university of groningen

faculty of science and engineering

mathematics and applied mathematics

Probable primality testing for Wagstaff primes

Bachelor's Project Mathematics

July 2024

Student: D.G. Sikkema

First supervisor: Prof.dr. J. Top

Second assessor: Prof.dr. P. Kilicer

Abstract

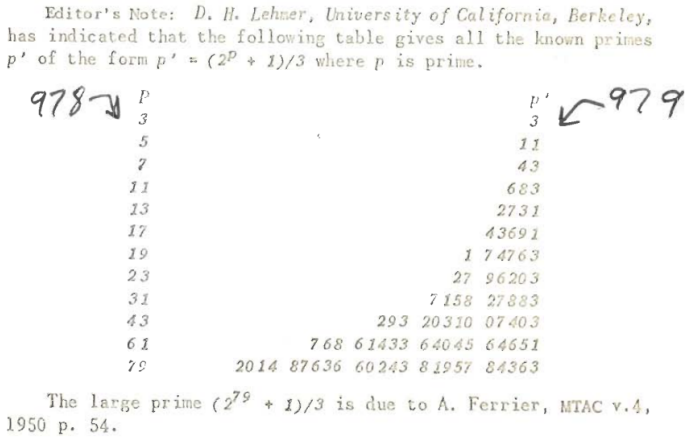
This thesis describes multiple probable prime tests specifically designed for Wagstaff numbers. Wagstaff numbers are of the form $W_n = \frac{2^n+1}{3}$ where n is an odd positive integer. Several properties of Wagstaff numbers are covered and proven. Which allow to describe and prove multiple probable prime tests. A proof of the Lifschitz test is presented and analyzed, which is a derivation of Miller's test. After which a discussion and proof of a generalized probable prime test based on Lucas-Lehmer recurrences is given. Case distinctions of this generalized test are the Anton Vrba test and Robert Gerbicz test. In terms of speed, the Lifschitz test outperforms the Vrba and Gerbicz test. However, these latter two tests provide some insights into finding a prime test that works in both directions. The theory used to prove these tests allows to determine primality for "smaller" Wagstaff numbers in a fairly straightforward manner, which is demonstrated in multiple examples. Finally an argument is given on why an attempted proof on whether there exist infinitely many Wagstaff primes is incorrect.

Contents

1 Introduction

This thesis describes multiple probable prime tests specifically designed for Wagstaff numbers. Wagstaff numbers[12] are of the form $W_n = \frac{2^n+1}{3}$ where n is an odd positive integer e.g. $W_3 = 3, W_5 = 11$ and $W_7 = 43$. The largest known probable Wagstaff prime at this moment is $W_{15135397}$[11], which has over 4.5 million digits. As of today no efficient test exists that states: W_n is prime if and only if this specific condition is satisfied. Determining whether for example $W_{15135397}$ is prime relies on factorization, which is something one wants to avoid given the size. Hence it is of importance to understand what exactly Wagstaff numbers are, what their properties are and how the probable prime tests work. This information may perhaps lay the foundation of finding a test that does not involve factorizations.

Wagstaff numbers are closely related to Mersenne numbers given that $3W_n - 2 = M_n = 2^n - 1$. They are named after S.S. Wagstaff who in collaboration with colleagues used them in their New Mersenne Conjecture[1]. However, Wagstaff numbers have been studied before by both E. Lucas[6] and D.H. Lehmer. In 1954 Lehmer[5] published a table of all known Wagstaff primes till that date.



Editor's Note: D. H. Lehmer, University of California, Berkeley, has indicated that the following table gives all the known primes p' of the form $p' = (2^p + 1)/3$ where p is prime.

p	p'
3	3
5	11
7	43
11	683
13	2731
17	43691
19	1 74763
23	27 96203
31	7158 27883
43	293 20310 07403
61	768 61433 64045 64651
79	2014 87636 60243 81957 84363

The large prime $(2^{79} + 1)/3$ is due to A. Ferrier, MTAC v.4, 1950 p. 54.

Figure 1: Table of known Wagstaff primes up till 1954

The largest known Wagstaff prime in 1954 was $\frac{2^{79}+1}{3}$, which was proven by A.Ferrier[5]. Back then solving this was a complicated task given that most people did not own computers. Nowadays factorizing $2^{79} + 1$ can be done on most modern laptops.

In the text published by Lehmer, two results from E. Lucas were mentioned that are related to Wagstaff numbers. The first result is:

Theorem 1.1. *If $n \in \mathbb{N}$ and $2n+1$ are prime and $n \equiv 1 \pmod 4$. Then $2^n + 1 \equiv 0 \pmod{2n+1}$.*

In chapter 3 it is shown that $2^n + 1$ is divisible by 3 for any odd integer. Hence this Theorem tells us if all assumptions are met regarding n, that $2^n + 1 = 3(2n+1)k$ for some natural number k. Now $k > 1$ automatically implies that W_n is composite. $k = 1$ however implies that $2^n + 1 = 6n + 3$ and these functions intersect at $n = 5$. Hence we get that $W_n = 11$. The main function of this Theorem is to quickly show that W_n has to have some divisor given some prime $n \neq 5$.

For example take $n = 29$. Then $n \equiv 1 \pmod 4$ and $2n + 1 = 59$ is also prime. Then $2^{29} + 1 = 3 \cdot 59 \cdot k$ for some $k \in \mathbb{N}$. This quickly shows that W_{29} is not prime given that $2^{29} + 1 > 3 \cdot 59$.

This works no matter the size, take for example $n = 953$ and $2n + 1 = 1907$. Checking whether $\frac{2^{953}+1}{3}$ is prime in a naive way might seem impossible. But Theorem 1.1 quickly shows that $2^{953} + 1 > 3 \cdot 1907$, hence W_{953} has to be composite.

The second result mentioned in the text by Lehmer is:

Theorem 1.2. *If $n \in \mathbb{N}$ and $6n+1$ are prime and in the unique decomposition $6n + 1 = 4L^2 + 3M^2$, L and M are multiples of 2 and 3 respectively. Then $2^n + 1 \equiv 0 \pmod{6n+1}$.*

This Theorem has the same function as Theorem 1.1, namely ruling out that W_n is prime. If all assumptions are met on n and $6n+1$, then $3(6n+1)k = 2^n+1$ for some $k \in \mathbb{N}$. $k > 1$ automatically implies that W_n is not prime. The case where $k = 1$ gives $2^n + 1 = 18n + 3$. These functions intersect at $n = 7$, hence these criteria are only met for $W_7 = 43$. Consider the following counter examples.

Let $n = 367$, then $6n+1 = 2203$. Both are prime. Note that $2203 = 16+2187 = 4(2)^2 + 3(3^2)^2$. So $n = 367$ satisfies all criteria of Theorem 1.2. But one quickly sees that $2^{367} + 1 > 2203$, hence W_{367} has to be composite.

Another example is $n = 6011$ with $6n + 1 = 36067$. Both are prime and $36067 = 16384 + 19683 = 4(2^6)^2 + 3(3^4)^2$. Hence n satisfies all assumptions. $2^{6011} + 1 > 36067$ then shows that W_{6011} is not prime.

Even though the Wagstaff primes were not of main interest, they did arise when both Lehmer and Lucas were working on Mersenne primes. Hence it is of no surprise that multiple probable prime tests for Wagstaff numbers are based on so called Lucas-Lehmer recurrences of the form $S_n = S_{n-1}^2 - 2$. Named after the recurrences used in the Lucas-Lehmer test[2]. The beauty of the Lucas-Lehmer test is the fact that it works in both directions, something that we would like to achieve for Wagstaff numbers as well. Now what is interesting is that none of the probable prime tests based on Lucas-Lehmer recurrences that are described throughout this thesis, have shown a counter-example of them not working both ways. Hence they very well might.

In chapter two theory about Legendre symbols and their properties is covered. These Legendre symbols are extensively used throughout this thesis to prove multiple Theorem's and properties, however this chapter can be skipped if the reader is already familiar with Legendre symbols. In chapter three Wagstaff numbers and their properties are described. Then in chapter four general probable prime tests that work for all integers are discussed and a slightly modified version of Miller's[8] test is presented. Chapter five is then dedicated to probable prime tests based on Lucas-Lehmer recurrences. Two examples of such tests are the Anton Vrba[16] test and the Robert Gerbicz[4] test. In chapter five a proof is presented of a generalized test of which the Vrba and Gerbicz test are case distinctions. This generalization allows one to construct new tests, which is demonstrated. Ideally one wants these tests to work in both directions. The analysis done in the previous chapters allows to touch upon this subject in section 5.2. The final chapter presents an attempted proof of whether there exist infinitely many primes argues why it is incorrect.

2 Quadratic residues

Throughout this text multiple proofs that involve quadratic residues are presented. Quadratic residues contain useful properties that are essential for number theoretic purposes and allow us to provide proofs in a straightforward manner. In this section the necessary Definitions and Theorems involving quadratic residues needed to comprehend this text are given. Proofs of these Theorems can be found in the textbook by Rosen[9]. It contains excellent examples and well-explained proofs.

Definition 2.1. *If m is a positive integer, we say that an integer a is a quadratic residue of m if (a,m) = 1 and the congruence* $x^2 \equiv a \pmod{m}$ *has a solution. If the congruence has no solution, we say that a is a quadratic non-residue of m.*

If we evaluate quadratic residues over a prime p then we know the exact number of quadratic residues and non-residues.

Theorem 2.1. *If p is an odd prime, then there are exactly* $\frac{p-1}{2}$ *quadratic residues of p and* $\frac{p-1}{2}$ *quadratic non-residues of p among the integers* $\{1, 2, ..., p-1\}$.

Evaluating quadratic residues of a prime p gives rise to the Legendre symbol.

Definition 2.2. *Let p be an odd prime and a an integer not divisible by p. Then the Legendre symbol* $\left(\frac{a}{p}\right)$ *is defined by*

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

The Legendre symbol allows us to simplify expressions modulo a prime. The next criterion is an example that helps to determine if an integer is composite or not.

Theorem 2.2. *Euler's Criterion. Let p be an odd prime and let a be an integer not divisible by p. Then* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Calculations with Legendre symbols are quite straightforward as the following Theorem will show.

Theorem 2.3. *Let p be an odd prime and a and b be integers not divisible by p. Then*

1. *if* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;
3. $\left(\frac{a^2}{p}\right) = 1$.

