University of Groningen

Bachelor Project Mathematics

Primality Testing

Author:
J.H. Dwarshuis

First supervisor:
Prof. dr. J. Top

Second supervisor:
Prof. dr. ir. R.W.C.P. Verstappen

July 13, 2017

Abstract

This thesis deals with the primality of numbers of certain forms. Two methods to develop such tests are described. The first one is the group-order method. This method has been applied to the Mersenne numbers, $M_n := 2^n - 1$, in which case it coincides with the classical Lucas-Lehmer test. The first goal of this thesis is to apply the group-order method to numbers of the form $3 \cdot 2^n + 1$ and $3 \cdot 2^n - 1$. This will result in tests that give a condition on when these numbers are prime. However, these tests only work for limited values of n. The second method that is dealt with is the elliptic curve method. Using theory about elliptic curves a test is found for numbers of the form $121 \cdot 16^n + 1$. The tests are implemented in order to generate some large prime numbers.

Contents

1 Introduction **3**

2 Group-order method **4**
2.1 Number of elements of $G_d(\mathbb{F}_q)$ 5
2.2 Element not divisible by 2 in $G_d(\mathbb{F}_q)$ 5
2.3 Elements of order 2 and order 4 in $G_d(K)$ 6
2.4 Proofs of Theorem 1 and 2 7

3 Primality tests for numbers q_n and t_n **8**
3.1 Primality test for numbers q_n 8
3.2 Primality test for numbers t_n 10
3.3 Improving the tests 10

4 Elliptic curve primality testing **12**
4.1 Elliptic curve test for numbers P_n 17
4.2 Actual prime test 19

5 Results **20**

6 Conclusions **22**

A Magma code **23**

1 Introduction

In this thesis the primality of numbers of certain forms is discussed. Prime numbers have always fascinated people and go back as far as the ancient Greeks. After some time of little development, mathematicians (Fermat, Euler, Legendre and Gauss for example) started to study prime numbers again from the 17th century onwards. From the late 19th century onwards, the focus lies more on developing tests for integers of some specific form. In this way it is possible to prove the primality of large numbers. Some tests developed in the 19th century are Pepin's test for Fermat numbers (1877), Proth's theorem (1878) and the Lucas-Lehmer test for Mersenne numbers (1878, 1935).

The basis for my research is the bachelor's thesis by P. van der Sluis [1] which deals with two methods to develop primality tests: the group-order method and the elliptic curve method. In this thesis both of these methods will be discussed.

Van der Sluis applies the group-order method to the Mersenne numbers, numbers of the form $M_n := 2^n - 1$. This is known as the Lucas-Lehmer test. The first goal of this thesis is to find out if it is possible to apply the group-order method to similar numbers. Two types of numbers are discussed: numbers $q_n := 3 \cdot 2^n + 1$ and the Thabit numbers $t_n := 3 \cdot 2^n - 1$. These last numbers are named after the Sabian mathematician Thabit ibn Qurra, who studied the relation between amicable numbers and the numbers t_n in the 9th century. For the first type of numbers, the test considers some group G over the ring $\mathbb{Z}/q\mathbb{Z}$, $G(\mathbb{Z}/q\mathbb{Z})$. The condition of the test guarantees that for a prime divisor p of q_n, $G(\mathbb{F}_p)$ has an element of large order, which gives a lower bound on p. This will imply the primality of q_n. In the same way, we build a test for the numbers t_n.

By the end of the 20th century, fast probabilistic algorithms were developed, which give deterministic support for the primality of numbers. But to actually prove their primality, other (fast) tests needed to be developed. One of the methods that were invented in that period is elliptic curve primality testing. This idea was introduced in the 80's, for example by Bosma [2] in 1985.

The second goal of this thesis is to use the elliptic curve method to develop a test for the numbers $P_n := 121 \cdot 16^n + 1$, by adapting a test described by Denomme and Savin [3]. We use the elliptic curve $E_{30} : 30y^2 = x^3 - x$. Now for a prime p with $p \equiv 1 \bmod 4$, $E_{30}(\mathbb{F}_p)$ admits a complex multiplication by $\mathbb{Z}[\iota]$, the ring of Gaussian integers. We take a point P on E_{30} that by assumption has large order and it generates the 2-Sylow subgroup of $E_{30}(\mathbb{Z}/P_n\mathbb{Z})$ as $\mathbb{Z}[\iota]$-module. Similar to the group-order method, this gives a lower bound on prime divisors of P_n. With this idea we can build a primality test for the numbers P_n.

The thesis is structured as follows: Chapter 2 deals with the group-order method and two theorems that give conditions on the primality of the numbers q_n and t_n are stated and proven. The next chapter deals with how to build an actual test from the theorems given in Chapter 2. The elliptic curve method is treated in Chapter 4. It builds up some theory to eventually state the main theorem. Both the group-order and the elliptic curve test are implemented and the results are given in Chapter 5. Lastly, the conclusion of our results is given.

2 Group-order method

In this chapter we will apply the group-order method to numbers of the form $t_n = 3 \cdot 2^n - 1$ and $q_n = 3 \cdot 2^n + 1$. This will give us tests for the primality of these numbers. In order to do so, we adapt the test for Mersenne numbers as written down by Van der Sluis [1]. Before stating the tests we need some definitions.

Definition 1. *Let P be a polynomial. By $Z(P)$ we mean the set of all zeros of the polynomial P.*

We consider the family of groups

$$G_d := Z(x^2 - dy^2 - 1).$$

An element $(a, b) \in G_d$ satisfies $a^2 - db^2 = 1$.

Definition 2. *Let R be a commutative ring. Then*

$$G_d(R) := \{(x, y) \in R \times R \mid x^2 - dy^2 = 1\}$$

is an abelian group, with zero element $(1, 0)$ and group operation:

$$(x_1, y_1) + (x_2, y_2) := (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1).$$

The proof that $G_d(R)$ is an abelian group is analogous to the proof on pages 5 and 22 in [1].

Let $(a, 1)$ be a point on G_d. Then a satisfies $d = a^2 - 1$. We define the following recurrence relation:

$$a_0 = 4a^3 - 3a, \qquad a_{k+1} = 2a_k^2 - 1.$$

Here $4a^3 - 3a$ is the x-coordinate of $3(a, 1)$ (see Lemma 1).

An important concept for the primality tests is that of squares in a finite field.

Definition 3. *Let R be a commutative ring. $R^{*2} := \{x \in R^* \mid \exists y \in R : x = y^2\} \subset R^*$. An element of R^{*2} is called a square in R^*.*

Now we can state the two theorems that give the conditions for the primality of the numbers $q_n = 3 \cdot 2^n + 1$ and $t_n = 3 \cdot 2^n - 1$ respectively.

Theorem 1. *Let $n \geq 2$.*
a) If $a_{n-2} \equiv 0$ mod q_n, then q_n is prime.
b) Let q_n be prime and let $d = a^2 - 1$ be a square in $\mathbb{F}_{q_n}$ and $2a + 2$ be not a square in $\mathbb{F}_{q_n}$. Then $a_{n-2} \equiv 0$ mod q_n.

Theorem 2. *Let $n \geq 2$.*
a) If $a_{n-2} \equiv 0$ mod t_n, then t_n is prime.
b) Let t_n be prime and let neither $d = a^2 - 1$ nor $2a + 2$ be a square in $\mathbb{F}_{t_n}$. Then $a_{n-2} \equiv 0$ mod t_n.

In order to prove these two theorems, we first need to develop some theory. In section 2.4 the theorems will be proven.

The element $3(a,1) \in G_d$ is important for the proofs of Theorem 1 and 2. The relation between this element and the recurrence relation is given by the following Lemma.

