\chi_\pi,\chi_\pi) = \pi$ or $J(\chi_\pi,\chi_\pi) = \bar\pi$. By the definition of Jacobi sums,

$$J(\chi_\pi,\chi_\pi) = \sum_{x+y=1} \chi_\pi(x)\chi_\pi(y).$$

Since $x, y \in \mathbb{Z}_p$, it follows that

$$J(\chi_\pi, \chi_\pi) = \sum_{x=0}^{p-1} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x=0}^{p-1} x^{\frac{p-1}{3}} (1-x)^{\frac{p-1}{3}} \pmod{\pi}.$$

Set $f(x) = x^{\frac{p-1}{3}} (1-x)^{\frac{p-1}{3}}$. Since $\frac{p-1}{3}$ is an integer, $f(x)$ is a polynomial of the form $f(x) = a_k x^k + \cdots + xa_1 + a_0$, where $k = \frac{2}{3}(p-1)$ and $a_i \in \mathbb{Z}$ for $0 \leq i \leq k$. Thus

$$J(\chi_\pi, \chi_\pi) \equiv \sum_{x=0}^{p-1} f(x) = \sum_{x=0}^{p-1} a_k x^k + \cdots + a_0 = a_k \sum_{x=0}^{p-1} x^k + \cdots + a_1 \sum_{x=0}^{p-1} x + pa_0 \pmod{\pi}.$$

Let $g$ be a generator of $\mathbb{Z}_p^*$ and $0 < l < p-1$, then

$$\sum_{x=1}^{p-1} x^l \equiv \sum_{j=0}^{p-2} (g^j)^l \pmod{p}.$$

Multiplying by $1 - g^l$ gives the congruence

$$\left(1-g^l\right) \sum_{x=1}^{p-1} x^l \equiv \left(1-g^l\right) \sum_{j=0}^{p-2} (g^j)^l = 1 - g^{(p-1)l} \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Since $l$ is less than $p-1$ which is the order of $g$, $g^l \not\equiv 1$, so $1 - g^l \not\equiv 0 \pmod{p}$. It follows that

$$\sum_{x=1}^{p-1} x^l \equiv 0 \pmod{p},$$

for $1 \leq l \leq k$, and so we must have that $\sum f(x) \equiv 0 \pmod{p}$, or more specifically

$$J(\chi_\pi, \chi_\pi) \equiv \sum_{x=0}^{p-1} f(x) \equiv 0 \pmod{\pi}.$$

In other words, $\pi \mid J(\chi_\pi, \chi_\pi)$, and so $J(\chi_\pi, \chi_\pi) = \pi$. □

**Corollary 3.33** $g(\chi_\pi)^3 = p\pi$.

*Proof* By the corollary to Proposition 8.3.3 in [3],

$$g(\chi)^3 = pJ(\chi, \chi),$$

for any cubic character $\chi$. The result immediately follows from Lemma 3.32. □

We need one more lemma before we can prove the law of cubic reciprocity:

**Lemma 3.34** If $a$ is a non-zero integer and $\chi$ is a non-trivial multiplicative character, then

$$g_a(\chi) = \chi(a^{-1})g(\chi).$$

*Proof* By definition,

$$\chi(a)g_a(\chi) = \chi(a)\sum \chi(t)\zeta^{at} = \sum \chi(at)\zeta^{at} = g(\chi).$$

We multiply both sides by $\chi(a^{-1})$ and get

$$g_a(\chi) = \chi(a^{-1})g(\chi). \square$$

Now let us prove the law of cubic reciprocity.

*Proof of* Theorem 3.27 We have 3 different cases to consider:

(i) $\pi_1$ and $\pi_2$ are both rational,

(ii) $\pi_1$ is rational and $\pi_2$ is irrational,

(iii) or both $\pi_1$ and $\pi_2$ are irrational primes.

The first case follows immediately from Corollary 3.31 because if $\pi_1 = q_1$ and $\pi_2 = q_2$ are rational primes, then

$$\chi_{q_1}(q_2) = 1 = \chi_{q_2}(q_1).$$

To prove (ii), let $\pi_1 = q \equiv 2 \pmod 3$ and let $\pi_2 = \pi$, with norm $N(\pi) = p \equiv 1 \pmod 3$. By Corollary 3.33,

$$g(\chi_\pi)^3 = p\pi.$$

If we raise both sides to $\frac{q^2-1}{3}$, we get

$$g(\chi_\pi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}} \equiv \chi_q(p\pi) = \chi_q(p)\chi_q(\pi) \pmod q$$

since $N(q) = q^2$. By Corollary 3.31, $\chi_q(p) = 1$. Thus by multiplying both sides by $g(\chi_\pi)$, we obtain the congruence

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)g(\chi_\pi) \pmod q. \tag{2}$$