The main result of Quadratic residues is the Law of Quadratic Reciprocity. It allows us to flip the numerator and denominator inside the Legendre symbol, given some conditions. This allows us to evaluate the Legendre symbols of large numbers fairly easily.

Theorem 2.4. *The Law of Quadratic Reciprocity. Let p and q be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Consequently we have that*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \pmod 4 \text{ or } q = 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases} \tag{2}$$

Using property 2 of Theorem 2.3 often results in evaluating $\left(\frac{-1}{p}\right)$ or $\left(\frac{2}{p}\right)$ for a prime p. These Legendre symbols can be evaluated by using the following two Theorems:

Theorem 2.5. *If p is an odd prime, then*

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

Theorem 2.6. *If p is an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Hence, 2 is a quadratic residue of all primes $p \pm 1 \pmod 8$ and 2 is a quadratic non-residue of all primes $p \pm 3 \pmod 8$.*

3 Wagstaff numbers and their properties

To understand primality tests involving Wagstaff numbers means to first understand Wagstaff numbers themselves. In this section important properties of Wagstaff numbers are presented. An acknowledgement is in order for Piet van Eeghen [15] as this section is largely based on his Thesis. The formal definition of a Wagstaff number is as follows:

Definition 3.1. *For $n \in \mathbb{N}$ we call a number of the form $W_n = \frac{2^n+1}{3}$ a Wagstaff number.*

Wagstaff numbers have the following properties:

1. $W_{n+2} = 4W_n - 1$.
2. If $n \in \mathbb{N}$ is odd, then $W_n \in \mathbb{N}$.
3. If $n \in \mathbb{N}$ is odd and W_n is prime, then n is prime.
4. If n is prime but W_n is not prime, then for all prime divisors q of W_n we have that $q \equiv 1 \pmod{2n}$.
5. If n is prime and q is a prime such that $q|W_n$, then $q \equiv 1 \pmod 8$ or $q \equiv 3 \pmod 8$.
6. If $n > 1$ is an odd integer, then W_n is not a square.

Proof. property 1: $W_{n+2} = \frac{2^{n+2}+1}{3} = \frac{4\cdot 2^n+1}{3} = 4 \cdot \frac{2^n+1}{3} - 1 = 4W_n - 1$. □

Proof. property 2: Observe that $W_1 = 1 \in \mathbb{N}$. Then use induction on property 2 and the result follows. □

Proof. Property 3: Assume n is composite i.e. $n = ab$ where both a and b are odd and ≥ 3. Then $W_n = \frac{2^n+1}{3} = \frac{2^{ab}+1}{3}$. Now let $c = (-2)^a$. Then we get $\frac{1-c^b}{3} = \frac{(1-c)(1+c+c^2+\ldots+c^{b-1})}{3}$. Here $\frac{1-c}{3} = \frac{2^a+1}{3}$ is in $\mathbb{N}$, and because $a, b \geq 3$ it is > 1 and $< W_n$. Hence W_n is not prime. □

Proof. Property 4: Let q be a prime divisor of W_n. Then $\frac{2^n+1}{3} \equiv 0 \pmod q$. Hence $2^n + 1 \equiv 0 \pmod q \Leftrightarrow 2^n \equiv -1 \pmod q$ which in turn implies that $2^{2n} \equiv 1 \pmod q$. The order of 2 is either $1, 2, n$ or $2n$. The order cannot be 1 since we have that $2^n \equiv -1 \pmod q$. If the order of 2 is 2, then q is automatically 3 as $4 \equiv 1 \pmod q$ only holds for the prime $q = 3$. Hence $q = W_n$ and $n = 3$ meaning W_n is prime and thus we have a contradiction. If the order is n, then we cannot have $2^n \equiv -1 \pmod q$. Hence the order of 2 has to be $2n$, i.e. $2n|q-1 \Leftrightarrow q = 1 \pmod{2p}$ where $2n|q-1$ follows from Lagrange's Theorem[13]. □

Proof. Property 5: Similar as in the proof of property 4, we have $2^n \equiv -1 \pmod{q}$. This gives us $2^{n+1} \equiv -2 \pmod{q}$ and thus we have a solution for $x^2 \equiv -2 \pmod{q}$. So we know that $\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = 1$ using Theorem 2.3. So either we have $\left(\frac{-1}{q}\right) = \left(\frac{2}{q}\right) = 1$ or we have $\left(\frac{-1}{q}\right) = \left(\frac{2}{q}\right) = -1$. Then we can apply Theorem 2.5 and Theorem 2.6 to deduce that in the former case we have $q \equiv 1 \pmod{4}$ and $q \equiv \pm 1 \pmod{8}$. Implying that $q \equiv 1 \pmod{8}$. And in the latter case we have $q \equiv 3 \pmod{4}$ and $q \equiv \pm 3 \pmod{8}$. Giving us $q \equiv 3 \pmod{8}$. □

Proof. Property 6: From property 1 we know that for any odd $n > 1 \in \mathbb{N}$ we have that $W_n \equiv -1 \pmod{4}$. No x exists such that $x^2 \equiv -1 \pmod{4}$. Hence W_n is not a square. □

4 Probable prime tests

Probable prime tests verify conditions that are satisfied by all prime numbers. A famous example of such a test is Fermat's Little Theorem.

Theorem 4.1. *Fermat's Little Theorem. If p is a prime and a is an integer such that $(p, a) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. [9] □

Fermat's Little Theorem being a probable prime test implies that there exist composite integers that pass this test, so called pseudo-primes[9]. For example $341 = 11 \cdot 31$. This composite integer is a pseudo-prime to the base 2 since $2^{341} \equiv (2^{10})^{34} \cdot 2 \equiv (1)^{34} \cdot 2 \equiv 2 \pmod{341}$. The formal definition of pseudo-primes is as follows:

Definition 4.1. *Let b be a positive integer. If n is a composite integer such that $(b, n) = 1$ and $b^n \equiv b \pmod{n}$. Then n is a pseudo-prime to the base b.*

Despite this apparent flaw, Fermat's Little Theorem proves to be very useful in finding primes. Say we have a composite integer n and we choose some base $b \in \{1, 2, ..., n-1\}$. We can check if $b^{n-1} \equiv 1 \pmod{n}$, but we could also check if $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. If n is prime, then Euler's Criterion 2.2 tells us that this is either 1 or -1. Miller's test[8] takes this one step further.

Definition 4.2. *Miller's test. Let n be an integer with $n > 2$ and $n - 1 = 2^s t$, where s is a non-negative integer and t is an odd positive integer. We say that n passes Miller's test for the base b if either $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some $j \in \{0, 1, ..., s-1\}$.*

What Miller's test does is catching bases b for which n passes early. Since if $b^t \equiv 1 \pmod{n}$ or if $b^{2^j t} \equiv -1 \pmod{n}$, then $b^{n-1} \equiv 1 \pmod{n}$. Meaning all composite integers that pass Miller's test are pseudo-primes. In the case of Miller's test we know an estimate for how many such bases b exist. A well written version of this proof is provided by René Schoof[10].

Theorem 4.2. *If n is an odd composite integer, then n passes Miller's test for at most $\frac{n-1}{4}$ bases b with $b \in \{1, 2, ..., n-1\}$.*

This provides the tools to deduce whether an integer is prime with high certainty. Given any composite integer n and a randomly chosen base b between 1 and $n-1$, the chance of it passing the test is at most $\frac{1}{4}$. Repeating this test for 10 random bases, already brings the probability of n passing all 10 tests to less than 1 in 1 million.

4.1 Miller's test and Wagstaff numbers

Applying Miller's test to Wagstaff numbers is quite straightforward. Note that $W_n - 1 = \frac{2^n-2}{3} = 2(\frac{2^{n-1}-1}{3})$. One cannot take out any other factors of 2 given that $\frac{2^{n-1}-1}{3}$ is odd. Hence Miller's test simply reduces to checking if $b^{\frac{2^{n-1}-1}{3}} \equiv \pm 1 \pmod{W_n} \Longrightarrow b^{2^{n-1}-1} \equiv \pm 1 \pmod{W_n}$ for some b between 1 and $W_n - 1$.

Theorem 4.3. *Miller's test for Wagstaff primes. If W_n is a Wagstaff prime, then $b^{2^{n-1}-1} \equiv \pm 1 \pmod{W_n}$ for any $b \in \{1, 2, ..., W_n - 1\}$.*

A slightly modified version of Miller's test was introduced by Renaud and Henri Lifschitz[3]. It essentially evaluates a base b the same way as in Miller's test, but now the test evaluates the base b over the larger ring modulo $3W_n$ and considers $b^{2^{n-1}}$ instead of $b^{2^{n-1}-1}$.

Theorem 4.4. *If W_n is prime and $n > 3$, then $b^{2^n} \equiv b^2 \pmod{2^n + 1}$ where $b \in \{1, 2, ..., W_n - 1\}$.*

Proof. Assume $W_n = \frac{2^n+1}{3}$ is prime. Then Fermat's Little Theorem 4.1 implies that for any integer b such that $\gcd(b, W_n) = 1$, one has $b^{W_n-1} \equiv 1 \pmod{W_n}$. Hence $b^{\frac{2^n-2}{3}} \equiv 1 \pmod{W_n}$ which implies that $b^{2^n-2} \equiv 1 \pmod{W_n}$. Multiplying both sides with b^2 results in $b^{2^n} \equiv b^2 \pmod{W_n}$. Note that $\frac{2^n+1}{3}$ is a divisor of $2^n + 1$. To apply the Chinese Remainder Theorem [13] we require $gcd(W_n, 3) = 1$. Determining for which n this holds is equivalent to looking at when $2^n + 1 \equiv 0 \pmod 9$. Note that $2^6 = 64 \equiv 1 \pmod 9$. $2^1 + 1 \equiv 3 \pmod 9$, $2^3 + 1 \equiv 0 \pmod 9$ and $2^5 + 1 \equiv 6 \pmod 9$. n is larger than 3 by assumption. Hence the Chinese Remainder Theorem is applicable and therefore the congruence $b^{2^n} \equiv b^2 \pmod{2^n + 1}$ also holds. □

NB : In the test by Renaud and Henri Lifschitz $b = 5$ was used.