Lemma 1. *(x-coordinate of $2^k(3(a,1))) = a_k$.*

Proof. First we compute the x-coordinate of $3(a,1)$.

$$\begin{aligned} 3(a,1) &= (a,1) + (a^2+d, 2a) \\ &= (a,1) + (2a^2-1, 2a) \\ &= (a(2a^2-1) + 2a(a^2-1), *) \\ &= (4a^3 - 3a, *) \end{aligned}$$

Note that on lines 2 and 3 the relation $d = a^2 - 1$ is used. Observe from line 2 that the x-coordinate of $2(a,b)$ equals $2a^2 - 1$, independent of b. Therefore, the x-coordinate of the element $2^k(3(a,1))$ is the same as the k-th element in the recursive relation a_k. □

2.1 Number of elements of $G_d(\mathbb{F}_q)$

When we want to prove that congruences in Theorem 1b) and 2b) hold whenever q_n and t_n are prime respectively, we need to have that the number of elements of the groups $G_d(\mathbb{F}_{q_n})$ and $G_d(\mathbb{F}_{t_n})$ is equal to $3 \cdot 2^n$. This is the case because that will allow us to say something about the group structure of $G_d(\mathbb{F}_{q_n})$ and $G_d(\mathbb{F}_{t_n})$.

The following lemma gives the number of elements of $G_d(\mathbb{F}_q)$, where q is a prime so that $\mathbb{F}_q$ is a finite field with q elements. A crucial point is the question whether $d = a^2 - 1$ is a square in $\mathbb{F}_q$.

Lemma 2. *Assume the characteristic of $\mathbb{F}_q$ is not equal to 2 or 3. Then*

$$\#G_d(\mathbb{F}_q) = \begin{cases} q+1 & \text{if } d \notin \mathbb{F}_q^{*2} \\ q-1 & \text{if } d \in \mathbb{F}_q^{*2} \end{cases}$$

Proof. The proof is analogous to Lemma 3 in [1]. □

2.2 Element not divisible by 2 in $G_d(\mathbb{F}_q)$

We now state a condition on when the element $(a,1)$ is not divisible by 2 in $G_d(\mathbb{F}_q)$. In the proofs of Theorem 1b) and 2b) this property will help us to determine the order of $(a,1)$ in $G_d(\mathbb{F}_{q_n})$ and $G_d(\mathbb{F}_{t_n})$, so provided q_n resp. t_n are prime.

Lemma 3. *Let $\mathbb{F}_q$ be an odd prime. The element $(a,1) \in G_d(\mathbb{F}_q)$ is not divisible by 2 in $G_d(\mathbb{F}_q)$ if and only if $2a+2$ is not a square in $\mathbb{F}_q$.*

Proof. The element $(a,1)$ is divisible by 2 if there exists an element $(x,y) \in G_d(\mathbb{F}_q)$ such that

$$(x,y) + (x,y) = (a,1).$$

Such an element (x, y) satisfies the equations

$$\begin{cases} x^2 - dy^2 = 1 \\ x^2 + dy^2 = a \\ 2xy = 1 \end{cases} \tag{1}$$

Adding up the first two equations yields $2x^2 = a + 1$.

Suppose that $2a + 2$ is not a square in $\mathbb{F}_q$. Then $(2x)^2 = 2a + 2$ does not have a solution. Therefore, there does not exist an (x, y) such that $2(x, y) = (a, 1)$.

Now suppose that $2a + 2$ is a square in $\mathbb{F}_q$. Then there exists an $r \in \mathbb{F}_q$ such that $r^2 = 2a + 2$. Now define $x := 2^{-1}r \in \mathbb{F}_q$, then $2x^2 = a + 1$. Now put $y := r^{-1} \in \mathbb{F}_q$. Then $(x, y) \in G_d(\mathbb{F}_q)$ and it satisfies equation 1. Therefore, $2(x, y) = (a, 1)$. This completes the proof. □

2.3 Elements of order 2 and order 4 in $G_d(K)$

In this section we determine the elements of order 2 and 4 in $G_d(K)$, where K is some field. If the characteristic of K is 2 then every element except for the unit has order 2. When the characteristic of K is not 2, we have only one element of order 2, as the following lemma shows.

Lemma 4. *Let K be a field with characteristic not equal to 2. The only element of order 2 in $G_d(K)$ is $(-1, 0)$.*

Proof. An element of order 2 in $G_d(K)$ satisfies the equations

$$\begin{cases} x^2 + dy^2 = 1 \\ 2xy = 0 \\ x^2 - dy^2 = 1 \\ (x, y) \neq (1, 0) \end{cases}$$

The only point that satisfies these equations is $(-1, 0)$. □

Now we consider the points of order 4 in $G_d(K)$.

Lemma 5. *Let $b \in G_d(K)$. If the characteristic of the field K is not equal to 2 and $d \in K^*$, the order of b in $G_d(K)$ is 4 if and only if the x-coordinate of b equals 0.*

Proof. Suppose (x, y) has order 4. Then the (x-coordinate of $2(x, y)$) $= -1$ by Lemma 4. Thus $2x^2 - 1 = -1$, so $2x^2 = 0$. Since char$(K) \neq 2$, this implies $x = 0$.

Now suppose we have an element $(0, *)$. Now $2(0, *) = (-1, **)$ and we want to show that its y-coordinate is 0. Since $(-1, **) \in G_d(K)$ we have $1 - dy^2 = 1$, so $dy^2 = 0$. Since $d \in K^*$ this implies $y = 0$. Therefore, $(0, *)$ has order 4 in $G_d(K)$. □

2.4 Proofs of Theorem 1 and 2

Now that we have all the tools we need, we can prove both Theorem 1 and 2.

Proof. a) Assume $a_{n-2} \equiv 0 \bmod q_n$ for some $n \geq 2$. Let p be a prime dividing q_n. Since q_n divides a_{n-2}, so does p. In $G_d(\mathbb{F}_p)$ we thus get that the x-coordinate of $2^{n-2}(3(a,1))$ is equal to 0 by Lemma 1. Note that $p \neq 2$, because if $p = 2$ then q_n would be even, which is not true for $n \geq 1$. Therefore the characteristic of $\mathbb{F}_p$ is not 2 and thus $2^{n-2}(3(a,1))$ has order 4 in $G_d(\mathbb{F}_p)$ by Lemma 5. Then $2^n(3(a,1)) = (1,0)$, thus $\text{ord}(3(a,1))$ divides 2^n. But if $\text{ord}(3(a,1))$ is less than 2^n, $2^{n-1}(3(a,1)) = (1,0)$, which contradicts the fact that $2^{n-2}(3(a,1))$ has order 4 in $G_d(\mathbb{F}_p)$. Therefore, $\text{ord}(3(a,1)) = 2^n$. Since the order of an element in $G_d(\mathbb{F}_p)$ is 2^n, we get $2^n \leq \#G_d(\mathbb{F}_p)$. We also know that $G_d(\mathbb{F}_p)$ has at most $p+1$ elements, so

$$2^n \leq \#G_d(\mathbb{F}_p) \leq p+1.$$

Therefore $p \geq 2^n - 1$. Now suppose q_n is not prime. Then we distinguish two cases. In the first case we have $q_n = p_1 \cdot p_2 \cdot ...$, with $p_1 \neq p_2$ are prime. Then we get

$$3 \cdot 2^n + 1 = q_n \geq p_1 p_2 \geq (2^n - 1)^2.$$

For $n \geq 3$ this equation does not hold and thus we have a contradiction. The second case is $q_n = p^a$, with $a \geq 2$. This results in

$$3 \cdot 2^n + 1 = q_n \geq p^2 \geq (2^n - 1)^2,$$

and thus in this case there is also a contradiction. Therefore, q_n is prime.