Let us look at $g(\chi_\pi)$, but first, let us look at a general case for any sum

$$S_k = \sum_{t=0}^{k} a_t,$$

for any sequence $\{a_t\}$. Assume that $S_k^q = \sum a_t^q$ for a prime integer $q$. Then

$$(S_{k+1})^q = (S_k + a_{k+1})^q \equiv S_k^q + a_{k+1}^q \pmod q.$$

The congruence follows from the binomial theorem. Now by assumption,

$$S_k^q + a_{k+1}^q \equiv \sum_{t=0}^{k} a_t^q + a_{k+1}^q = \sum_{t=0}^{k+1} a_t^q \pmod q.$$

Thus it follows by induction that

$$S_n^q \equiv \sum_{t=0}^{q} a_t^q \pmod q,$$

for any $n \geq 0$, since it is trivial for $n = 0$. We apply this result to $g(\chi_\pi)^{q^2}$ twice as follows.

$$g(\chi_\pi)^{q^2} = \left(\sum \chi_\pi(t)\zeta^t\right)^{q^2} \equiv \left(\sum \chi_\pi(t)^q \zeta^{qt}\right)^q \equiv \sum \chi_\pi(t)^{q^2}\zeta^{q^2 t} \pmod{q}.$$

Using the fact that $q$ is primary, i.e. $q^2 \equiv 1 \pmod 3$, and that the order of $\chi_\pi$ is 3, $\chi_\pi(t)^{q^2} = \chi_\pi(t)$. It follows that

$$g(\chi_\pi)^{q^2} \equiv \sum \chi_\pi(t)\zeta^{q^2 t} = g_{q^2}(\chi_\pi) \pmod{q}.$$

Using Lemma 3.34,

$$g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi)\chi_\pi(q^3) = \chi_\pi(q)g(\chi_\pi).$$

From (2) we get

$$\chi_q(\pi)g(\chi_\pi) \equiv g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \equiv \chi_\pi(q)g(\chi_\pi) \pmod{q}.$$

Proposition 8.2.2 in [3] states that if $\chi \neq \varepsilon$, then $|g(\chi)| = \sqrt{p}$. Squaring both sides for $\chi = \chi_\pi$, we get $g(\chi)\overline{g(\chi)} = p$, so by multiplying by $\overline{g(\chi_\pi)}$ on both sides, we get the congruence

$$\chi_q(\pi)p \equiv \chi_\pi(q)p \pmod{q}.$$

Cancelling $p$ we end up with

$$\chi_q(\pi) \equiv \chi_\pi(q) \pmod{q},$$

which implies

$$\chi_q(\pi) = \chi_\pi(q),$$

concluding the proof of (ii).

For case (iii), the proof is very similar to that of case (ii). Let $\pi_1$ and $\pi_2$ be irrational primary primes such that $N(\pi_1) = p_1 \equiv 1 \pmod 3$ and $N(\pi_2) = p_2 \equiv 1 \pmod 3$. Since $\pi_1$ and $p_1$ are primary, $\bar{\pi}_1$ must be primary too, because

$$2 \equiv 2p_1 = 2\pi_1\bar{\pi}_1 \equiv 4\bar{\pi}_1 \equiv \bar{\pi}_1 \pmod 3.$$

By Corollary 3.33,

$$g(\chi_{\bar{\pi}_1})^3 = p_1\bar{\pi}_1.$$

Raise both sides of the equation to $\frac{N(\pi_2-1)}{3}$ to get

$$g(\chi_{\bar{\pi}_1})^{p_2-1} = (p_1\bar{\pi}_1)^{\frac{N(\pi_2)-1}{3}} \equiv \chi_{\pi_2}(p_1\bar{\pi}_1) \pmod{\pi_2}.$$

Parallel to the previous case, multiply by $g(\chi_{\bar{\pi}_1})$ and we have

$$g(\chi_{\bar{\pi}_1})^{p_2} \equiv \chi_{\pi_2}(p_1\bar{\pi}_1)g(\chi_{\bar{\pi}_1}) \pmod{\pi_2}.$$

By the same argument as in (ii), we see that

$$g(\chi_{\bar{\pi}_1})^{p_2} \equiv g_{p_2}(\chi_{\bar{\pi}_1}) \pmod{\pi_2}.$$

Using Lemma 3.34 again,

$$g_{p_2}(\chi_{\bar{\pi}_1}) = \chi_{\bar{\pi}_1}(p_2^{-1})g(\chi_{\bar{\pi}_1}) = \chi_{\bar{\pi}_1}(p_2^2)g(\chi_{\bar{\pi}_1}).$$

Combining the congruence relations, we get

$$\chi_{\bar{\pi}_1}(p_2^2)g(\chi_{\bar{\pi}_1}) \equiv \chi_{\pi_2}(p_1\bar{\pi}_1)g(\chi_{\bar{\pi}_1}) \pmod{\pi_2}.$$