Two improvements have been made to optimize Miller's test. Working over the ring modulo $2^n + 1$ efficiently stores integers in binary form. $2^n + 1$ reduces to a string of $n + 1$ bits where only the first and the last bit are 1 and the others bits are 0. This makes it very efficient to reduce any number modulo $2^n + 1$ as the bit wise operations are minimal. Although $\frac{2^n+1}{3}$ is smaller as an integer, its binary representation consists of more 1's and hence requires more bit operations when subtracted. Moreover, in the ring modulo $2^n + 1$ it holds that $2^n \equiv -1$. So any element r can be reduced by looking at how many factors of 2^n it has. Meaning that if $r = q2^n + s$ where $s < 2^n$, then $r \equiv -q + s \pmod{2^n + 1}$. Finally one of its biggest improvements is the fact that it only uses n operations as it squares b only n times. Similar reasoning as before. The binary representation of 2^n is a string of $n + 1$ bits where only the most left bit is 1 and all the other bits are 0. Now if one has to evaluate $b^{2^{n-1}-1}$ and if we assume that its binary representation consists of k bits of 1. Then for each of those k bits equal to 1, b has to be raised to a certain power of 2 and finally all

those products would have to be added as well as well. Which will always result in more than n operations. So even though large numbers 2^n are evaluated. The test only uses n operations to evaluate.

5 Probable prime tests based on Lucas-Lehmer recurrences

As mentioned earlier, the Lucas-Lehmer test is a primality test for Mersenne numbers. The recurrences on which the Lucas-Lehmer test is based, can also be used for Wagstaff numbers. These Lucas-Lehmer recurrences are of the form $S_n = S_{n-1}^2 - 2$. Consider the following two probable Wagstaff prime tests based on the recurrences. First the Anton Vrba[16] test:

Theorem 5.1. *The Anton Vrba test. If* $W_n = \frac{2^n+1}{3}$ *is prime, then* $S_n \equiv S_2 \pmod{W_n}$ *where* $S_n = S_{n-1}^2 - 2$ *and* $S_0 = 6$.

And second the Robert Gerbicz[4] test:

Theorem 5.2. *The Robert Gerbicz Test. If* $W_n = \frac{2^n-1}{3}$ *is prime, then* $S_n \equiv S_1 \pmod{W_n}$ *where* $S_n = S_{n-1}^2 - 2$ *and* $S_0 = \frac{3}{2}$.

In order to prove these two probable Wagstaff prime tests and analyze why they work, first the necessary tools to do so have to be provided. Consider the following Lemma:

Lemma 5.3. *Let* τ *and* $\bar{\tau}$ *be the solutions of* $x^2 - S_0 x + 1 = 0$ *where* $S_0 \in \mathbb{R}$ *i.e.* $\tau = \frac{S_0+\sqrt{S_0^2-4}}{2}$ *and* $\bar{\tau} = \frac{S_0-\sqrt{S_0^2-4}}{2}$. *Then* $S_n = \tau^{2^n} + \bar{\tau}^{2^n}$, *where* $S_n = S_{n-1}^2 - 2$.

Proof. We will prove this by means of induction. Let $n = 0$, then $\tau^{2^0} + \bar{\tau}^{2^0} = \tau + \bar{\tau} = S_0$. Now assume this holds for $n = k$ where $k \in \mathbb{N}$ is taken arbitrarily. Then it should also hold for $n = k + 1$. Plugging in $n = k + 1$ and observing that $\tau\bar{\tau} = 1$ results in $S_{k+1} = \tau^{2^{k+1}} + \bar{\tau}^{2^{k+1}} = (\tau^{2^k})^2 + (\bar{\tau}^{2^k})^2 = (\tau^{2^k} + \bar{\tau}^{2^k})^2 - 2(\tau\bar{\tau})^{2^k} = S_k^2 - 2$. □

An example would $S_0 = 6$ from the Anton Vrba test, this results in $\tau = 3 + 2\sqrt{2}$. Another example is $S_0 = \frac{3}{2}$ from the Robert Gerbicz test, then $\tau = \frac{3+\sqrt{-7}}{4}$. The value inside the square root is of importance and depends on S_0. In general one wants to avoid $S_0 in \{0, \pm 1, \pm 2\}$ to avoid repeating sequences. For $S_0 \in \mathbb{Q}$ one has $\tau = \frac{\frac{c}{d}+\sqrt{\frac{c^2}{d^2}-4}}{2} = \frac{c+\sqrt{c^2-db^2}}{2d}$. S_0 needs to be chosen in such a way that $gcd(W_n, d) = 1$ as it is not always known that W_n is prime. τ is then rewritten as $\tau = a + b\sqrt{q}$ where $a, b \in \mathbb{Q}$, $q \in \mathbb{Z}$ and q cannot be simplified any further.

Note that $\tau\bar{\tau} = 1$ implies that it naturally belongs to the multiplicative group $(\mathbb{Z}[\sqrt{q}]/(W_n))^*$. This can be used to simplify the representation of τ such that no calculations involving $\sqrt{q}$ have to be done directly. This is done by denoting it as the pair $(\bar{a}, \bar{b})$ instead of $\bar{a} + \bar{b}\sqrt{q}$. To norm map has to be introduced in order to prove this.

Definition 5.1. *Let* $R = \mathbb{Z}[\sqrt{m}]/(M) = \mathbb{Z}[x]/(x^2 - m, M) = \{\bar{a} + \bar{b}\sqrt{m} : a, b \in \mathbb{Z}/(M)\}$ *where* $m, M \in \mathbb{Z}$. *Then the Norm map is defined as* $N : R \to \mathbb{Z}/(M)$ *where* $N(\bar{a} + \bar{b}\sqrt{m}) = (\bar{a} + \bar{b}\sqrt{m})(\bar{a} - \bar{b}\sqrt{m}) = \overline{a^2 - mb^2}$.

The norm map N has some useful properties:

Theorem 5.4. *The norm map N as defined in Definition 5.1 has the following properties:*

1. *For all $x, y \in R$ we have $N(xy) = N(x)N(y)$.*
2. *$N(0) = 0$ and $N(1) = 1$.*

Proof. Property 1: Let $x = \bar{a} + \bar{b}\sqrt{m}$ and $y = \bar{c} + \bar{d}\sqrt{m}$ be arbitrary elements in R. Then $N(xy) = N(\overline{ac + mbd} + \overline{(ad + bc)}\sqrt{m}) = \overline{(ac + mbd)^2 - m(ad + bc)^2} = \overline{(ac)^2 + (mbd)^2 + 2acmbd - m(ad)^2 - m(bc)^2 - 2acmbd} =$
$\overline{(ac)^2 - m(ad)^2 + (mbd)^2 - m(bc)^2} = N(x)N(y)$.
Property 2: $N(\bar{0}) = (\bar{0}+\bar{0}\sqrt{m})(\bar{0}-\bar{0}\sqrt{m}) = \bar{0}$ and $N(\bar{1}) = (\bar{1}+\bar{0}\sqrt{m})(\bar{1}-\bar{0}\sqrt{m}) = \bar{1}$. □

τ naturally belongs to the pre-image $N^{-1}(\{1\})$. This set is defined for any commutative ring R in the following way:

Definition 5.2. *Let the set $G(R, q)$ be defined as follows: $G(R, q) = \{(a, b) \in R \times R : a^2 - qb^2 = 1$ **where R is a commutative ring and** $q \in R\}$ with $(1, 0)$ as identity element, multiplication defined as $(a, b) * (c, d) = (ac + qbd, ad + bc)$ and the inverse of any element (a, b) is $(a, -b)$.*

As one might suspect, this is actually a group.

Theorem 5.5. *The set $G(R, q)$ where R is a commutative ring and $q \in R$ as defined in Definition 5.2 is a group.*

Proof. The set G is closed under its group law, given that for all $a, b, c, d \in R$ it holds that $(a, b) * (c, d) = (ac + qbd, ad + bc)$ and $(ac)^2 + (qbd)^2 + 2(acqbd) - q((ad)^2 + (bc)^2 + 2adbc) = (ac)^2 + (qbd)^2 - q(ad)^2 - q(bc)^2 = (a^2 - qb^2)(c^2 - qd^2) = 1 \cdot 1 = 1$. Additionally take any $e, f \in R$. Then $(a, b) * ((c, d) * (e, f)) = (a, b) * (ce + qdf, cf + de) = (a(ce + qdf) + qb(cf + de), a(cf + de) + b(ce + qdf)) = (ace + aqdf + qbcf + qbde, acf + ade + bce + bqdf) = ((ac + qbd)e + q(ad + bc)f, (ac + qbd)f + (ad + bc)e) = (ac + qbd, ad + bc) * (e, f) = ((a, b) * (c, d)) * (e, f)$. Hence associativity holds in G. Now note that $(a, b) * (1, 0) = (a \cdot 1 + q \cdot 0, 0 + b \cdot 1) = (a, b) = (1 \cdot a + q \cdot 0, 0 + 1 \cdot b) = (1, 0) * (a, b)$. Hence G has a well defined identity element. Next for any $(a, b) \in G$, it holds that $(a, -b) \in G$ as well since $a^2 - qb^2 \equiv a^2 - q(-b)^2 \equiv 1$. Note that $(a, b) * (a, -b) = (a^2 - qb^2, ab - ab) = (1, 0)$. Hence every element in G also has an inverse in G. □

This group allows one to evaluate $\tau = \bar{a} + \bar{b}\sqrt{q} \in (\mathbb{Z}[\sqrt{q}]/(M))^*$ as the pair $(\bar{a}, \bar{b})$. Naturally the set $\{\bar{a} + \bar{b}\sqrt{q} \in (\mathbb{Z}[\sqrt{q}]/(M))^* : N(\bar{a} + \bar{b}\sqrt{q}) \equiv \bar{1}\}$ is a subgroup of $(\mathbb{Z}[\sqrt{q}]/(M))^*$. It has the same group law, identity element and is closed under multiplication since for all $\bar{a} + \bar{b}\sqrt{q}$ and $\bar{c} + \bar{d}\sqrt{q}$ it holds that $N((\bar{a} + \bar{b}\sqrt{q})(\bar{c} + \bar{d}\sqrt{q})) = N(\bar{a} + \bar{b}\sqrt{q})N(\bar{c} + \bar{d}\sqrt{q}) \equiv \bar{1}$ using Theorem5.4.