b) Let $n \geq 2$ be such that q_n is prime. Let a be such that $d = a^2 - 1$ is a square in $\mathbb{F}_{q_n}$ and $2a+2$ is not. Since q_n is prime and $n \geq 3$, the characteristic of $\mathbb{F}_{q_n}$ is not 2 or 3. Because also d is a square in $\mathbb{F}_{q_n}$, we have by Lemma 2

$$\#G_d(\mathbb{F}_{q_n}) = q_n - 1 = 3 \cdot 2^n.$$

Since $G_d(\mathbb{F}_{q_n})$ is an finite group, it is finitely generated. G_d is also abelian therefore we have that

$$G_d(\mathbb{F}_{q_n}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z},$$

with $2 \leq d_1 \mid d_2 \mid ... \mid d_t$ and $d_1 \cdot d_2 \cdot \ldots \cdot d_t = 3 \cdot 2^n$. Therefore, $d_t = 3 \cdot 2^{m_t}$ and $d_j = 2^{m_j}$ for $j < t$. Here we have $1 \leq m_1 \leq m_2 \leq \cdots \leq m_t$ and $\sum_{i=1}^{t} m_i = n$.

Since every d_i is even, every $\mathbb{Z}/d_i\mathbb{Z}$ contains exactly one element of order 2. Therefore the group

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$$

has $2^t - 1$ elements of order 2. As stated in Lemma 4, $G_d(\mathbb{F}_{q_n})$ has only one element of order 2, namely $(-1,0)$. Therefore $2^t - 1 = 1$, which implies $t = 1$. Therefore, $G_d(\mathbb{F}_{q_n}) \cong \mathbb{Z}/3 \cdot 2^n\mathbb{Z}$.

In $\mathbb{Z}/3 \cdot 2^n\mathbb{Z}$ we have that a point is divisible by 2 if and only if 2^n does not divide its order. Let $(a,1) \in G_d(\mathbb{F}_{q_n})$, then by Lemma 3, $(a,1)$ is not divisible by 2 because $2a+2$ is not a square in $\mathbb{F}_{q_n}$. Therefore, $\text{ord}(a,1) = 2^n$ or $3 \cdot 2^n$.

Now consider the point $3(a,1) \in G_d(\mathbb{F}_{q_n})$. If $\text{ord}(a,1) = 3 \cdot 2^n$, clearly $\text{ord}(3(a,1)) = 2^n$. If $\text{ord}(a,1) = 2^n$ then also $\text{ord}(3(a,1)) = 2^n$. Therefore in all cases, $\text{ord}(3(a,1)) = 2^n$ in $G_d(\mathbb{F}_{q_n})$.

Since $(a,1)$ is not divisible by 2, $3(a,1)$ is not divisible by 2 in $G_d(\mathbb{F}_{q_n})$. Thus its order is 2^n. Therefore, $2^{n-2}(3(a,1))$ has order 4. By Lemma 5, $2^{n-2}(3(a,1))$ then has x-coordinate equal to 0. Therefore by Lemma 1, $a_{n-2} \equiv 0 \bmod q_n$. □

Proof. The proof of Theorem 2a) is completely analogous to the proof of Theorem 1a). Part b) is also analogous if

$$\#G_d(\mathbb{F}_{t_n}) = t_n + 1 = 3 \cdot 2^n,$$

for t_n is prime. But this is a direct consequence of Lemma 2 and the assumption that $2a+2$ is not a square in $\mathbb{F}_{t_n}$. This completes the proof. □

3 Primality tests for numbers q_n and t_n

Theorem 1 and 2 provide a useful condition for the primality of the numbers q_n and t_n. But we first need to find good choices for d and a in order to apply them. In order to do so we need the concept of quadratic reciprocity.

Definition 4. *Let p be an odd prime. Then the Legendre symbol is a function defined as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p \\ -1 & \text{if } a \text{ is not a square modulo } p \\ 0 & \text{if } a \equiv 0 \bmod p \end{cases}$$

The following property of the Legendre symbol is important to us. It is multiplicative in its top argument:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

We will also need the following well-known result.

Proposition 1. *(law of quadratic reciprocity) Let p and q be odd primes. Then*

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

Furthermore, we need the next proposition.

Proposition 2. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,7 \text{ mod } 8 \\ -1 & \text{if } p \equiv 3,5 \text{ mod } 8 \end{cases}$$

For proofs of Proposition 1 and 2 see [4].

3.1 Primality test for numbers q_n

Recall that in Theorem 1b), when q_n is prime, we need to have that $d = a^2 - 1$ is a square in $\mathbb{F}_{q_n}$ and $2a+2$ is not. We will now try to find values for a such that these conditions are satisfied.

Considering the numbers $q_n = 3 \cdot 2^n + 1$, we notice $q_n \equiv 1 \bmod 3$. For $n \geq 3$, they also satisfy $q_n \equiv 1 \bmod 8$. Thus we conclude $q_n \equiv 1 \bmod 24$. We will use this property to check

whether some small primes are squares in $\mathbb{F}_{q_n}$. In order to do so, we need the law of quadratic reciprocity.

As an example, consider the prime $p = 5$. By Proposition 1 we have

$$\left(\frac{5}{q_n}\right)\left(\frac{q_n}{5}\right) = (-1)^{\frac{4\cdot(q_n-1)}{4}} = (-1)^{24k} = 1,$$

where the second step follows from the fact $q_n \equiv 1 \bmod 24$. Thus we have

$$\left(\frac{5}{q_n}\right) = -1 \iff \left(\frac{q_n}{5}\right) = -1,$$

so we want to know when a number is a square modulo 5. Note that $0^2 \equiv 0 \bmod 5$, $1^2 \equiv 4^2 \equiv 1 \bmod 5$ and $2^2 \equiv 3^2 \equiv 4 \bmod 5$. Hence 2 and 3 are not squares modulo 5, and thus

$$\left(\frac{5}{q_n}\right) = -1 \iff q_n \equiv 2, 3 \bmod 5. \tag{2}$$

In the same way we find

$$\left(\frac{7}{q_n}\right) = -1 \iff q_n \equiv 3, 5, 6 \bmod 7. \tag{3}$$

Note that since $q_n \equiv 1 \bmod 8$ and $q_n \equiv 1 \bmod 3$, we have

$$\left(\frac{2}{q_n}\right) = 1 \quad \text{and} \quad \left(\frac{3}{q_n}\right) = 1. \tag{4}$$

Now let $a = 6$, so $d = 6^2 - 1 = 35$. So we now want that 35 is a square in $\mathbb{F}_{q_n}$ but $2 \cdot 6 + 2 = 14$ is not. Thus

$$\left(\frac{5}{q_n}\right)\left(\frac{7}{q_n}\right) = \left(\frac{35}{q_n}\right) = 1 \quad \text{and} \quad \left(\frac{2}{q_n}\right)\left(\frac{7}{q_n}\right) = \left(\frac{14}{q_n}\right) = -1.$$

By equation 4 we have that 2 is a square, which implies that 7 should not be a square and thus also that 5 is not a square in $\mathbb{F}_{q_n}$. Thus we need to know which q_n satisfy the conditions given in equations 2 and 3. It is easily shown that condition 2 is satisfied for $n \equiv 1, 2 \bmod 4$ and condition 3 for $n \equiv 2 \bmod 3$. Combining these two conditions gives $n \equiv 2, 5 \bmod 12$. We plug in these conditions on n and therefore define

$$q'_m := 12 \cdot 4096^m + 1 \quad \text{and} \quad q''_j := 96 \cdot 4096^j + 1,$$

with m and j positive integers.