We multiply by $\overline{g(\chi_{\bar{\pi}_1})}$ and cancel $p_1$ on both sides so we get

$$\chi_{\bar{\pi}_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\bar{\pi}_1) \pmod{\pi_2},$$

implying that

$$\chi_{\bar{\pi}_1}(p_2^2) = \chi_{\pi_2}(p_1\bar{\pi}_1). \tag{3}$$

Starting with $g(\chi_{\pi_2}) = p_2\pi_2$ by Corollary 3.33, we can repeat the process to attain

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{4}$$

Finally, we get

$$\begin{aligned}
\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\bar{\pi}_1) &= \chi_{\pi_1}(\pi_2)\chi_{\bar{\pi}_1}(p_2^2) \\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2^4) \\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) \\
&= \chi_{\pi_1}(\pi_2 p_2) \\
&= \chi_{\pi_2}(p_1^2) \\
&= \chi_{\pi_2}(p_1\pi_1\bar{\pi}_1) \\
&= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\bar{\pi}_1),
\end{aligned}$$

by using (3) in the first equation, Lemma 3.30 in the second equation, Proposition 3.28 in the third equation and (4) in the fifth equation. By cancelling $\chi_{\pi_2}(p_1\bar{\pi}_1)$, we get

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1),$$

and we are done with the proof. □

# 4 Generalised Lucas–Lehmer Test

This section is based on [1], so unless otherwise specified, the proofs presented can be found in [1]. However, the author has added more details and arguments, that have been omitted in the source material, to make it easier for the reader to follow the presented proof.

## 4.1 Objective

We want to generalise the Lucas–Lehmer primality test to be used on integers $M = A \cdot 3^n \pm 1$, where $A$ is even and $3 \nmid A$. If $M = A \cdot 3^n + 1$, we need the extra condition $M \neq \left(\frac{A}{2} \pm 1\right)^2$. A final condition states that $\frac{A}{2} < 4 \cdot 3^n - 1$. Needless to say, the frequency of integers fulfilling these conditions is much greater than the frequency of the Mersenne numbers, which increase exponentially.

## 4.2 Preliminary

Before testing, one must choose a small rational prime $l$ such that $M$ is not a cube modulo $l$. By Corollary 3.31, $l \equiv 1 \pmod 3$, because if $l \equiv 2 \pmod 3$, then $l$ is prime in $D$, by Theorem 3.14, and so $\chi_l(M) = 1$. Thus $l$ splits, and $l = \pi\overline{\pi}$ for some prime $\pi$. Furthermore, we can choose $\pi$ to be primary by Theorem 3.20.

**Definition 4.1** Define $\tau$ such that

$$\tau\pi \equiv \overline{\pi} \pmod M. \tag{5}$$

$\tau$ is well-defined because $D$ is a Euclidean ring by Proposition 3.9, so the equation

$$\pi\xi_1 + M\xi_2 = \overline{\pi}$$

has a solution as $\pi$ and $M$ are relatively prime. If $\xi_1 = \tau$ and $\xi_2 = \alpha$ is a solution, then all solutions can be written as $\xi_1 = \tau + \beta M$ and $\xi_2 = \alpha - \beta\pi$ for all $\beta \in D$. Thus $\tau$ is unique modulo $M$.

**Proposition 4.2** $N(\tau) \equiv 1 \pmod M$.

*Proof* Taking the norm of (5), we get the congruence

$$N(\tau\pi) = N(\tau)N(\pi) \equiv N(\bar{\pi}) \pmod M,$$

and since $N(\pi) = N(\bar{\pi}) = l$ and $l \nmid M$, it follows that

$$N(\tau) \equiv 1 \pmod M. \ \square$$

The following lemma is partly found in [4], but generalised by the author to also work for $M = A \cdot 3^n + 1$, and not only $M = A \cdot 3^n - 1$ as presented in [4].

**Lemma 4.3** Let $M = A \cdot 3^n \pm 1$, where $A$ is even and $1 \leq \frac{A}{2} < 4 \cdot 3^n - 1$, and assume that if $M = A \cdot 3^n + 1$, then $M \neq \left(\frac{A}{2} \pm 1\right)^2$. Also assume that $3 \nmid A$. Then if all prime divisors of $M$ are of the form $k \cdot 3^n \pm 1$, then $M$ is prime.

*Proof* The smallest possible prime divisor of $M$ is $2 \cdot 3^n - 1$. Now

$$(2 \cdot 3^n - 1)^3 = 8 \cdot 3^{3n} - 12 \cdot 3^{2n} + 6 \cdot 3^n - 1,$$

and it follows from $1 \leq \frac{A}{2} < 4 \cdot 3^n - 1$ that

$$M = A \cdot 3^n \pm 1 < 2\left(4 \cdot 3^n - 1\right)3^n + 1 = 8 \cdot 3^{2n} - 2 \cdot 3^n + 1.$$

So

$$\begin{aligned}(2 \cdot 3^n - 1)^3 - M &> 8 \cdot 3^{3n} - 12 \cdot 3^{2n} + 6 \cdot 3^n - 1 - \left(8 \cdot 3^{2n} - 2 \cdot 3^n + 1\right) \\ &= 8 \cdot 3^{3n} - 20 \cdot 3^{2n} + 8 \cdot 3^n - 2 \\ &= 4 \cdot 3^{2n}\left(2 \cdot 3^n - 5\right) + 8 \cdot 3^n - 2 > 0.\end{aligned}$$

Consequently, $M$ can at most have two prime divisors.