To formalize this:

Theorem 5.6. *Let $N : (\mathbb{Z}[\sqrt{q}]/(M))^* \longrightarrow \mathbb{Z}/(M)$ be the Norm map as defined in Definition 5.1 with $q \in \mathbb{Z}$ and $M \in \mathbb{N}$. Then $\{\bar{a} + \bar{b}\sqrt{q} \in (\mathbb{Z}[\sqrt{q}]/(M))^* : N(\bar{a} + \bar{b}\sqrt{q}) \equiv \bar{1}\} \simeq G(\mathbb{Z}/(M), q)$.*

Proof. Define $f : \{\bar{a}+\bar{b}\sqrt{q} \in (\mathbb{Z}[\sqrt{q}]/(M))^* : N(\bar{a}+\bar{b}\sqrt{q}) \equiv \bar{1}\} \longrightarrow G(\mathbb{Z}/(M), q)$ where $\bar{a}+\bar{b}\sqrt{q} \longrightarrow (\bar{a}, \bar{b})$. Let $\bar{a}+\bar{b}\sqrt{q}$ and $\bar{c}+\bar{d}\sqrt{q}$ in $\{\bar{a}+\bar{b}\sqrt{q} \in (\mathbb{Z}[\sqrt{q}]/(M))^* : N(\bar{a}+\bar{b}\sqrt{q}) \equiv \bar{1}\}$ be arbitrary. Then f is a group isomorphism since $f((\bar{a}+\bar{b}\sqrt{q})*(\bar{c}+\bar{d}\sqrt{q})) = f(\overline{ac+qbd} + (\overline{ad+bc})\sqrt{q}) = (\overline{ac+qbd}, \overline{ad+bc}) = (\bar{a}, \bar{b}) * (\bar{c}, \bar{d}) = f(\bar{a} + \bar{b}\sqrt{q})f(\bar{c} + \bar{d}\sqrt{q})$. Now assume $f(\bar{a} + \bar{b}\sqrt{q}) = f(\bar{c} + \bar{d}\sqrt{q})$. Then $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d}) \iff \bar{a} \equiv \bar{c}$ and $\bar{b} \equiv \bar{d}$. Hence f is injective. Surjectivity follows since for all $(\bar{a}, \bar{b}) \in G(\mathbb{Z}/(M), q)$ we have that $\overline{a^2 - qb^2} \equiv \bar{1}$. Now let $\tau = \bar{a} + \bar{b}\sqrt{q}$, then $\tau\bar{\tau} = 1$ and $\tau \in \{\bar{a} + \bar{b}\sqrt{q} \in (\mathbb{Z}[\sqrt{q}]/(M))^* : N(\bar{a} + \bar{b}\sqrt{q}) \equiv \bar{1}\}$. Hence f is surjective as well, making it an isomorphism. □

Performing calculations with $(\bar{a}, \bar{b})$ in $G(\mathbb{Z}/(M), q)$ are identical to doing calculations with $\bar{a} + \bar{b}\sqrt{q}$ in $(\mathbb{Z}[\sqrt{q}]/(M))^*$. Note the one to one correspondence between $(\bar{a} + \bar{b}\sqrt{q})(\bar{c} + \bar{d}\sqrt{q}) = \overline{ac+qbd} + (\overline{ad+bc})\sqrt{q}$ and $(\bar{a}, \bar{b})(\bar{c}, \bar{d}) = (\overline{ac+qbd}, \overline{ad+bc})$.

In Theorem 5.1 and Theorem 5.2 τ is evaluated over the ring modulo W_n where W_n is assumed to be prime. What does the group $G(\mathbb{Z}/(W_n), q)$ then look like? Given that W_n is prime, the order of $G(\mathbb{F}_{W_n}, q)$ can exactly be determined.

Theorem 5.7. *Assume p is prime and let $G(\mathbb{F}_p, q)$ be the group defined in Definition 5.2. Then $G(\mathbb{F}_p, q)$ has order $p - \left(\frac{q}{p}\right)$.*

Proof. Finding the order of $G(\mathbb{F}_{W_n}, q)$ is identical to findings all the solutions of the hyperbola $\bar{a}^2 - q\bar{b}^2 \equiv \bar{1}$ in $\mathbb{F}_p$. To do so, any point on this hyperbola is chosen, then a line is constructed through this point and intersected with other points on the hyperbola. For simplicity, let this point be $(1, 0)$. This gives the line $y = t(x - 1)$. Intersecting this line with $x^2 - qy^2 = 1$ results in:

$$
\begin{aligned}
& x^2 - qt^2(x-1)^2 = 1 \\
\iff & -qt^2(x-1)^2 + (x+1)(x-1) = 0 \\
\iff & (x-1)(-qt^2(x-1) + x + 1) = 0.
\end{aligned}
$$

Note that $x = \bar{1}$ is one solution. The other solutions depend on $(-qt^2(x - 1) + x + 1) = 0 \iff x(1 - qt^2) + qt^2 + 1 = 0$. This gives incorrect solutions when $qt^2 = 1$ as this would imply $2 = 0$. In general the following pairs : $x = -(qt^2 + 1)(1 - qt^2)^{-1}, y = \overline{t(x - 1)}$ are obtained where t runs over $\mathbb{F}_p$. This gives p pairs of solutions. Now uniqueness has to be proven. Let $f : \{0, 1, 2, ..., p - 1\} \longrightarrow (x(t), y(t))$ be a map that sends a to $(x(a), y(a))$. Assume there exist $a, b \in \{0, 1, 2, ..., p-1\}$ such that $(x(a), y(a)) = (x(b), y(b))$. Consider the x coordinate first, $x(a) = x(b)$ implies that $(qa^2 + 1)(1 - qb^2) = (qb^2 + 1)(1 - qa^2) \iff -a^2b^2q^2 + (a^2 - b^2)q + 1 = a^2b^2q^2 + (-a^2 + b^2)q + 1$. Hence $a^2 - b^2 = -a^2 + b^2$ implying that $a = \pm b$. And for the y coordinate it holds

that: $a(qa^2+1)(1-qb^2) = b(qb^2+1)(1-qa^2) \iff -a^3b^2q^2 + a(a^2-b^2)q + a = a^2b^3q^2 + b(-a^2+b^2)q + b$. Hence $a = \pm b$. Assume $a = -b$. Then $-a^5q^2 + a(a^2 - a^2)q + a = -a^5q^2 + b(-a^2+a^2) + b$. But then $a = b$, contradicting the assumption $a = -b$. This only holds if $a = b = 0$. Hence $(x(a), y(a)) = (x(b), y(b))$ implies that $a = b$ i.e. f is injective. This automatically implies that f is bijective as p different points are mapped to p different pairs of coordinates. In total there are then $p+1$ solutions. If $\left(\frac{q}{W_n}\right) = 1$, two of those solutions are incorrect. Subtracting those leaves $p-1$ solutions. □

Now that we know the size of $G(\mathbb{F}_p, q)$, we are able to deduce the size of $G(\mathbb{Z}/(p^k), q)$ for any $k \in \mathbb{N}$.

Theorem 5.8. *Let p be prime and $k \in \mathbb{N}$ be arbitrary. Then the order of $G(\mathbb{Z}/(p^k), q)$ is $p^{k-1}(p - \left(\frac{q}{p}\right))$.*

Proof. This proof will be done by induction. Let $k = 2$. We are looking for solutions modulo p^2. Let (a, b) be a solution of $x^2 - qb^2 \equiv 1 \pmod{p}$. Then $a^2 - qb^2 = 1 + rp$ for some $k \in \mathbb{Z}$. We need to find $c, d \in \{1, 2, ..., p-1\}$ such that $(a + cp, b + dp)$ are solutions of $x^2 - qb^2 \equiv 1 \pmod{p^2}$. Plugging those coordinates in gives us $a^2 + 2acp + (cp)^2 - qb^2 - 2qbdp - q(dp)^2 \equiv 1 \pmod{p^2} \iff p(r + 2ac - 2qbd) \equiv 0 \pmod{p^2}$. This is the same as looking at values for c, d such that $r^{-1}(d(2qb) - c(2a)) \equiv 1 \pmod{p}$. We know this solution is unique[9] and also that r^{-1} exists for $r \neq 0$ since p is prime. Now we let r run over $\{1, 2, ..., p-1\}$ to obtain $p-1$ additional solutions. Meaning we have p solutions of the form $(a + cp, b + dp)$. The number of different solutions (a, b) modulo p is $p - \left(\frac{q}{p}\right)$. Hence we have $p(p - \left(\frac{q}{p}\right))$ solutions in total. Note that $(a, b) \neq (0, 0) \pmod{q}$ since we assumed it to be a solution. Now let $k \in \mathbb{N}$ be arbitrary and assume the order of $G(\mathbb{Z}/(p^k), q)$ is $p^{k-1}(p - \left(\frac{q}{p}\right))$. We apply the same method as before. We are looking for solutions of the form $(a + cp^{k-1}, b + dp^{k-1})$ modulo p^k where (a, b) is a solution of $x^2 - qy^2 \equiv 1 \pmod{p^{k-1}}$. Substituting gives us $a^2 + (cp^{k-1})^2 + 2acp^{k-1} - qb^2 - (dp^{k-1})^2 - q2bdp^{k-1} \pmod{p^k} \iff p^{k-1}(r + 2ac - 2qbd) \equiv 0 \pmod{p^k}$ where we used $a^2 - qb^2 = rp^{k-1}$ for some $r \in \mathbb{Z}$. Similar reasoning as before, this is equivalent to finding values for c, d such that $r^{-1}(d(2qb) - c(2a)) \equiv 1 \pmod{p}$. Which gives a unique solution for a unique $r \in \{1, 2, ..., p-1\}$. We have $p-1$ options in total for r plus the initial solution (a, b) so p solutions in total. The assumption tells us that we have $p^{k-1}(p - \left(\frac{q}{p}\right))$ options for our initial solution (a, b). Hence we have $p^k(p - \left(\frac{q}{p}\right))$ solutions in total that are in $G(\mathbb{Z}/(p^{k+1}), q)$. □

The order of $G(\mathbb{Z}/(NM), q)$ can also be determined given N, M are relatively prime natural numbers.