We conclude that the numbers q'_m are prime if and only if $a_{12m} \equiv 0 \bmod q'_m$, where $a_0 = 4 \cdot 6^3 - 3 \cdot 6 = 846$. Similarly, the numbers q''_j are prime if and only if $a_{12j+3} \equiv 0 \bmod q''_j$.

It is possible to develop this test for other numbers as well. For example, when $a = 21$ we need

$$\left(\frac{2}{q_n}\right)^3\left(\frac{5}{q_n}\right)\left(\frac{11}{q_n}\right) = \left(\frac{440}{q_n}\right) = 1 \quad \text{and} \quad \left(\frac{2}{q_n}\right)^2\left(\frac{11}{q_n}\right) = \left(\frac{44}{q_n}\right) = -1.$$

From this we conclude that neither 5 nor 11 should be a square in $\mathbb{F}_{q_n}$. Now one can use the same methods as above to find a prime test for numbers of the form $h \cdot 1048576^m + 1$, with $h = 6, 12, 192, 1536$ or 49152. In this thesis, we restrict ourselves to one choice of a.

3.2 Primality test for numbers t_n

In order to build a test for numbers of the form $t_n = 3 \cdot 2^n - 1$, we will use the same methods as in section 3.1. The condition in Theorem 2b) we need to satisfy is that $2a+2$ and $d = a^2 - 1$ are not squares in $\mathbb{F}_{t_n}$, provided t_n is prime.

The numbers t_n satisfy $t_n \equiv 2 \bmod 3$ and for $n \geq 3$ we also have $t_n \equiv 7 \bmod 8$. For such n we get $t_n \equiv 23 \bmod 24$. We now check whether (or when) 2, 3 and 5 are squares in $\mathbb{F}_{t_n}$. Since $t_n \equiv 7 \bmod 8$ and $t_n \equiv 2 \bmod 3$, we have

$$\left(\frac{2}{t_n}\right) = 1 \quad \text{and} \quad \left(\frac{3}{t_n}\right) = 1. \tag{5}$$

To check when 5 is a square in $\mathbb{F}_{t_n}$ we use Proposition 1 and the same reasoning as in section 3.1. We see that 5 is not a square in $\mathbb{F}_{t_n}$ when $t_n \equiv 2, 3 \bmod 5$. We can just plug in the numbers $0, 1, 2$ and 3 in t_n and conclude that this holds for $n \equiv 0, 3 \bmod 4$.

We now take $a = 4$. Then $2a + 2 = 10$ and $d = a^2 - 1 = 15$, so we want to have

$$\left(\frac{2}{t_n}\right)\left(\frac{5}{t_n}\right) = \left(\frac{10}{t_n}\right) = -1 \quad \text{and} \quad \left(\frac{3}{t_n}\right)\left(\frac{5}{t_n}\right) = \left(\frac{15}{t_n}\right) = -1.$$

With equation 5 we conclude that these conditions hold when 5 is not a square in $\mathbb{F}_{t_n}$. We already saw that this is the case for $n \equiv 0, 3 \bmod 4$.

Therefore, we define

$$t'_m := 3 \cdot 16^m - 1 \quad \text{and} \quad t''_j := 24 \cdot 16^j - 1,$$

with m and j positive integers. We now get the following two tests: the numbers t'_m are prime if and only if $a_{4m-2} \equiv 0 \bmod t'_m$ and the numbers t''_j are prime if and only if $a_{4j+1} \equiv 0 \bmod t''_j$. Here the initial value of the recurrence relation is given by $a_0 = 4 \cdot 4^3 - 3 \cdot 4 = 244$.

3.3 Improving the tests

For some numbers we know beforehand that they are not prime for some values of m or j. This is because they are divisible by a small prime. We do not want to test these numbers because it requires unnecessary computation time. Therefore, we are going to check if there are small primes that divide the numbers q'_m, q''_j, t'_m or t''_j for some values of m or j.

Consider the numbers $q''_j = 96 \cdot 4096^j + 1$. By looking at the prime factorization of the first few values for j, we expect q''_j to be divisible by 11 and 29 for some values of j. Thus we want to know for which j we have

$$96 \cdot 4096^j + 1 \equiv 0 \bmod 11.$$

This is equivalent to

$$8 \cdot 4^j \equiv 10 \bmod 11$$

and thus we have

$$4^j \equiv 4 \bmod 11.$$

This equivalence holds for $j \equiv 1 \bmod 5$. In a similar way, we find that q''_j is divisible by 29 for $j \equiv 5 \bmod 7$.

Primes that frequently occur in the numbers $t'_m = 3 \cdot 16^m - 1$ are 11 and 13. Using the techniques from above, we find that 11 divides t'_m for $m \equiv 3 \bmod 5$ and 13 divides t'_m for $m \equiv 2 \bmod 3$.

The numbers t''_j are divisible by 19 for $j \equiv 5 \bmod 9$ and divisible by 29 for $j \equiv 5 \bmod 7$.

Lastly, we find $q'_m = 12 \cdot 4096^m + 1$ is divisible by 13 for every m, so the only prime of this form is 13, occurring form $m = 0$.

In chapter 5 the tests are implemented and some primes are generated.

4 Elliptic curve primality testing

In this chapter we briefly recall the method introduced by Denomme and Savin [3] and we adapt this method to a test for numbers $P_n := 121 \cdot 16^n + 1$. The elliptic curve method resembles the group-order method in the following sense. We replace the group $G_d(\mathbb{Z}/q\mathbb{Z})$ by an elliptic curve over this ring, $E_k(\mathbb{Z}/q\mathbb{Z})$, which is also a group. We try to find a point of large order on this curve to find a condition on prime divisors of P_n.

Let p be an odd prime, k an integer such that p does not divide k. Now consider the elliptic curve $E : y^2 = x^3 - kx$ over a field $\mathbb{F}_p$.
Consider the map $\iota : E \to E$, $(x, y) \mapsto (-x, iy)$. This is an endomorphism and $\iota^2 = [-1]$, where $[-1]$ denotes multiplication by -1. Let $\mathrm{End}(E)$ denote the ring of all homomorphisms from E to itself. Now define the map

$$\phi : \mathbb{Z}[\iota] \to \mathrm{End}(E), \qquad a + b\iota \mapsto a + b\iota.$$

This is a ring homomorphism. It is also injective, because $\phi(a+b\iota) = 0$ implies $(a^2+b^2)P = (a - b\iota)(a + b\iota)P = O$ for every point $P \in E$ and thus $a, b = 0$, since it is known that not all points in E with coordinates in an algebraic closure have order $\leq a^2 + b^2$.

Proposition 3. *Let p be prime and $p \equiv 1$ mod 4. Then $End(E) = \mathbb{Z}[\iota]$.*

Proof. This follows by combining the reasoning in Example *V*.4.5 and Theorem *V*.3.1(b) in Silverman [5] and the fact that $\mathbb{Z}[\iota]$ is the maximal order in the imaginary quadratic field $\mathbb{Q}(\iota)$. □

Now we want to have a way to determine the number of elements of $E(\mathbb{F}_p)$. This is given in Proposition 4. For that we need the following Lemma.

Lemma 6. *Consider the set $S := \{P \in E \mid 2P = (0, 0)\}$. We have $ker(2 + 2\iota) = S \cup E[2]$.*

Proof. Suppose $P \in S \cup E[2]$. Now if $P \in S$, we have

$$-2\iota P = -\iota 2P = -\iota(0, 0) = (0, 0) = 2P,$$

and therefore $P \in ker(2 + 2\iota)$. Points of order 2 are clearly elements of $ker(2 + 2\iota)$, thus $S \cup E[2] \subset ker(2 + 2\iota)$.