We begin by treating the case where $M = A \cdot 3^n - 1$. Assume that $q = 2 \cdot 3^n - 1$ divides $M$. We then have

$$A \cdot 3^n - 1 \equiv 0 \pmod{q},$$

or equivalently

$$A \cdot 3^n \equiv 1 \pmod{q}.$$

We get

$$\frac{A}{2} - 1 \equiv \frac{A}{2} - A \cdot 3^n = -\frac{A}{2}(2 \cdot 3^n - 1) \equiv 0 \pmod{q},$$

i.e. $\frac{A}{2} - 1 = mq$ for some integer $m$. If $m = 1$,

$$\frac{A}{2} - 1 = 2 \cdot 3^n - 1,$$

but then $A = 4 \cdot 3^n$ which contradicts $3 \nmid A$. Thus $m \geq 2$, but then

$$\frac{A}{2} = mq + 1 \geq 2(2 \cdot 3^n - 1) + 1 = 4 \cdot 3^n - 1,$$

but $\frac{A}{2} < 4 \cdot 3^n - 1$, so $q \neq 2 \cdot 3^n - 1$. If $q = 2 \cdot 3^n + 1$, we get

$$\frac{A}{2} + 1 \equiv \frac{A}{2} + A \cdot 3^n = \frac{A}{2} q \equiv 0 \pmod{q}.$$

So $\frac{A}{2} + 1 = mq = m(2 \cdot 3^n + 1)$. By the same argument as before, it follows that $m \geq 2$. But again it leads to the contradiction $\frac{A}{2} \geq 4 \cdot 3^n - 1$. Thus we can conclude that any prime divisor must be of the form $q = k \cdot 3^n \pm 1$ where $k \geq 4$. If we assume that $M$ is not prime, $M$ must have two prime divisors we call $q_1$ and $q_2$. Now if both divisors are of the form $k \cdot 3^n + 1$ or both are of the form $k \cdot 3^n - 1$, then

$$M = q_1 q_2 = (k_1 \cdot 3^n \pm 1)(k_2 \cdot 3^n \pm 1) = k_1 k_2 \cdot 3^{2n} \pm k_1 \cdot 3^n \pm k_2 \cdot 3^n + 1 \equiv 1 \pmod{3},$$

but by assumption, $M = A \cdot 3^n - 1 \equiv -1 \pmod{3}$, so this cannot be the case. Thus,

$$A \cdot 3^n - 1 = M = q_1 q_2 = (k_1 \cdot 3^n + 1)(k_2 \cdot 3^n - 1) \geq (4 \cdot 3^n + 1)(4 \cdot 3^n - 1) = 16 \cdot 3^{2n} - 1.$$

By cancelling $-1$ and dividing by $2 \cdot 3^n$ on both sides we get

$$\frac{A}{2} \geq 8 \cdot 3^n > 4 \cdot 3^n - 1.$$

We conclude that $M$ cannot have two prime divisors and so $M$ must be prime.

Now let $M = A \cdot 3^n + 1$. Then $M \equiv 1 \pmod{3}$, so if $M$ has two prime divisors, $q_1$ and $q_2$, we must have $q_1 = k_1 \cdot 3^n + 1$ and $q_2 = k_2 \cdot 3^n + 1$, or $q_1 = k_1 \cdot 3^n - 1$ and $q_2 = k_2 \cdot 3^n - 1$. In the first case, the smallest possible divisor is $q = 2 \cdot 3^n + 1$. If $q_1 = q_2 = 2 \cdot 3^n + 1$, then

$$M = (2 \cdot 3^n + 1)^2 = 4 \cdot 3^{2n} + 4 \cdot 3^n + 1 = 2 \cdot (2 \cdot 3^n + 2)\, 3^n + 1.$$

Then $\frac{A}{2} = 2 \cdot 3^n + 2$, but if so,

$$M = (2 \cdot 3^n + 1)^2 = \left(\frac{A}{2} - 1\right)^2,$$

which contradicts that $M \neq \left(\frac{A}{2} \pm 1\right)^2$. Thus at least one prime divisor must be greater than or equal to $4 \cdot 3^n + 1$. Therefore,

$$M \geq (2 \cdot 3^n + 1)(4 \cdot 3^n + 1) = 8 \cdot 3^{2n} + 6 \cdot 3^n + 1 > 8 \cdot 3^{2n} - 2 \cdot 3^n + 1,$$

which is a contradiction. Thus we know that unless $M$ is prime,

$$M = (k_1 \cdot 3^n - 1)(k_2 \cdot 3^n - 1).$$

If $q = 2 \cdot 3^n - 1$ divides $M$, then $M = A \cdot 3^n + 1 \equiv 0 \pmod{q}$, or equivalently,

$$A \cdot 3^n \equiv -1 \pmod{q}.$$

It follows that

$$\frac{A}{2} + 1 \equiv \frac{A}{2} - A \cdot 3^n = -\frac{A}{2} q \equiv 0 \pmod{q}.$$