Theorem 5.9. *Let N, M be relatively prime natural numbers and $q \in \mathbb{Z}$. Then $G(\mathbb{Z}/(NM), q) \cong G(\mathbb{Z}/(N), q) \times G(\mathbb{Z}/(M), q)$.*

Proof. The Chinese Remainder Theorem [13] maps all points $(a \pmod{NM}, b \pmod{NM})$ to $(a \pmod{N}, b \pmod{N}, a \pmod{M}, b \pmod{M})$ and this mapping is a bijection. Note that $\overline{a^2 - qb^2} \equiv 1 \pmod{NM}$ implies that $\overline{a^2 - qb^2} \equiv 1 \pmod{N}$ and $\overline{a^2 - qb^2} \equiv 1 \pmod{M}$. Hence the pair $(a \pmod{N}, b \pmod{N})$ belongs to $G(\mathbb{Z}/(N), q)$. And similarly the pair $(a \pmod{M}, b \pmod{M})$ belongs to $G(\mathbb{Z}/(M), q)$. Hence $G(\mathbb{Z}/(NM), q) \cong G(\mathbb{Z}/(N), q) \times G(\mathbb{Z}/(M), q)$. □

So in general the order of $G(\mathbb{Z}/(W_n), q)$ is as follows:

Theorem 5.10. *Let $W_n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where all the p_i are distinct primes and all $a_i \in \mathbb{N}$, then the order of $G(\mathbb{Z}/(W_n), q)$ with $q \in \mathbb{Z}$ is $(p_1^{a_1 - 1}(p_1 - \left(\frac{q}{p_1}\right)))(p_2^{a_2 - 1}(p_2 - \left(\frac{q}{p_2}\right))) \cdots (p_k^{a_k - 1}(p_k - \left(\frac{q}{p_k}\right)))$*

Proof. Simply apply Theorem 5.8 and Theorem 5.9. □

Before the generalized Theorem for the Anton Vrba test and the Robert Gerbicz test can be proven. One final thing has to be pointed out. Given some $\tau = a + b\sqrt{q}$ that satisfies Lemma 5.3, then it holds that $\tau + \bar{\tau} = 2a$. This essentially means that when τ is represented as the pair (a, b), one only needs to look at the x coordinate. In general it then holds that $t^{2^n} \equiv (\bar{c}, \bar{d}) \pmod{W_n}$ is equivalent to $\overline{2c} \equiv \overline{S_n} \pmod{W_n}$. The generalized Theorem is as follows:

Theorem 5.11. *If W_n is prime, then $S_n \equiv S_1 \pmod{W_n}$ if $\left(\frac{q}{W_n}\right) = 1$ and $S_n \equiv S_2 \pmod{W_n}$ if $\left(\frac{q}{W_n}\right) = -1$. Where $S_n = S_{n-1}^2 - 2$ and $S_0 = \frac{c}{d} \in \mathbb{Q}$ is chosen such that $S_0 \notin \{\pm 1, \pm 2, 0\}$. And $\tau = \frac{S_0 + \sqrt{S_0^2 - 4}}{2} = a + b\sqrt{q}$ where $a, b \in \mathbb{Q}$ and $q \in \mathbb{Z}$ cannot be simplified any further.*

Proof. Assume W_n is prime and $S_0 \in \mathbb{Q}$ satisfies the criteria. By Theorem 5.3 some τ of the form $\tau = \bar{a} + \bar{b}$ is obtained which can be represented as $(\bar{a}, \bar{b})$ using Theorem 5.6. Now assume $\left(\frac{q}{W_n}\right) = 1$. Then $G(\mathbb{F}_{W_n}, q)$ has order $W_n - 1$ using Theorem 5.7. Hence $(\bar{a}, \bar{b})^{W_n - 1} \equiv (\bar{1}, \bar{0}) \pmod{W_n} \implies (\bar{a}, \bar{b})^{2^n - 2} \equiv (\bar{1}, \bar{0}) \pmod{W_n} \iff (\bar{a}, \bar{b})^{2^n} \equiv (\bar{a}, \bar{b})^2 \pmod{W_n}$. The x coordinate of $(\bar{a}, \bar{b})^{2^n}$ is therefore identical to the x coordinate of $(\bar{a}, \bar{b})^2$ modulo W_n. Hence automatically it holds that $S_n \equiv S_1 \pmod{W_n}$. In a similar way, if $\left(\frac{q}{W_n}\right) = -1$, then $G(\mathbb{Z}/(W_n), q)$ has order $W_n + 1$. Hence $(\bar{a}, \bar{b})^{W_n + 1} \equiv (\bar{1}, \bar{0}) \pmod{W_n} \implies (\bar{a}, \bar{b})^{2^n + 4} \equiv (\bar{1}, \bar{0}) \pmod{W_n} \iff (\bar{a}, \bar{b})^{2^n} \equiv (\bar{a}, \bar{b})^{-2^2} \pmod{W_n}$. The x coordinate of $(\bar{a}, \bar{b})^{2^2}$ and $(\bar{a}, \bar{b})^{-2^2}$ are identical. Therefore the x coordinate of $(\bar{a}, \bar{b})^{2^n}$ and $(\bar{a}, \bar{b})^{2^2}$ are also identical modulo W_n and thus $S_n \equiv S_2 \pmod{W_n}$. □

Theorem 5.11 is a generalization of the Vrba test and the Gerbicz test. In combination with the following Theorem one automatically proves the Anton Vrba test:

Theorem 5.12. *If W_p is prime, then $\left(\frac{2}{W_p}\right) = -1$.*

Proof. Note that $W_p \equiv 9W_p = 3(2^p + 1) \equiv 3 \pmod 8$ for $p > 2$. Now apply Theorem 2.6 to deduce that $\left(\frac{2}{W_p}\right) = -1$. □

Proof. The Anton Vrba Test. By using Lemma 5.3 and plugging in $S_0 = 6$, $\tau = 3 + 2\sqrt{2}$ is obtained. Now simply use Theorem 5.12 and Theorem5.11. □

With the following Theorem the Robert Gerbicz test can be proven:

Theorem 5.13. *If $W_n > 3$ is prime, then $\left(\frac{-7}{W_n}\right) = 1$*

Proof. Note that $W_n = 9W_n = 3(2^n + 1) \equiv 3 \pmod 4$ for $n > 1$. Hence by using Theorem 2.4 and Theorem 2.5 we get $\left(\frac{-7}{W_n}\right) = \left(\frac{-1}{W_n}\right)\left(\frac{7}{W_n}\right) = \left(\frac{W_n}{7}\right)$. Note that in modulo $7, W_n$ behaves in a repetitive way, since $2^3 \equiv 1 \pmod 8$. Hence we have the following options $3W_n = 2^n + 1 \pmod 7$. For $n = 1 + 3k$ with $k \in \mathbb{Z}$, $3W_n \equiv 3 \pmod 7 \Longrightarrow W_n \equiv 1 \pmod 7$. For $n = 2+3k$ with $k \in \mathbb{Z}$, $3W_n = 2^n + 1 \equiv 5 \pmod 7 \Longrightarrow W_n \equiv 4 \pmod 7$ and finally for $n = 3 + 3k$ with $k \in \mathbb{Z}$ it holds that $3W_n = 2^n + 1 \equiv 2 \pmod 7 \Longrightarrow W_n \equiv 3 \pmod 7$. We know that $\left(\frac{1}{7}\right) = 1$ and $\left(\frac{4}{7}\right) = 1$. But also that if W_n is prime, then n is prime as well. $n = 3 + 3k$ is only prime for $k = 0$. Hence this only holds for $k = 0$ i.e. W_3. □

Proof. The Robert Gerbicz Test. By plugging in $S_0 = \frac{3}{2}$ in Lemma 5.3 we obtain $\tau = \frac{3+\sqrt{-7}}{4}$. Hence our $q = -7$. Next we apply Theorem 5.13 and Theorem 5.11. □

Theorem 5.11 allows to easily prove the Anton Vrba and Robert Gerbicz tests, but also allows to construct new tests. Take for example a test with $q = 5$ where $S_0 = 3$ as initial value of our sequence S_n. Then if W_n is prime, $\left(\frac{5}{W_n}\right) = \left(\frac{W_n}{5}\right)$ using Theorem 2.4. Note that $6W_n = 2(2^n + 1) \equiv W_n \pmod 5$ and $2^4 \equiv 1 \pmod 5$. For $n = 1 + 4k$ with $k \in \mathbb{N}$ one then gets $W_n \equiv 1 \pmod 5$ and $\left(\frac{5}{W_n}\right) = \left(\frac{1}{5}\right) = 1$. And for $n = 3 + 4k$ with $k \in \mathbb{N}$ one gets $W_n \equiv 3 \pmod 5$ and $\left(\frac{5}{W_n}\right) = \left(\frac{3}{5}\right) = -1$. To test if a given W_n is a probable prime, then if $n \equiv 1 \pmod 4$ one has to check if $S_n \equiv S_1 \pmod{W_n}$. And if $n \equiv 3 \pmod 4$, then one has to check if $S_n \equiv S_2 \pmod{W_n}$.

A natural question to ask is whether new tests are actually helpful or essentially the same test. Assuming W_n is prime, the obtained τ from Lemma 5.3 is evaluated modulo W_n. So τ actually resides in the ring:

$$R = \mathbb{Z}[\sqrt{q}]/(W_n) \cong \mathbb{Z}[x]/(x^2 - q, W_n) \cong \mathbb{F}_{W_n}[x]/(x^2 - \bar{q}) \tag{4}$$

This ring is a field if $x^2 - \bar{q}$ is irreducible in $\mathbb{F}_{W_n}[x]$.