To prove the reverse direction, suppose $P \in ker(2+2\iota)$, so $(2+2\iota)P = O$. Now if $2P = O$, $P \in E[2]$ so then we are done. If $2P \neq O$, $Q := 2P$ satisfies $(1 + \iota)Q = O$. Such points in the kernel of $1 + \iota$ satisfy $Q = -\iota Q$. Write $Q = (x, y)$, then $(x, y) = (-x, -iy)$. The only points that satisfy this relation are O and $(0, 0)$ and thus $ker(1 + \iota) = \{O, (0, 0)\}$. Therefore we have $2P = O$ or $2P = (0, 0)$ and thus P is either in S or in $E[2]$. □

Proposition 4. *Let p be an odd prime and E the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_p$. If $p \equiv 1$ mod 4, then $\#E(\mathbb{F}_p) = p + 1 - 2a$ where $p = a^2 + b^2$ and $a + b\iota \equiv 1$ mod $(2 + 2\iota)$.*

Proof. Let F denote the Frobenius map $(x, y) \mapsto (x^p, y^p)$. This is an element of the ring $\mathrm{End}(E)$ and by Proposition 3 we therefore have $F = a + b\iota$ for some $a, b \in \mathbb{Z}$. In field extensions of $\mathbb{F}_p$ we have $x^p = x$ if and only if $x \in \mathbb{F}_p$ and therefore

$$ker(F - id) = E(\mathbb{F}_p).$$

Now we have

$$\#E(\mathbb{F}_p) = \text{"}deg\text{"}(F - id) = deg(a - 1 + b\iota).$$

Since $\deg(n + m\iota) = n^2 + m^2$, we obtain

$$\begin{aligned}\#E(\mathbb{F}_p) &= (a-1)^2 + b^2 \\ &= a^2 + b^2 + 1 - 2a \\ &= p + 1 - 2a.\end{aligned}$$

Here the last step follows from $p = deg(F) = deg(a + b\iota) = a^2 + b^2$.

Now we claim the following:

$$ker(2 + 2\iota) \subset ker(F - id) \iff 2 + 2\iota \mid F - id \tag{6}$$

The 'only if'-statement is a special case of Cor III.4.11 in Silverman [5], where we take $E_1 = E_2 = E_3 = E$.

For the reverse direction, suppose $F - id = f \cdot (2 + 2\iota)$ for some $f \in \text{End}(E)$. Then for $P \in ker(2 + 2\iota)$ we have $(F - id)(P) = f((2 + 2\iota)(P)) = f(0) = 0$. Therefore, $ker(2 + 2\iota) \subset ker(F - id)$ and thus the claim is proven.

By Lemma 6 we have $ker(2 + 2\iota) = S \cup E[2]$. Since $ker(F - id) = E(\mathbb{F}_p)$, the claim in equation 6 leads to

$$S \cup E[2] \subset E(\mathbb{F}_p) \iff 2 + 2\iota \mid F - id. \tag{7}$$

The points of order 2 on E are $(0, 0), (1, 0)$ and $(-1, 0)$ (because their tangent line is vertical) and these are elements of $E(\mathbb{F}_p)$. Therefore, we only need to check if the points of L are in $E(\mathbb{F}_p)$.

A point P satisfies $2P = (0, 0)$ if its tangent line goes through $(0, 0)$ in $\mathbb{F}_p$. Such tangent line is given by $y = tx$, and thus satisfies

$$t^2x^2 = x^3 - x.$$

It is the tangent line of P if

$$x^2 - t^2x - 1$$

has a double zero. That happens when the discriminant vanishes:

$$t^4 + 4 = 0.$$

This has as solutions $t = \pm 1 \pm i$. Since $p \equiv 1 \bmod 4$, these solution are in $\mathbb{F}_p$. So $S \subset E(\mathbb{F}_p)$ and thus by relation 7 we have

$$2 + 2\iota \mid F - id.$$

Since $F = a + b\iota$ for some $a, b \in \mathbb{Z}$, we get

$$2 + 2\iota \mid a + b\iota - 1$$

and thus $a + b\iota \equiv 1 \bmod (2 + 2\iota)$. □

We have expressed the number of elements of the elliptic curve $E : y^2 = x^3 - x$ in terms of a. The condition $a + b\iota \equiv 1 \bmod (2 + 2\iota)$ implies that a is odd and allows us to determine the sign of a. This is done in the following lemma.

Lemma 7. *Let $a, b \in \mathbb{Z}$. Then $a + b\iota \equiv 1$ mod $(2 + 2\iota)$ if and only if either $a \equiv 3$ mod 4 and $b \equiv 2$ mod 4 or $a \equiv 1$ mod 4 and $b \equiv 0$ mod 4.*

Proof. The statement $a+b\iota \equiv 1 \bmod (2+2\iota)$ is equivalent to $(2+2\iota) \mid a-1+b\iota$. Thus 2 divides both $a - 1$ and b. Let $n, m \in \mathbb{Z}$ such that $a - 1 = 2n$ and $b = 2m$. Then $2(1 + \iota) \mid 2(n + m\iota)$ which is equivalent to $(1 + \iota) \mid (n + m\iota)$. An element that is divided by $1 + \iota$ is of the form $(1 + \iota)(c + d\iota) = c - d + (c + d)\iota$. From this we conclude that either both n and m are odd or they are both even. In case n, m are odd we have $b \equiv 2 \bmod 4$ and $a - 1 \equiv 2 \bmod 4$ and when n, m are even we have $b \equiv 0 \bmod 4$ and $a - 1 \equiv 0 \bmod 4$. The claim follows immediately. All the steps in this proof are equivalences so we are done. □

Example 1. *In Lemma 7 we have seen that $a \equiv 1$ or 3 mod 4, thus that a is odd. The sign of a depends on in which case we are.*
Let $p = 41$. We write p as the sum of two squares: $41 = 16 + 25$. Since a is odd it is either 5 or -5. Because b is either 4 or -4, $b \equiv 0$ mod 4. Thus we are in the second case, which means $a \equiv 1$ mod 4. Therefore, $a = 5$. The number of rational point on the curve are then $E(\mathbb{F}_p) = 41 + 1 - 2 \cdot 5 = 32$.
Let $p = 101$. Then $101 = 1 + 100$, which means $a = 1$ or $a = -1$. Since $b \equiv 2$ mod 4 we are in the first case and thus get $a = -1$. We obtain $E(\mathbb{F}_p) = 101 + 1 - 2 \cdot -1 = 104$.

From this point on, we develop theory that is needed for a primality test for the Fermat numbers $F_n := 2^{2n} + 1$. This is a bit easier than the numbers $P_n = 121 \cdot 16^n + 1$, for which we make our actual test. The techniques, however, are completely similar.