Thus $\frac{A}{2} = mq - 1 = m(2 \cdot 3^n - 1) - 1$, for some integer $m$. If $m = 1$, we get $\frac{A}{2} = 2 \cdot 3^n - 2$, and

$$\begin{aligned} M &= A \cdot 3^n + 1 = 2(2 \cdot 3^n - 2)3^n + 1 \\ &= 4 \cdot 3^{2n} - 4 \cdot 3^n + 1 = (2 \cdot 3^n - 1)^2 \\ &= \left(\frac{A}{2} + 1\right)^2, \end{aligned}$$

which is another contradiction. If $m = 2$, then

$$\frac{A}{2} = 2(2 \cdot 3^n - 1) - 1 = 4 \cdot 3^n - 3,$$

but 3 does not divide $A$, so we get yet another contradiction. Thus $m \geq 3$. If $n = 0$, $q = 2 \cdot 3^0 - 1 = 1$, but $q$ is prime, so $n > 0$. It follows that

$$\frac{A}{2} \geq 3(2 \cdot 3^n - 1) - 1 = 6 \cdot 3^n - 4,$$

and

$$6 \cdot 3^n - 4 - (4 \cdot 3^n - 1) = 2 \cdot 3^n - 3 \geq 2 \cdot 3 - 3 = 3 > 0.$$

However, this gives the contradiction

$$\frac{A}{2} \geq 6 \cdot 3^n - 4 > 4 \cdot 3^n - 1,$$

so $q = 2 \cdot 3^n - 1$ cannot be a divisor of $M$. It follows that $M$ must be prime, unless

$$M = (k_1 \cdot 3^n - 1)(k_2 \cdot 3^n - 1),$$

where $k_1, k_2 \geq 4$. In the latter case,

$$\begin{aligned} M &\geq (4 \cdot 3^n - 1)^2 = 16 \cdot 3^{2n} - 8 \cdot 3^n + 1 \\ &> 8 \cdot 3^{2n} + 1 > 8 \cdot 3^{2n} - 2 \cdot 3^n + 1, \end{aligned}$$

but this is a contradiction and therefore $M$ must be prime. □

**Definition 4.4** For $\alpha \in D$, consider the linear transformation $F : D \mapsto D$ defined by $F(\xi) = \alpha\xi$. The trace of $\alpha$ is the trace of $F$, which subsequently is the trace of the matrix $A$ of $F$ with respect to any basis for $D$, where the trace of the matrix $A$ is defined as the sum of the elements of the main diagonal of $A$. We denote the trace of $\alpha$ by $\mathrm{Tr}\,(\alpha)$.

**Proposition 4.5** If $\alpha = a + b\omega$, then $\mathrm{Tr}\,(\alpha) = 2a - b$.

*Proof* Since one can choose any basis for $D$, we choose the basis to be 1, $\omega$. If $\alpha = a + b\omega$,

$$\begin{aligned} F(1) &= \alpha = a + b\omega, \\ F(\omega) &= \alpha\omega = a\omega + b\omega^2 = -b + (a - b)\,\omega. \end{aligned}$$

Thus the matrix $A$ becomes

$$A = \begin{bmatrix} a & -b \\ b & a - b \end{bmatrix} = aI + bJ,$$

where $I$ is the identity matrix and

$$J = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

It follows that $\mathrm{Tr}\,(\alpha) = \mathrm{Tr}\,(A) = 2a - b$. □

The next lemma was only stated as a fact in [1], but a proof was never provided. Thus the following proof was found independently of the source material.

**Lemma 4.6** Let $M$, $A$ and $\tau$ be as in Sections 4.1 and 4.2 and define the sequence $\{Q_k\}$ recursively by

$$Q_0 = \mathrm{Tr}\,(\tau^A);\ Q_{k+1} = Q_k^2\,(Q_k - 3)\,.$$

Then $Q_k \equiv \mathrm{Tr}\,(\tau^{A\cdot 3^k}) \pmod{M}$ for all $k$.