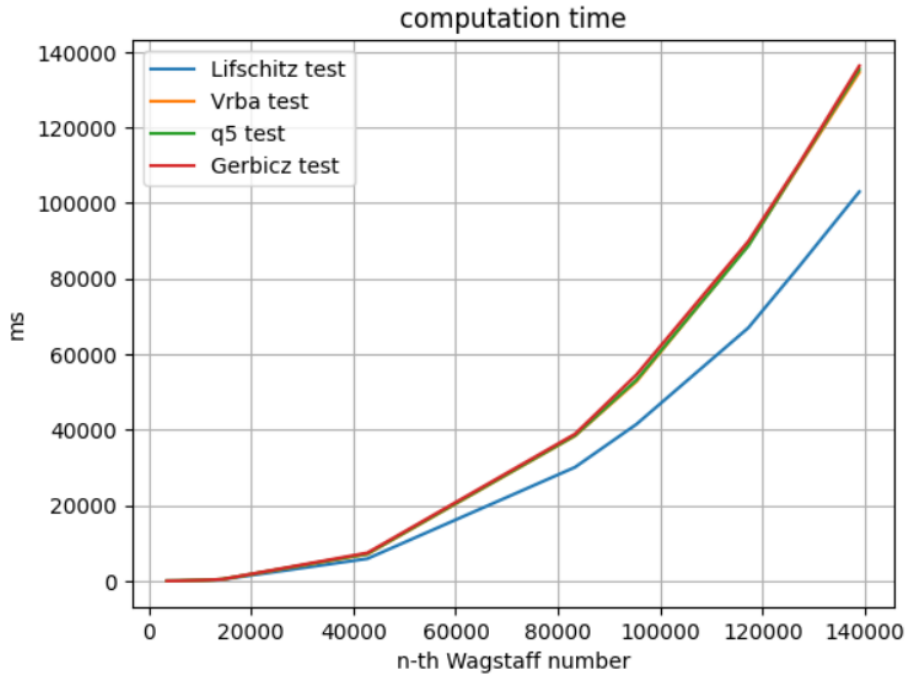
Theorem 5.14. *Let $R = \mathbb{Z}[\sqrt{q}]/(W_n)$ where W_n is prime and $\left(\frac{q}{W_n}\right) = -1$. Then R is a field.*

Proof. $x^2 - \bar{q}$ is irreducible in $\mathbb{F}_{W_n}[x]$. We know that $\mathbb{F}_{W_n}[x]$ is a principal ideal domain since W_n is prime. Thus we also know that $x^2 - \bar{q}$ being irreducible is equivalent to $(x^2 - \bar{q})$ being a maximal ideal[14]. Which implies that $\mathbb{F}_{W_n}[x]/(x^2 - \bar{q})$ is a field. □

If $R = \mathbb{Z}[x]/(x^2 - q, W_n)$ is not a field $q \not| W_n$, then it has order $(W_n - 1)^2$. And if R is a field, then it has order $W_n^2 - 1$. Although the difference between $(W_n - 1)^2$ and $W_n^2 - 1$ gets larger as n increases, τ still resides in the group $G(\mathbb{F}_{W_n}, q)$. And this group has order $W_n \pm 1$, implying that any difference is likely negligble. So the main difference seems to be that the greater structure to which the obtained τ belongs, is either a ring or a field. But the smaller subgroups, are almost identical. Hence in terms of speed one would not expect these tests to perform different. To show if this is indeed the case, computation times are compared in the next subsection.

5.1 Time comparison

In this section the performance between all the probable prime tests based on Lucas-Lehmer recurrences i.e. the Gerbicz test, the Vrba test and the newly crafted $q = 5$ test are compared. The probable prime test by Henri and Renaud Lifschitz has also been added. The scripts are written in GP/Pari. The script calculates the time needed to compute all known Wagstaff primes till date. The exponents of the Wagstaff primes are on the x-axis and the time needed to compute is on the y-axis. The time in milliseconds.



The following known Wagstaff primes have been used W_n with $n \in \{3539, 5807, 10501, 10691, 11279, 12391, 14479, 42737, 83339, 95369, 117239, 127031, 138937\}$

The computation times in ms:

For the Lifschitz test: $\{16, 47, 187, 194, 226, 296, 422, 5900, 30100, 41500, 67000, 83000, 103000\}$

For the $q = 5$ test: $\{16, 46, 207, 223, 250, 315, 475, 7200, 38500, 53200, 88700, 109850, 135400\}$

For the Vrba test: $\{16, 46, 203, 219, 250, 313, 470, 7100, 38400, 52800, 88900, 109550, 134600\}$

For the Gerbicz test: $\{16, 47, 219, 234, 266, 329, 484, 7450, 38900, 54600, 89900, 110150, 136300\}$

The code in GP/Pari for the Anton Vrba test:

```
VAppt(p) = {
    w = ((2^p) + 1) / 3;
    s_2 = (34^2) - 2;
    s_var = Mod(s_2,w);
    for(n = 3, p,
        s_var = Mod(s_var^2 - 2, w);
    );
    if(s_var == Mod(s_2, w), print(1), print(0));
}
```

The code in GP/Pari for the newly generate probable prime test using $S_0 = 3$ and $q = 5$:

```
pptq5(p) = {
    w = ((2^p) + 1) / 3;
    s_1 = 7;
    s_2 = 47;
    s_var = Mod(s_2,w);
    if (Mod(p, 4) == 1,
        for (n = 3, p,
            s_var = Mod(s_var^2 - 2, w);
        );
if(s_var == Mod(s_1, w),print(1),print(0));
        ,
        for (n = 3, p,
            s_var = Mod(s_var^2 - 2, w);
            );
if(s_var == Mod(s_2, w),print(1),print(0));
        );
}
```

The code in GP/Pari for the Robert Gerbicz test:

```
GRppt(p) = {
    w = ((2^p) + 1) / 3;
    s_1 = 1/4;
    s_var = Mod(s_1,w);
    for(n = 2, p,
        s_var = Mod(s_var^2 - 2, w);
    );
    if(s_var == Mod(s_1,W), print(1), print(0));
}
```

The algorithms of the Gerbicz, Vrba and $q = 5$ test basically work the same. They evaluate the new S_k value based on the previous one and reduce it modulo W_n. The algorithms loops until S_n is reached and check if its congruent to S_1 or S_2 depending on the algorithm and the value of n. The $q = 5$ test has to do 1 additional check compared to the others, namely checking whether n is 1 modulo 4 or if it is 3 modulo 4. So all in all these algorithms have roughly the same amount of operations, hence it is of no surprise that these three tests appear to perform similarly. The Lifschitz test however performs better in terms of speed.

The code in GP/Pari for the Henri and Renaud Lifschitz test with $b = 5$:

```
HRppt(a) = {
if(Mod(Mod(25, (2^a + 1))^(2^a-1),(2^a + 1)) == 25,
print(1), print(0))
}
```

The way this algorithm is written is identical to the so called power mod function in GP/Pari. It is efficient in evaluating modular exponention by performing modular reduction before raising it to a certain power. The results show us that the Lifschitz test is faster than the other three tests. This may be explained by the fact the modular reduction requires many lot bit operations whenever we are reducing integers modulo $\frac{2^n+1}{3}$. Like we mentioned in chapter 4. The Lifschitz test is an optimization of Miller's test, where bit operations are minimized by reducing everything modulo $2^n + 1$ instead. Similar optimizations have not been done to the Gerbicz, Vrba or our new $q = 5$ test.

5.2 The only if implication.

Ideally Theorem 5.11 would work in both directions ways i.e. that $S_n \equiv S_1$ or S_2 depending on q, implies that W_n is prime. One way to do this is to assume that W_n is composite and reach some sort of contradiction. This approach is used in the proof of the Lucas-Lehmer test[2]. For our purposes showing just the only if part of the proof sufficient.

Theorem 5.15. *The Lucas-Lehmer primality test Let* $S_n = S_{n-1}^2 - 2$ *with* $S_0 = 4$. *Then* $M_p = 2^p - 1$ *is prime if and only if* M_p *divides* S_{p-2}.

Proof. $\Longleftarrow$ Assume M_p has a proper prime divisor q. Note that Lemma 5.3 can be applied here as well. Plugging in $S_0 = 4$ results in $\tau = 2 + \sqrt{3}$. M_p is assumed to be composite, hence knowing the order of $G(\mathbb{Z}/(M_p), 3)$ means knowing the factorization of M_p. The order of $G(\mathbb{F}_q, 3)$ however is known. Depending on q its either $q-1$ or $q+1$. M_p divides S_{p-2} implies there exists some $k \in \mathbb{N}$ such that $kM_p = S_{p-2} = \tau^{2^{p-2}} + \tau^{-2^{p-2}}$. Multiplying both sides with $\tau^{2^{p-2}}$ results in $kM_p\tau^{2^{p-2}} - 1 = \tau^{2^{p-1}}$. However, by assumption $q|M_p$. Hence $\tau^{2^{p-1}} \equiv -1 \pmod{q}$. This implies that the order of τ in $G(\mathbb{F}_q, 3)$ is 2^p. But then $2^p \leq q \pm 1 < 2^p - 1$. □

A similar test could be created using Wagstaff primes, by plugging in $S_0 = 4$ in Theorem 5.11. The same group $G(\mathbb{Z}/(W_n), 3)$ is obtained. But finding some $k \in \mathbb{N}$ such that $W_n|S_k$ turns out to be very hard, if not impossible. We tried multiple known Wagstaff primes and observed all possible S_k values. None of which were congruent to zero. What was found is that $W_n|\tau^e$ where e is an odd positive integer, but not a power of 2. Making it impossible to get an expression for some S_k. Hence even if W_n is assumed to be composite with some proper prime divisor q. It seems that the same trick cannot be applied. The only thing that is known is that τ^{2^n} is equivalent to τ^{2^2} or τ^2 modulo W_n and that the order of τ therefore divides $2^n + 4$ or $2^n + 2$. For $W_n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ the order of $G(\mathbb{Z}/(W_n), 3)$ is $(p_1^{a_1-1}(p_1 - (\frac{3}{p_1})))(p_2^{a_2-1}(p_2 - (\frac{3}{p_2})))\cdots(p_k^{a_k-1}(p_k - (\frac{3}{p_k})))$. Hence finding any contradiction likely requires some form of factorization which by itself would already prove that W_n is not prime.

As of today we have not seen any examples where W_n is composite and $S_n \equiv S_2$ or S_1 modulo W_n. Or found proof of others that did. So it may very well be that W_n being composite implies that S_n is not equivalent to S_1 or S_2 modulo W_n. The first possible example is $W_9 = \frac{2^9+1}{3} = 171$. $G(\mathbb{Z}/(171), 2)$ has order 240 using the Vrba test and Theorem 5.7. The order of $(3, 2)$, the representative of τ in $G(\mathbb{Z}/(171), 2)$ has order 60. And 60 does not divide 516, hence W_9 not prime implies that $S_9 \not\equiv S_2 \pmod{171}$. The order was calculated in GP/Pari with the following script:

```
selfmult(p) = {
    w = (2^p + 1)/3;
    flag = 0;
    a = 3;
    b = 2;
    a_flag = 3;
    for(n = 2, w + 1,
a = Mod(3*a + 4*b, w);
b = Mod(3*b + 2*a_flag, w);
a_flag = a;
        if(a == 1 && b == 0,
            flag = n;
            break;
        );
    );
    print(flag);
}
```

This algorithm simply multiplies τ represented as $(3, 2)$ in $G(\mathbb{Z}/(W_n), 2)$ with itself until it reaches $(1, 0)$. It then returns the flag value which represents the order.