Corollary 1. *For $n > 1$ if $F_n := 2^{2n} + 1$ is a prime number, then the group $E(\mathbb{F}_{F_n})$ satisfies $\#E(\mathbb{F}_{F_n}) = 2^{2n}$.*

Proof. Note that $2^{2n} + 1 = (2^n)^2 + 1^2$. Therefore, $a = 1$ or $a = -1$. For $n > 1$ we have $4 \mid 2^n$, thus we are in the second case of Lemma 7. Therefore, $a \equiv 1 \bmod 4$ and thus $a = 1$. By Proposition 4, $\#E(\mathbb{F}_{F_n}) = F_n + 1 - 2 \cdot 1 = 2^{2n}$. □

Remark 1. A necessary condition for the numbers F_n to be prime is that n is a power of 2 (for $n > 0$). This can be seen as follows. If n is not a power of 2 it has an odd prime factor $s > 2$. Thus $n = rs$, with $1 \leq r < n$. For odd k we have the following identity:

$$x^k + y^k = (x + y)(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}).$$

We plug in $x = 2^{2r}$, $y = 1$ and $k = s$ to get

$$(2^{2r} + 1) \mid (2^{2rs} + 1).$$

Thus $(2^{2r} + 1) \mid (2^{2n} + 1)$ and since $1 < 2^{2r} + 1 < 2^{2n} + 1$, we have $2^{2n} + 1$ is not prime. Thus F_n is prime implies that it is of the form 2^{2^l} which makes it a Fermat prime.

Lemma 8. *Let p be a prime divisor of F_n. Then $p \equiv 1$ mod 4.*

Proof. Define $x := 2^n$, then $F_n = x^2 + 1$. Since p is a divisor of F_n, $x^2 + 1 \equiv 0 \bmod p$. Then $x^2 \equiv -1 \bmod p$ and $x^4 \equiv 1 \bmod p$. Thus the order of x mod p is either $1, 2$ or 4. $\mathrm{Ord}(x) = 1$ implies $x = 1$, and thus $2 = x^2 + 1 = 0$ in $\mathbb{F}_p$. This gives $p = 2$, but that contradicts the fact that $F_n \equiv 1 \bmod 2$. $\mathrm{Ord}(x) = 2$ implies $x = -1$ and then again with $2 = x^2 + 1 = 0$ in $\mathbb{F}_p$ we arrive at a contradiction. Therefore, $\mathrm{ord}(x) = \mathrm{ord}(2^n) = 4$. Therefore, $4 \mid p - 1$ and hence $p \equiv 1 \bmod 4$. □

Proposition 5. *Consider $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(x^2 - ax - b)$, with $\alpha = x$ mod $(x^2 - ax - b)$ for some $a, b \in \mathbb{Z}$. For any $(n, m) \in \mathbb{Z}$ with $(n, m) \neq (0, 0)$ and $n^2 + nma - m^2 b \neq 0$ one has*

$$\#\mathbb{Z}[\alpha]/(n + m\alpha) = |N(n + m\alpha)| = |n^2 + nma - m^2 b|.$$

Proof. This is proposition 3 of Van der Sluis' bachelor's thesis [1], so the proof can be found there. □

Proposition 6. *Assume that $n > 1$ and F_n is prime. Then*

$$E(\mathbb{F}_{F_n}) \cong \mathbb{Z}[\iota]/(1 + \iota)^{2n}$$

as $\mathbb{Z}[\iota]$-modules.

Proof. Since $F_n \equiv 1 \bmod 4$ we have by Proposition 3 that $\mathbb{Z}[\iota] = End(E)$ and thus $E(\mathbb{F}_{F_n})$ is a $\mathbb{Z}[\iota]$-module. We know that $E(\mathbb{F}_{F_n})$ has a finite number of elements, thus it is a finitely generated $\mathbb{Z}[\iota]$-module. Therefore, it is isomorphic to the additive group

$$\mathbb{Z}[\iota]/(\alpha_1) \oplus \mathbb{Z}[\iota]/(\alpha_2) \oplus \cdots \oplus \mathbb{Z}[\iota]/(\alpha_t)$$

for some $t \in \mathbb{N}$ and $\{\alpha_j\} \subset \mathbb{Z}[\iota]$. Here each $\mathbb{Z}[\iota]/(\alpha_j)$ is a subgroup of $E(\mathbb{F}_{F_n})$, which implies that $\#\mathbb{Z}[\iota]/(\alpha_j) = N(\alpha_j)$ divides the order of $E(\mathbb{F}_{F_n})$. Here $\#\mathbb{Z}[\iota]/(\alpha_j) = N(\alpha_j)$ follows from Proposition 5. In Corollary 1 we saw $\#E(\mathbb{F}_{F_n}) = 2^{2n}$, so $N(\alpha_j) = \alpha_j \bar{\alpha_j}$ is a power of 2. In $\mathbb{Z}[\iota]$ we can factor 2 as $-\iota(1 + \iota)^2$ and this factorization is unique because $\mathbb{Z}[\iota]$ is a unique factorization ring. Therefore, the α_j's are powers of $(1 + \iota)$ and thus we can write

$$\mathbb{Z}[\iota]/(1 + \iota)^{m_1} \oplus \mathbb{Z}[\iota]/(1 + \iota)^{m_2} \oplus \cdots \oplus \mathbb{Z}[\iota]/(1 + \iota)^{m_t}, \tag{8}$$

where $m_j \geq 1$ for $j = 1, 2, \ldots, t$. We now look at the annihilator of $1 + \iota$ in this $\mathbb{Z}[\iota]$-module given in 8. Each $\mathbb{Z}[\iota]/(1 + \iota)^{m_j}$ has two elements that are annihilated by $1 + \iota$, namely 0 and $(1 + \iota)^{m_j - 1}$. Thus the annihilator of $1 + \iota$ in the group in equation 8 has 2^t elements. We have seen before that there are two points in $E(\mathbb{F}_{F_n})$ that are annihilated by $1 + \iota$, namely O and $(0, 0)$. This implies $t = 1$. Therefore, $E(\mathbb{F}_{F_n})$ is a cyclic $\mathbb{Z}[\iota]$-module and since it has 2^{2n} elements we have $m_1 = 2n$ by Proposition 5. This completes the proof. □

If we want to construct a test for numbers F_n, we need a point P that generates $E(\mathbb{F}_{F_n})$. We do that by introducing the curves E_m given by $my^2 = x^3 - x$, where m is either an integer or a rational number. Now if m is a nonzero square modulo F_n, the map

$$(x, y) \mapsto (x, m^{1/2} \cdot y)$$

is an isomorphism between the $\mathbb{Z}[\iota]$-modules E_m and E. So the machinery above also applies to the curves E_m.

Now consider the curve E_{30} with the point $P := (5, 2)$ on it. When n is even and F_n prime we have

$$\left(\frac{30}{F_n}\right) = \left(\frac{2}{F_n}\right) \cdot \left(\frac{3}{F_n}\right) \cdot \left(\frac{5}{F_n}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$

As we noted in Remark 1, F_n is prime implies n is a power of 2 and therefore even. Thus 30 is a square modulo F_n when F_n is prime. We then have

$$E_{30}(\mathbb{F}_{F_n}) \cong E(\mathbb{F}_{F_n}) \cong \mathbb{Z}[\iota]/(1+\iota)^{2n}.$$

Lemma 9. *Let $n > 1$ and F_n be prime. The point $P = (5, 2)$ is a generator of the $\mathbb{Z}[\iota]$-module $E_{30}(\mathbb{F}_{F_n})$.*

Proof. We first need to know how to multiply by $1 + \iota$ on E_{30}. As calculated in [3] we get $(1 + \iota) \cdot (x, y) = (x', y')$ where

$$\begin{cases} x' = 30 \cdot A^2 \\ y' = -y - A(x' - x). \end{cases} \tag{9}$$

Here A is the slope of the line through (x, y) and $(-x, \iota y)$ which is given by $A = \frac{(1-\iota)y}{2x}$.