*Proof* Let $\sigma = \tau^{A\cdot 3^k}$, and assume that $\sigma = a + b\omega$. Set $S_k = \mathrm{Tr}\,(\sigma)$. We want to prove that $S_k \equiv Q_k \pmod{M}$. From the definition of $\sigma$ and $S_k$, we have $S_{k+1} = \mathrm{Tr}\,(\sigma^3)$. Since $N(\tau) \equiv 1 \pmod{M}$ by Proposition 4.2, we get

$$N(\sigma) = N\left(\tau^{A\cdot 3^k}\right) = (N(\tau))^{A\cdot 3^k} \equiv 1^{A\cdot 3^k} = 1 \pmod{M}.$$

As in Definition 4.4, let $F(\xi) = \sigma\xi$, and $B$ be the matrix of $F$ with respect to the basis 1, $\omega$. It follows that $B = aI + bJ$ as before, and

$$S_k = \mathrm{Tr}\,(\sigma) = \mathrm{Tr}\,(B) = 2a - b,$$

by Proposition 4.5. We get

$$S_k = 1 \cdot S_k \equiv N(\sigma)S_k = (a^2 - ab + b^2)(2a - b) = 2a^3 - 3a^2b + 3ab^2 - b^3 \pmod{M}, \quad (6)$$

and

$$S_k^3 = (2a - b)^3 = 8a^3 - 12a^2b + 6ab^2 - b^3.$$

Looking at the linear transformation $G : D \mapsto D$ defined as $G(\xi) = \sigma^3\xi$, we have $G = F\circ F\circ F$, thus its matrix is

$$B^3 = (aI + bJ)^3 = a^3I + 3a^2bJ + 3ab^2J^2 + b^3J^3 = a^3I + 3a^2bJ + 3ab^2\begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix} + b^3I.$$

Consequently,

$$S_{k+1} = \mathrm{Tr}\,(\sigma^3) = \mathrm{Tr}\,(B^3) = 2a^3 - 3a^2b - 3ab^2 + 2b^3. \tag{7}$$

By (6) and (7),

$$\begin{aligned} S_{k+1} + 3S_k &\equiv 2a^3 - 3a^2b - 3ab^2 + b^3 + 3\left(2a^3 - 3a^2b + 3ab^2 - b^3\right)\\ &= 8a^3 - 12a^2b + 6ab^2 - b^3 = S_k^3 \pmod M. \end{aligned}$$

Thus we have shown that $S_{k+1} \equiv S_k^2(S_k - 3) \pmod M$. So if $S_k \equiv Q_k \pmod M$, it follows that

$$S_{k+1} \equiv S_k^2(S_k - 3) \equiv Q_k^2(Q_k - 3) = Q_{k+1} \pmod M.$$

Since $S_0 = \mathrm{Tr}\,(\tau^{A\cdot 3^0}) = \mathrm{Tr}\,(\tau^A) = Q_0$, it follows by induction that $S_k \equiv Q_k \pmod M$, and we are done. □

## 4.3 Generalised Lucas–Lehmer

**Theorem 4.7** Let $M = A\cdot 3^n \pm 1$ where $A$ is an even integer and $3 \nmid A$. If $M = A\cdot 3 + 1$, assume that $M \neq \left(\frac{A}{2} \pm 1\right)^2$. Further assume that $\frac{A}{2} < 4\cdot 3^n - 1$. If $\{Q_k\}$ is defined by

$$Q_0 = \mathrm{Tr}\,(\tau^A); \quad Q_{k+1} = Q_k^2(Q_k - 3),$$

then $M$ is prime if and only if $Q_{n-1} \equiv -1 \pmod M$.

*Proof* We shall prove it for $M = A\cdot 3^n - 1$ first. Assume that $M$ is prime. Since $M$ is not a cube modulo $l = N(\pi)$, $M$ is not a cube in $\mathbb{Z}_l$. Since one can identify $\mathbb{Z}_l$ with $D/\pi D$, $M$ cannot be a cube modulo $\pi$ either, i.e. $\chi_\pi(M) = \omega^i$ for $i = 1$ or 2. Since we have assumed that $M = A\cdot 3^n - 1 \equiv 2 \pmod 3$, $M$ is primary. By construction, so is $\pi$. Furthermore, $M^2 \neq l$ because $l$ is a rational prime, hence $N(\pi) = l \neq M^2 = N(M)$. It is just as easily argued that $N(\pi) \neq 3$ and $N(M) \neq 3$. Thus it is permissible to use the law of cubic reciprocity. We get

$$\chi_M(\pi) = \chi_\pi(M) = \omega^i.$$

It follows that

$$\pi^{\frac{M^2-1}{3}} \equiv \omega^i \pmod M,$$

or

$$\left(\pi^{M-1}\right)^{\frac{M+1}{3}} \equiv \omega^i \pmod M. \tag{8}$$

By the definition of $\tau$,

$$\tau\pi \equiv \bar\pi \pmod M.$$

But $\bar{\pi} \equiv \pi^M \pmod{M}$, because

$$\pi^M = (a+b\omega)^M = \sum_{k=0}^{M} \binom{M}{k} a^{M-k} b^k \omega^k \equiv a^M + b^M \omega^M \equiv a + b\omega^2 = \bar{\pi} \pmod{M}.$$