This approach can also be used for larger Wagstaff numbers. However, instead of calculating the order of τ, factorizations are used from the so called Cunningham Tables[17]. The Cunningham tables contain all factorizations of $2^n \pm 1$ for $n < 1200$. In this example the Anton Vrba test with $q = 2$ is again used. This test states that if W_n is prime, then $S_n \equiv S_2 \pmod{W_n}$. Lemma5.3 plus W_n being prime implies that $\tau^{W_n+1} \equiv \tau^{\frac{2^n+4}{3}} \equiv 1 \pmod{W_n} \implies \tau^{2^n+4} \equiv 1 \pmod{W_n}$. Hence the order of τ to needs to divide $2^n + 4 = 4(2^{n-2} + 1)$. Now consider the Wagstaff number W_{107}. Then the order of τ has to divide $2^{107} + 4 = 4(2^{105} + 1)$ and also the order of $G(\mathbb{Z}/(W_{107}), 2)$. The factorization of $2^{105} + 1 = 3^2 \cdot 11 \cdot 43 \cdot 211 \cdot 281 \cdot 331 \cdot 5419 \cdot 86171 \cdot 664441 \cdot 1564921$. And the factorization of $2^{107} + 1 = 3 \cdot 643 \cdot 84115747449047881488635567801$. Note that $643 \equiv 3 \pmod 8$ and $84115747449047881488635567801 \equiv 1 \pmod 8$. Hence Theorem 2.6 implies that $\left(\frac{2}{643}\right) = -1$ and $\left(\frac{2}{84115747449047881488635567801}\right) = 1$. Then the order of $G(\mathbb{F}_{643}, 2)$ is 644 and the order of $G(\mathbb{F}_{84115747449047881488635567801}, 2)$ is $84115747449047881488635567800$ using Theorem 5.7. Theorem 5.9 implies that the order of $G(\mathbb{Z}/(W_{107}), 2)$ is their product. The prime factorization of their product is $2^4 \cdot 5^2 \cdot 7 \cdot 23 \cdot 107 \cdot 39306424041611159574128 77$. None of the prime factors of $2^{105} + 1$ and the prime factors of the order of $G(\mathbb{Z}/(W_{107}), 2)$ are similar. Hence the order of τ cannot divide both. Meaning that W_{107} composite implies $S_n \not\equiv S_2 \pmod{W_{107}}$.

Just to support the possibility that it might work both ways in general, consider the following two examples. Two additional arbitrary prime numbers are chosen, $n = 251$ and $n = 337$. Then the Vrba test is applied again and the same reasoning as in the W_{107} case. Theorem 2.6 is used to deduce if 2 is a quadratic residue or a quadratic non-residue for all the prime factors of W_n. Then Theorem 5.7 and Theorem 5.9 is applied to obtain the order of $G(\mathbb{Z}/(W_n), 2)$

5.3 Example with $n = 251$

The prime factorization of $2^{251} + 1$ is: $3 \cdot 238451 \cdot 5035345723951854..$
$..68850566542884631380649090303121677364358901199128608233$. And the prime factorization of the order of $G(\mathbb{Z}/(W_{251}), 2)$ is: $2^5 \cdot 3 \cdot 13 \cdot 31 \cdot 89 \cdot 641 \cdot$
$838659329526148899570406581140 51 \cdot 648664851319405936384384380073628147$.
The prime factorization of $2^{249} + 1$ is:$3^2 \cdot 499 \cdot 1163 \cdot 2657 \cdot 155377 \cdot 13455809771 \cdot$
$9202419446683 \cdot 338809829056758737705201652256279485 93$. The order of $G(\mathbb{Z}/(W_{251}), 2)$ and $2^{249} + 1$ do not have any common prime factors except 3. The order of the representative $(3, 2)$ of τ in $G(\mathbb{Z}/(W_{251}), 2)$ cannot have order 3 since $(3, 2)^3 = (99, 60) \not\equiv (1, 0) \pmod{W_{251}}$. Hence W_{251} being composite implies that $S_n \not\equiv S_2 \pmod{W_{251}}$.

5.4 Example with $n = 337$

The prime factorization of $2^{337} + 1$ is: $3 \cdot 21569 \cdot 5333388961 \cdot 964094242760707 \cdot$
$8414620353884002547092001308011404753546603219833407092467 97..$
$..058685767257$. And the prime factorization of the order of $G(\mathbb{Z}/(W_{337}), 2)$ is:
$2^{16} \cdot 3 \cdot 5 \cdot 23^2 \cdot 151 \cdot 337^3 \cdot 32971 \cdot 430085009 \cdot 3017358263 \cdot 7641670808360088680058401 \cdot$
$9496684466729007018843657623731757 9$. The prime factorization of $2^{335} + 1$ is:
$3 \cdot 11 \cdot 93131 \cdot 7327657 \cdot 6713103182899 \cdot P75$. The $P75$ stands for a prime number that has 75 digits. The only shared prime factor is again 3. The order of τ cannot equal 3 because of similar reasoning in the W_{251} example. More over, the largest prime factor of the order of $G(\mathbb{Z}/(W_{337}), 2)$ has 69 digits. Hence it cannot equal the prime factor of 75 digits. Hence W_{337} being composite implies that $S_n \not\equiv S_2 \pmod{W_{337}}$.

6 Primality proofs of W_{79}, W_{191} and W_{313}

In this section the primality of W_{79}, W_{191} and W_{313} is shown using the Cunningham tables. The approach is follows. To determine the primality of W_n, we search for an element that has order $W_n - 1$ in $\mathbb{Z}/(W_n)$. After finding such an element, we the following Theorem is applied:

Theorem 6.1. *The multiplicative group $(\mathbb{Z}/(W_n))^*$ has order $W_n - 1$ if and only if W_n is prime.*

Proof. $\Longrightarrow$ The multiplicative group $(\mathbb{Z}/(W_n))^*$ having order $W_n - 1$ implies that for all $a \in \{1, 2, ..., W_n - 1\}$ that $gcd(a, W_n) = 1$. Hence W_n has no prime divisors i.e. W_n is prime. $\Longleftarrow$ W_n prime implies that for all $a \in \{1, 2, ..., W_n - 1\}$ we have $gcd(a, w_n) = 1$. Hence there are $W_n - 1$ elements in $(\mathbb{Z}/(W_n))^*$. $\square$

Finding an element that has order $W_n - 1$ is rather exhaustive. But finding an element x such that $x^{2^{n-1}} \equiv x \pmod{W_n}$ is not. When such an element is found, then its order has to divide $2^{n-1} - 1$. Then the Cunningham Tables are used to find the factorization of $2^{n-1} - 1$ and evaluate $x^{\frac{2^{n-1}-1}{p_i}} \pmod{W_n}$ for all prime factors p_i of $2^{n-1} - 1$ to see if it evaluates to 1. If this is only true for the prime factor 3, then the order of x is $\frac{2^{n-1}-1}{3} = \frac{W_n-1}{2}$. Now $(\mathbb{Z}/(W_n))^*$ is an abelian group. Hence for any two elements x, y in $(\mathbb{Z}/(W_n))^*$ such that their orders are co-prime, the order of their product is the product of their orders[9]. Note that -1 has order 2 and the order of x is always odd given that $2^{n-1} - 1$ is odd and is being divided by 3. Hence the order of $-x$ will be the product of 2 and $\frac{W_n-1}{2}$ i.e. it has order $W_n - 1$.

The algorithm to find this element x is as follows:

```
order(p,start,size) = {
w = (2^p + 1)/3;
for(k = start, size,
if(Mod(Mod(k,w)^(2^(p-1)),w) == k,
print(k);
break;
);
if(k == size - 1,
print("increase the size");
);
);
}
```

6.1 primality proof of W_{79}

The algorithm to find the element x returned the value 6. Hence we know that the order of 6 divides $2^{79}-1$. The factorization of $2^{79}-1$ is given by $3^2 \cdot 7 \cdot 79 \cdot 2731 \cdot 8191 \cdot 121369 \cdot 22366891$. Then by using the following algorithm:

```
order_func79(x) = {
    prime_factors = [3,7,79,2731,8191,121369,22366891];
    w =  (2^79 + 1) / 3;
    e = 2^78 - 1;
    for (i = 1, #prime_factors,
        val = Mod(x, w)^(e / prime_factors[i]);
if(val == 1,
print(1),print(0));
    );
}
```

Using this algorithm we found that the order of 6 in $\mathbb{Z}/(W_{79})$ is $\frac{W_n-1}{2}$ and hence -6 has to have order $W_{79}-1$ i.e. W_{79} is prime.

6.2 primality proof of W_{191}

The order of 3 divides $2^{190}-1$ using the algorithm mentioned earlier. The factorization of $2^{90}-1$ is: $3 \cdot 11 \cdot 31 \cdot 191 \cdot 2281 \cdot 524287 \cdot 174763 \cdot 420778751 \cdot 30327152671 \cdot 3011347479614249131$. With the following algorithm we confirmed that the order of 3 in $\mathbb{Z}/(W_{191})$ is $\frac{2^{190}-1}{3}$.

```
order_func191(x) = {
    prime_factors = [3, 11, 31, 191, 2281, 524287,
    174763, 420778751, 30327152671, 3011347479614249131];
    w =  (2^191 + 1) / 3;
    e = 2^190 - 1;
    for (i = 1, #prime_factors,
        val = Mod(x, w)^(e / prime_factors[i]);
if(val == 1,
print(1),print(0));
    );
}
```

Hence -3 has to have order $W_{191}-1$ in $\mathbb{Z}/(W_{191})$ i.e. W_{191} is prime.