The point P is a generator of $E_{30}(\mathbb{F}_{F_n})$ if there does not exist a point R in $E_{30}(\mathbb{F}_{F_n})$ such that

$$(5, 2) \equiv (1 + \iota) \cdot R \mod F_n.$$

By equation 9 we have that for such a point R the following must hold:

$$5 \equiv 30 \cdot A^2 \mod F_n.$$

But since F_n is prime, n must be even, which means that in $E_{30}(\mathbb{F}_{F_n})$ we have that 30 is a square and 5 is not. Therefore this equation is not satisfied and thus we are done. □

We have proven useful properties of $E_{30}(\mathbb{F}_{F_n})$ in the case that F_n is prime: that it is isomorphic to a cyclic $\mathbb{Z}[\iota]$-module and that the point $(5, 2)$ is its generator. In the next section we will use these properties and the techniques for numbers of the form $P_n = 121 \cdot 16^n + 1$.

4.1 Elliptic curve test for numbers P_n

In this section we will prove a test for the numbers $P_n = 121 \cdot 16^n + 1$. Before stating the Theorem, we state some results about $E_{30}(\mathbb{F}_{P_n})$ in case P_n is prime which are very similar to what we did for the numbers F_n. The methods are referred to, without going into them again.

Proposition 7. *Let $n > 1$ be such that P_n is prime. Let E_{30} be the elliptic curve given by $30y^2 = x^3 - x$ and let $(5, 2)$ be a point on E_{30}. We have*

$$\#E_{30}(\mathbb{F}_{P_n}) = 121 \cdot 16^n.$$

Furthermore, we have

$$E_{30}(\mathbb{F}_{P_n}) \cong \mathbb{Z}[\iota]/(11) \times \mathbb{Z}[\iota]/(1+\iota)^{4n}$$

as $\mathbb{Z}[\iota]$-modules. Lastly, the point $11 \cdot (5, 2)$ generates $11 \cdot E_{30}(\mathbb{F}_{P_n}) \cong \mathbb{Z}[\iota]/(1+\iota)^{4n}$.

Proof. Note that we have $P_n = (11 \cdot 4^n)^2 + 1^2$ and that 4 divides 16^n because $n > 1$. By the same reasoning as in Corollary 1 we then get $\#E(\mathbb{F}_{P_n}) = P_n + 1 - 2 \cdot 1 = 121 \cdot 16^n$. The curves E and E_{30} are isomorphic if 30 is a square in $\mathbb{F}_{P_n}$. A simple calculation shows that 2 is a square in $\mathbb{F}_{P_n}$ and 3 and 5 are not. Thus we have

$$\left(\frac{30}{P_n}\right) = \left(\frac{2}{P_n}\right) \cdot \left(\frac{3}{P_n}\right) \cdot \left(\frac{5}{P_n}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$

Thus 30 is a square in $\mathbb{F}_{P_n}$ and we conclude

$$\#E_{30}(\mathbb{F}_{P_n}) = 121 \cdot 16^n.$$

We now apply the same reasoning as in Proposition 6 to $E_{30}(\mathbb{F}_{P_n})$. We see that it is a finitely generated $\mathbb{Z}[\iota]$-module and that it is cyclic. Therefore, we obtain

$$E_{30}(\mathbb{F}_{P_n}) \cong \mathbb{Z}[\iota]/(11 \cdot 4^n) \cong \mathbb{Z}[\iota]/(11) \times \mathbb{Z}[\iota]/(4^n),$$

where the last step follows from the Chinese Remainder theorem and the fact that 4^n and 11 are coprime. Now since $4 = -(1+\iota)^4$ we get

$$E_{30}(\mathbb{F}_{P_n}) \cong \mathbb{Z}[\iota]/(11) \times \mathbb{Z}[\iota]/(1+\iota)^{4n}$$

as $\mathbb{Z}[\iota]$-modules.

To show that the point $11 \cdot (5, 2)$ generates $11 \cdot E_{30}(\mathbb{F}_{P_n})$, we use the same reasoning as in Lemma 9. By the calculation above, we have that 30 is a square in P_n and 5 is not and thus we are done. □

We are now ready to prove the main theorem. We define $p_n := 11 \cdot 4^n + i$ so that $P_n = p_n \cdot \bar{p_n}$. Now P_n is a prime integer if and only if p_n is a Gaussian prime.

In the theorem we will show that when a certain condition holds, prime divisors p of the numbers P_n are at most 122. We want that there are no prime divisors p of P_n, because that implies that P_n is prime. Therefore we exclude the values of n for which P_n is divisible by primes p that satisfy $p \equiv 1 \bmod 4$ and $p \leq 122$. Table 4.1 gives us the values of n that we exclude.

p	n
13	1 mod 3
29	5 mod 7
61	0 mod 15
101	6 mod 25

Table 1: Complete list of values $p \leq 122$ and $p \equiv 1 \bmod 4$ and n such that $121 \cdot 16^n \equiv -1 \bmod p$

Theorem 3. *Let $P := 11 \cdot (5, 2)$ be a point on the elliptic curve $E_{30} : 30y^2 = x^3 - x$. Let n be a positive integer such that $n \not\equiv 1$ mod 3, $n \not\equiv 5$ mod 7, $n \not\equiv 0$ mod 15 and $n \not\equiv 6$ mod 25. Now P_n is prime if and only if*

$$(1 + \iota)^{4n-1} P \equiv (0, 0) \text{ mod } p_n.$$

Proof. $\Leftarrow$: Suppose p is a prime divisor of P_n. We apply the same reasoning as in Lemma 8 with $x := 11 \cdot 4^n$ to the numbers P_n to conclude that $p \equiv 1 \bmod 4$. Hence, because of [4], $p = \pi\bar{\pi}$, where π is irreducible in $\mathbb{Z}[\iota]$. Then $\mathbb{Z}[\iota]/(\pi) =: \mathbb{F}_p$ is a finite field with p elements.

Now consider the map

$$f : \mathbb{Z}[\iota] \to E_{30}(\mathbb{F}_p), \qquad a + b\iota \mapsto (a + b\iota) \cdot P$$

This is a homomorphism of $\mathbb{Z}[\iota]$-modules, hence the annihilator of P (which is the same as the kernel of f) is an ideal in $\mathbb{Z}[\iota]$. Since $\mathbb{Z}[\iota]$ is euclidean, it is a principal ideal domain and thus $\mathrm{Ann}(P)$ is of the form (α).
Without loss of generality, assume π divides p_n. With the assumption made we then get the congruence

$$(1 + \iota)^{4n-1} P \equiv (0, 0) \bmod \pi. \tag{10}$$

Because on E_{30} the point $(0, 0)$ is annihilated by $1 + \iota$, multiplying both sides by $1 + \iota$ gives

$$(1 + \iota)^{4n} P \equiv O \bmod \pi, \tag{11}$$

where O is the identity element in $E(\mathbb{F}_\pi)$.

We now want to determine the annihilator of P. By congruence 11 we have that $(1+\iota)^{4n} \in \mathrm{Ann}(P)$ and by congruence 10 that $(1 + \iota)^{4n-1} \notin \mathrm{Ann}(P)$. Also we have $1 + \iota$ is irreducible in $\mathbb{Z}[\iota]$, because $N(1 + \iota) = 2$. Therefore it follows that $\mathrm{Ann}(P) = ((1 + \iota)^{4n})$. This gives

$$f(\mathbb{Z}[\iota]) = \mathbb{Z}[\iota]P \cong \mathbb{Z}[\iota]/((1 + \iota)^{4n}).$$

By Proposition 5, we find

$$\#E_{30}(\mathbb{F}_p) \geq \#f(\mathbb{Z}[\iota]) = \#\mathbb{Z}[\iota]/((1 + \iota)^{4n}) = N((1 + \iota)^{4n})) = 2^{4n} = 16^n.$$

From the Hasse bound, see [5] Chapter V Theorem 1.1, it follows that

$$(\sqrt{p} - 1)^2 \leq \#E_{30}(\mathbb{F}_p) \leq (\sqrt{p} + 1)^2.$$

Then we use our minimum on $\#E_{30}(\mathbb{F}_p)$ to get $p \geq 16^n - 2 \cdot 4^n + 1$. Now using the fact that p divides $121 \cdot 16^n + 1$ one can show that p is at most 122. Since we excluded the values of n

for which there are such p's that divide P_n, there are no prime divisors p of P_n. Therefore, P_n is prime.