So $\tau\pi \equiv \pi^M \pmod{M}$, and since $M$ is prime, we can cancel $\pi$ on both sides and we get $\tau \equiv \pi^{M-1} \pmod{M}$. Inserting this into (8) we get

$$\tau^{\frac{M+1}{3}} \equiv \omega^i \pmod{M}.$$

From Proposition 4.5 we have $\operatorname{Tr}(\omega) = 2 \cdot 0 - 1 = -1$ and $\operatorname{Tr}(\omega^2) = 2 \cdot (-1) - (-1) = -1$, and by taking the trace of both sides of the congruence we get

$$\operatorname{Tr}(\tau^{\frac{M+1}{3}}) = \operatorname{Tr}(\tau^{A \cdot 3^{n-1}}) \equiv \operatorname{Tr}(\omega^i) = -1 \pmod{M}.$$

By Lemma 4.6, it follows that

$$Q_n \equiv \operatorname{Tr}(\tau^{A \cdot 3^{n-1}}) \equiv -1 \pmod{M},$$

and we are done.

To prove the converse, let $Q_{n-1} \equiv -1 \pmod{M}$. Suppose $M$ is not prime, and $q$ is a prime divisor of $M$. If $q \equiv 1 \pmod 3$, there exists a $\delta \in D$ such that $N(\delta) = \delta\bar{\delta} = q$. Otherwise, $q$ is primary since $M \equiv -1 \pmod 3$. If this is the case, $q$ is prime in $D$, so we set $\delta = q$. In either case, $\delta \mid M$, and it follows from our assumption that

$$Q_{n-1} \equiv -1 \pmod{\delta}.$$

From Proposition 4.2 we have that $N(\tau) \equiv 1 \pmod{M}$, and since $\delta$ divides $M$, it follows that $N(\tau^{A \cdot 3^{n-1}}) \equiv 1 \pmod{\delta}$. Assuming that $\tau^{A \cdot 3^{n-1}} = a + b\omega$ then gives us the congruences

$$\begin{aligned} N(\tau^{A \cdot 3^{n-1}}) &= a^2 - ab + b^2 \equiv 1 \pmod{\delta}, \\ Q_{n-1} = \operatorname{Tr}(\tau^{A \cdot 3^{n-1}}) &= 2a - b \equiv -1 \pmod{\delta}. \end{aligned}$$

The latter congruence implies $b \equiv 2a + 1 \pmod{\delta}$. Inserting this into the first congruence, we get

$$N(\tau^{A \cdot 3^{n-1}}) \equiv a^2 - a(2a+1) + (2a+1)^2 = 3a^2 + 3a + 1 \equiv 1 \pmod{\delta}.$$

Consequently, $3a(a+1) \equiv 0 \pmod{\delta}$. Since $\delta \nmid 3$, it we must have

$$a \equiv 0 \pmod{\delta} \quad \text{or} \quad a \equiv -1 \pmod{\delta}.$$

By the congruence $b \equiv 2a + 1 \pmod{\delta}$, it follows that $b \equiv 1 \pmod{\delta}$ or $b \equiv -1 \pmod{\delta}$. Thus either

$$\tau^{A \cdot 3^{n-1}} \equiv 0 + 1 \cdot \omega = \omega \pmod{\delta} \quad \text{or} \quad \tau^{A \cdot 3^{n-1}} \equiv -1 + (-1)\omega = \omega^2 \pmod{\delta}.$$

We write $\tau^{A \cdot 3^{n-1}} \equiv \omega^i$, where $i = 1$ or 2. It follows that

$$(\tau^A)^{3^n} = (\tau^{A \cdot 3^{n-1}})^3 \equiv (\omega^i)^3 = 1 \pmod{\delta}.$$

Thus the order of $\tau^A$ must be a power of 3, but since $(\tau^A)^{3^{n-1}} \equiv \omega^i \pmod{\delta}$, $\tau^A$ must have order $3^n$ in the group $(D/\delta D)^*$. The order of $(D/\delta D)^*$ is $N(\delta)-1$, i.e. $q-1$ or $q^2-1$ depending on whether $q$ is primary or not. As the order of $\tau^A$ must divide the order of $(D/\delta D)^*$ and $q^2-1 = (q+1)(q-1)$, we must have

$$3^n \mid q+1 \quad \text{or} \quad 3^n \mid q-1.$$

Meaning that $q+1 = k \cdot 3^n$ or $q-1 = k \cdot 3^n$. In other words, any prime divisor of $M$ can be written as

$$q = k \cdot 3^n \pm 1.$$

Thus it follows by Lemma 4.3 that $M$ is prime.