6.3 primality proof of W_{313}

The order of 5 divides $2^{312}-1$. The factorization of $2^{312}-1$ is: $3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 53 \cdot 79 \cdot 157 \cdot 241 \cdot 313 \cdot 1249 \cdot 1613 \cdot 2731 \cdot 3121 \cdot 8191 \cdot 21841 \cdot 121369 \cdot 858001 \cdot 22366891 \cdot 308761441 \cdot 84159375948762099254554456081$. With the following algorithm it was confirmed that the order of 5 in $\mathbb{Z}/(W_{313})$ is $\frac{2^{312}-1}{3}$.

```
order_func313(x) = {
    prime_factors = [3,5,7,13,17,53,79,157,241,313,1249,1613,
    2731,3121,8191,21841,121369,858001,22366891,308761441,
    84159375948762099254554456081];
    w =  (2^313 + 1) / 3;
    e = 2^312 - 1;
    print(Mod(x,w)^e);
    for (i = 1, #prime_factors,
        val = Mod(x, w)^(e / prime_factors[i]);
if(val == 1,
print(1),print(0));
    );
}
```

Hence -5 has to have order $W_{313}-1$ in $\mathbb{Z}/(W_{313})$ i.e. W_{313} is prime.

7 Are there infinitely many Wagstaff primes?

A natural question to ask is whether there exist infinitely many Wagstaff primes. As of today there is no conclusive answer. There is however an attempted proof by Stephen Marshall[7]. This proof can be found in the references section. Unfortunately his proof turned out to contain multiple flaws. The first apparent one being that he defines Wagstaff primes incorrect multiple times. On page 1 Wagstaff numbers are incorrectly defined as numbers of the form $q = \frac{2^p-1}{3}$ and then just a few sentences later correctly defined in the New Mersenne Conjecture which he mentions. Then on page 3 he starts his proof, with again the incorrect definition $\frac{2^p-1}{3}$. The way he sets his attempted proof up is however unaffected by the incorrect definition. He assumes there are finitely many Wagstaff primes which he calls $n_1, n_2, ..., n_p$ where $n_p = 3$ is the smallest one. He then argues that $\frac{1}{n_1} + \frac{1}{n_2} + ... + \frac{1}{n_p} > \frac{1}{2n_1} + \frac{1}{3n_2} + ... + \frac{1}{kn_p} := S$. He then rewrites the fractions in the following manner $\frac{1}{3n_2} = \frac{1}{6n_2} + \frac{1}{6n_2}$, $\frac{1}{4n_3} = \frac{1}{12n_3} + \frac{1}{12n_3} + \frac{1}{12n_3}$ etc,

so in general $\frac{1}{kn_{k-1}} = \sum_1^k = \frac{1}{k(k-1)n_{k-1}}$ and puts them in the following form.

$$A = \frac{1}{2n_1} + \frac{1}{6n_2} + \frac{1}{12n_3} + \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + ...$$
$$B = \frac{1}{6n_2} + \frac{1}{12n_3} + \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + ...+$$
$$C = \frac{1}{12n_3} + \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + ...$$
$$D = \frac{1}{20n_4} + \frac{1}{30n_5} + \frac{1}{42n_6} + \frac{1}{56n_7} + ...$$
$$.$$
$$.$$

They are constructed in such a way that if all the rows are summed up, S is obtained again. The next step is rearranging A as follows:

$$A = (\frac{1}{n_1} - \frac{1}{2n_1}) + (\frac{1}{3n_3} - \frac{1}{4n_3}) + (\frac{1}{4n_4} - \frac{1}{5n_4}) + ...$$

It is important to note here that it was assumed that there are finitely many Wagstaff primes, namely p. So A should actually be written up till $(\frac{1}{pn_p} - \frac{1}{(p+1)n_p})$ to be precise. The author probably oversaw this part as he proceeded to rewrite A once again in the following way:

$$A = \frac{1}{n_1} + (\frac{1}{2n_2} - \frac{1}{2n_1}) + (\frac{1}{3n_3} - \frac{1}{3n_2}) + (\frac{1}{4n_4} - \frac{1}{4n_3}) + (\frac{1}{5n_5} - \frac{1}{5n_4}) + ...$$

where he notes that $n_1 > n_2 > n_3 > n_4 > ...$ and that each intermediate $(\frac{1}{2n_2} - \frac{1}{2n_1}) > 0, (\frac{1}{3n_3} - \frac{1}{3n_2}) > 0, (\frac{1}{4n_4} - \frac{1}{4n_3}) > 0, (\frac{1}{5n_5} - \frac{1}{5n_4}) > 0$ etc. His conclusion is that A then has to be larger than $\frac{1}{n_1}$. He however forgets about the $-\frac{1}{(p+1)n_p}$ at the end of A. Stating that $A > \frac{1}{n_1}$ is equivalent to stating that $(\frac{1}{2n_2} - \frac{1}{2n_1}) + (\frac{1}{3n_3} - \frac{1}{3n_2}) + (\frac{1}{4n_4} - \frac{1}{4n_3}) + (\frac{1}{5n_5} - \frac{1}{5n_4}) + ... + (\frac{1}{pn_p} - \frac{1}{pn_{p-1}}) < \frac{1}{(p+1)n_p}$. Which is something one cannot know. The same reasoning is applied to the other rows $B, C, D, ...$ For row B he concludes that $B > \frac{1}{2n_2}$, for C he concludes that $C > \frac{1}{3n_3}$ and for D likewise concludes that $D > \frac{1}{4n_4}$. He then sums up all rows and concludes that their sum S is larger than $\frac{1}{n_1} + \frac{1}{2n_2} + \frac{1}{3n_3} + \frac{4}{n_4} + ...$ and that this contradicts the earlier definition $S = \frac{1}{2n_1} + \frac{1}{3n_2} + ... + \frac{1}{kn_p}$. However he cannot draw this conclusion because of the incorrect rearrangement of the rows.

Hence it is unfortunately still not known whether there are infinitely many Wagstaff primes.

8 Conclusion

The main aim of this thesis was to describe probable prime tests involving Wagstaff numbers. This was done by first looking at the properties of Wagstaff numbers and then making the distinction between two kinds of probable prime tests. The Henri and Renaud Lifschitz test, which is a derivation of Miller's test and probable prime tests based on Lucas-Lehmer recurrences. In terms of speed, the Renaud Lifschitz test out performs the tests derived from Lucas-Lehmer recurrences. That is, the Anton Vrba test, The Robert Gerbicz test and the newly crafted test with $q = 5$. The main interest however was not necessarily the speed difference between the tests, but how they operate and potentially finding a test that states: W_n is prime if and only if a certain condition is satisfied. The build up to proving Theorem 5.7 resulted in constructing the group $G(\mathbb{Z}/(M), q)$ which in turn allows to restrict the possible orders of τ from Lemma 5.3. These restrictions together with the Vrba test and the factorizations of $2^n \pm 1$ from the Cunningham tables were used to show that W_{107}, W_{251} and W_{337} being composite automatically implied that the order of τ cannot divide $2^{105}+1, 2^{249}+1$ and $2^{335}+1$ respectively. And therefore one cannot have $S_n \equiv S_2 \pmod{W_n}$. Although three examples is nowhere near a proof, it does support the idea that these tests based on Lucas-Lehmer recurrences may work both ways. In the introduction it was mentioned that the largest proven Wagstaff prime around 1954 was W_{79} and that nowadays one can prove this using their laptop at home. This was demonstrated by proving the primality of W_{79}, W_{191} and W_{313}. Finally an attempted proof on whether there are infinitely many Wagstaff primes is incorrect was covered. The author incorrectly rearranged sums of fractions, which led to an incorrect conclusion.

9 Acknowledgement

I would like to thank Prof.dr. Jaap Top for his guidance throughout this Thesis. I especially appreciated the weekly check-ups and the willingness to help.

References

[1] P. T. Bateman, J. L. Selfridge, and Jr S. S. Wagstaff. The Mersenne Conjecture. *The American Mathematical Monthly*, 96(2):125–128, 1989.

[2] J. W. Bruce. A really trivial proof of the Lucas-Lehmer test. *The American Mathematical Monthly*, Volume 100, issue 4, 1993. https://www.tandfonline.com/doi/abs/10.1080/00029890.1993.11990414.

[3] Renaud Lifschitz en Henri Lifschitz. An efficient probable prime test for numbers of the form $(2^n + 1)/3$. 2002.

[4] Robert Gerbicz. A proof of first part of conjectures 2 and 3 (wagstaff and fermat) of previous paper. 2008. https://trex58.wordpress.com/wp-content/uploads/2009/01/wagstaffandfermat.pdf.

[5] D.H. Lehmer. Table of Wagstaff primes sent by D. H. Lehmer. *Mathematical magazine*, 27:156–157, 1954.

[6] Edouard Lucas. Congres de Nancy. In *Sur l'emploi des critériums cubiques, biquadratiques et octiques suivant un module premier.*, 1886. `http://edouardlucas.free.fr/fr/liste_des_oeuvres.htm`, `https://gallica.bnf.fr/ark:/12148/bpt6k201165x/f104.item`.

[7] Stephen Marshall. Proof that wagstaff prime numbers are infinite. 2018. https://vixra.org/pdf/1904.0033v1.pdf.

[8] Michael O Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, Volume 12, Issue 1:128–138, 1980.

[9] Kenneth H. Rosen. *Elementary Number Theory*. Pearson. 2014.

[10] René Schoof. Four primality testing algorithms. *MSRI Publications*, 44:101–126, 2008.

[11] N. J. A. Sloane. *Wagstaff numbers: numbers k such that* $(2^k + 1)/3$ *is prime.* The OEIS Foundation Inc., 1964. https://oeis.org/A000978.

[12] N. J. A. Sloane. *Wagstaff primes: primes of form* $(2^p + 1)/3$. The OEIS Foundation Inc., 1964. https://oeis.org/A000979.

[13] Prof.dr. Jaap Top. *Group Theory Notes*. 2016.

[14] Prof.dr. Jaap Top. *Algebraic Structures Notes*. 2017.

[15] Piet van Eeghen. Wagstaff getallen. 2010. Bachelor's thesis, University of Groningen, `https://fse.studenttheses.ub.rug.nl/9462/`.

[16] Anton Vrba. A really trivial proof for proving wagstaff numbers prime. 2008. http://trex58.files.wordpress.com/2009/01/waggstaff ver20.pdf.

[17] Samuel S. Wagstaff, Bryant Tuckerman, John L. Selfridge, Derrick H. Lehmer, and John Brilliant. *Factorizations of* $b^n \pm 1, b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers.* Contemporary Mathematics. Vol 22. AMS, 1988. https://www.ams.org/books/conm/022/.