For the case when $M = A \cdot 3^n + 1$, the proof mainly follows the proof of Theorem 2 in [2], and can deviate somewhat from the original proof in [1]. In this case, $M \equiv 1 \pmod 3$, so $M$ splits in $D$. Define $\theta \in D$ as the primary prime such that

$$M = \theta\bar{\theta}.$$

An alternative notation to $\tau$ is

$$\tau \equiv \bar{\pi}\pi^{-1} \pmod{M}.$$

It follows that

$$\bar{\tau} \equiv \pi\bar{\pi}^{-1} \equiv \tau^{-1} \pmod{M}.$$

Let $j, k \in \{0, 1, 2\}$ such that

$$\chi_\theta(\pi) \equiv \pi^{\frac{M-1}{3}} \equiv \omega^j \pmod{\theta},$$

and

$$\chi_\theta(\bar{\pi}) \equiv \bar{\pi}^{\frac{M-1}{3}} \equiv \omega^k \pmod{\theta}.$$

We get

$$\bar{\tau}^{\frac{M-1}{3}} \equiv \pi^{\frac{M-1}{3}}\bar{\pi}^{-\frac{M-1}{3}} \equiv \omega^{j-k} \pmod{\theta}. \tag{9}$$

Taking the complex conjugate it follows that

$$\tau^{\frac{M-1}{3}} \equiv \bar{\omega}^{j-k} \pmod{\bar{\theta}},$$

which is the same as saying

$$\bar{\tau}^{-\frac{M-1}{3}} \equiv \omega^{-(j-k)} \pmod{\bar{\theta}},$$

because $\bar{\omega} = \omega^{-1}$ by Proposition 3.2, or equivalently

$$\bar{\tau}^{\frac{M-1}{3}} \equiv \omega^{j-k} \pmod{\bar{\theta}}. \tag{10}$$

Now since $\theta$ and $\bar{\theta}$ are relatively prime, we can combine (9) and (10) to get

$$\bar{\tau}^{\frac{M-1}{3}} \equiv \omega^i \pmod{M},$$

where $i \in \{0, 1, 2\}$. However we want to show that $i \neq 0$.

If $\pi^{\frac{M-1}{3}} \equiv 1 \pmod{M}$, then the same congruence holds modulo $\theta$ and $\bar{\theta}$ because $M = \theta\bar{\theta}$. It follows that

$$\chi_\theta(\pi) = \chi_{\bar{\theta}}(\pi) = 1,$$

and so $\chi_\theta(\pi)\chi_{\bar{\theta}}(\pi) = 1$. Using the law of cubic reciprocity we get the following

$$1 = \chi_\theta(\pi)\chi_{\bar{\theta}}(\pi) = \chi_\pi(\theta)\chi_\pi(\bar{\theta}) = \chi_\pi(\theta\bar{\theta}) = \chi_\pi(M).$$

But this is a contradiction because $M$ is not a cube modulo $l$, and by extension not a cube modulo $\pi$. Thus

$$\pi^{\frac{M-1}{3}} \equiv \omega^i \pmod{M},$$

for some $i \in \{1, 2\}$. The conjugate gives

$$\bar{\pi}^{\frac{M-1}{3}} \equiv \omega^{-i} \pmod{M}.$$

Thus

$$\bar{\tau}^{\frac{M-1}{3}} \equiv \left(\pi\bar{\pi}^{-1}\right)^{\frac{M-1}{3}} = \pi^{\frac{M-1}{3}}\bar{\pi}^{-\frac{M-1}{3}} \equiv \omega^{2i} = \omega \text{ or } \omega^2 \pmod{M}.$$

Finally, by noticing that

$$\bar{\tau}^{\frac{M-1}{3}} \equiv \tau^{-\frac{M-1}{3}} = \tau^{\frac{1-M}{3}} = \tau^{\frac{1-\left(A\cdot 3^n+1\right)}{3}} = \tau^{A\cdot 3^{n-1}} \pmod{M},$$

we get the desired result

$$Q_{n-1} = \mathrm{Tr}\left(\tau^{A\cdot 3^{n-1}}\right) \equiv \mathrm{Tr}\left(\bar{\tau}^{\frac{M-1}{3}}\right) \equiv \mathrm{Tr}\left(\omega^i\right) = -1 \pmod{M},$$

for some $i \in \{1, 2\}$.

The converse follows the exact procedure as that of the case when $M = A \cdot 3^n - 1$. □

# References

[1] Berrizbeita, P. and Berry, T. G., *Cubic Reciprocity and Generalised Lucas–Lehmer Tests for Primality of* $A.3n \pm 1$, Proceedings of the American Mathematical Society, Vol. 127, No. 7 (1999)

[2] Guthmann, A., *Effective Primality Tests for Integers of the Forms* $N = k^3n + 1$ *and* $N = k2^m3^n + 1$, BIT 32, 529–534 (1992)

[3] Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory* (2nd ed.), Springer (1990)

[4] Williams, H. C., *The Primality of* $N = 2A3^n - 1$, Canad. Math. Bull., Vol. 15 No. 4 (1972)

Bachelor's Theses in Mathematical Sciences 2022:K15
ISSN 1654-6229

LUNFMA-4137-2022

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lu.se/