$\Rightarrow$: Now assume P_n is prime. Since the finite fields $\mathbb{Z}/(P_n)$ and $\mathbb{Z}[\iota]/(p_n)$ are isomorphic we have by Proposition 7

$$E_{30}(\mathbb{F}_{p_n}) \cong \mathbb{Z}[\iota]/(11) \times \mathbb{Z}[\iota]/(1+\iota)^{4n}.$$

Also by Proposition 7, the point P generates $\mathbb{Z}[\iota]/(1+\iota)^{4n}$. It follows that $(1+\iota)^{4n-1}P$ is an element of order $1+\iota$ not equal to O. We already saw that $(0,0)$ is the only such point, so this completes the proof. □

4.2 Actual prime test

The condition in Theorem 3 states that after $4n-1$ times multiplying P by $1+\iota$, we should get the point $(0,0)$ mod p_n. Recall from Lemma 9 that we have a formula for the x-coordinate of a point when multiplying by $1+\iota$. Therefore we define the recurrence relation

$$x_{m+1} = \frac{1}{2}\Big(\frac{x_m}{i} + \frac{i}{x_m}\Big),$$

with x_0 the x-coordinate of P which is calculated in appendix A. Now we are able to state the prime test.

Theorem 4. *For $n \not\equiv 1$ mod 3, $n \not\equiv 5$ mod 7, $n \not\equiv 0$ mod 15 and $n \not\equiv 6$ mod 25 we have P_n is prime if and only if x_m is relatively prime to p_n for all $m = 1, \ldots, 4n-1$ and $x_{4n} \equiv 0$ mod p_n.*

5 Results

With both the group-order method and the elliptic curve method we found primality tests. Now we want to actually generate some primes with these tests. The code for the test described in Magma for the numbers $q''_j = 96 \cdot 4096^j + 1$ is given below.

Listing 1: Code for numbers q''_j

```
for n in [2..1200] do
for> if n mod 5 ne 1 and n mod 7 ne 5 then
for|if> Zq:=Integers(96*4096^n+1);
for|if> A:=846;
for|if> for i in [1..12*n+3] do
for|if|for> A:=Zq!2*A^2-1;
for|if|for> end for;
for|if> if A eq 0 then print n; end if;
for|if> end if;
for> end for;
```

We find that q''_j is prime for $j = 3, 17, 29$. This is a bit disappointing of course, but the numbers t'_m and t''_j give better results.

We adjust the code slightly to obtain primes of the form $t'_m = 3 \cdot 16^m - 1$.

Listing 2: Code for numbers t'_m

```
for n in [2..2000] do
for> if n mod 3 ne 2 and n mod 5 ne 3 then
for|if> Zt:=Integers(96*4096^n+1);
for|if> A:=244;
for|if> for i in [1..4*n-2] do
for|if|for> A:=Zt!2*A^2-1;
for|if|for> end for;
for|if> if A eq 0 then print n; end if;
for|if> end if;
for> end for;
```

We find primes for $m = 16, 19, 54, 81, 819$ and 1051.

Listing 3: Code for numbers t''_j

```
for n in [2..2000] do
for> if n mod 9 ne 5 and n mod 7 ne 5 then
for|if> Zt:=Integers(96*4096^n+1);
for|if> A:=244;
for|if> for i in [1..4*n+1] do
for|if|for> A:=Zt!2*A^2-1;
for|if|for> end for;
for|if> if A eq 0 then print n; end if;
for|if> end if;
for> end for;
```

For $t''_j = 24 \cdot 16^J - 1$ we find primes for $j = 10, 13, 25, 35, 97, 206$ and 1889. This is much better: t''_{1889} has 2275 decimal digits!

A way to implement the elliptic curve test given in section 4.2 is the following:

Listing 4: Code for numbers P_n

```
> for n in [2..1000]
for> do if n mod 3 ne 1 and n mod 7 ne 5 and n mod 15 ne 0 and n mod
   25 ne 6 then
for|if> Pn:=121*16^n+1;
for|if> ZP:=Integers(Pn);
for|if> w1:=11*4^n;
for|if> x:=(ZP!xi)/(ZP!30);
for|if> for k in [0..4*n-2]
for|if|for> if Gcd(ZP!x,Pn) ne 1 then break; end if;
for|if|for> x:=ZP!w1*(-x+1/x)/2;
for|if|for> if x eq ZP!0 then print n; break; end if;
for|if|for> end for; end if; end for;
```

In this code, xi is the x-coordinate of $11 \cdot (150, 1800)$ on the curve $\eta^2 = \xi^3 - 900\xi$, which is a translation of $30y^2 = x^3 - x$. Xi is calculated in appendix A.

We see that $P_n = 121 \cdot 16^n + 1$ is prime $n = 2, 3, 11, 21, 24, 57, 66, 80, 183, 197$ and 452. With probabilistic tests it is possible to find much larger primes of the form P_n, but this is because Magma is rather slow for the implementation of our test.

6 Conclusions

We managed to apply the group-order method to numbers of both the form $q_n = 3 \cdot 2^n + 1$ and $t_n = 3 \cdot 2^n - 1$. In order to do so, however, we had to restrict ourselves to limited values of n. This resulted in prime tests for numbers of the form $96 \cdot 4096^n + 1$, $3 \cdot 16^n - 1$ and $24 \cdot 16^n - 1$. The tests are fast and thus allowed us to find some large primes. The method can also be applied to numbers $h \cdot 2^n + 1$ and $h \cdot 2^n - 1$, with h a small odd integer not equal to 3. More big primes can be generated in this way.

We found a prime test for the numbers $P_n = 121 \cdot 16^n + 1$ using the elliptic curve method. Also for these numbers, we generated large primes.

A Magma code

The following Magma-code calculates the x-coordinate of $P = 11 \cdot (5, 2)$.

```
> E:=EllipticCurve([-30^2,0]);
> P:=E![150,1800];
> xi:=(11*P)[1];
> x:=xi/30;
```

This gives the following fraction as output:

```
> x;
95928164591506657472197604697825030516627872201045925895972809629481605/889388450616149985862892895831039919448842617632358601391569
1714210401
```

The numerator and denominator are factorized as follows.

```
> n:=Numerator(x);
> d:=Denominator(x);
> Factorization(n);
[ <5, 1>, <2377, 2>, <925293656981, 2>, <62976612837556140053, 2> ]
> Factorization(d);
[ <201875808365925671, 2>, <467155497539017319, 2> ]
```

References

[1] P. van der Sluis, Bachelor's thesis at University of Groningen, *Primality Testing* (2016), http://irs.ub.rug.nl/dbi/5729a9dac24ce

[2] W. Bosma, *primality testing using elliptic curves*, Mathematical institute at University of Amsterdam (1985).

[3] R. Denomme, G. Savin, *Elliptic curve primality tests for Fermat and related primes*, Journal of Number Theory 128.8 (2008): 2398-2412.

[4] B van Geemen, H.W. Lenstra, F. Oort, J. Top, *Algebraïsche Structuren*. http://www.math.rug.nl/~top/dic.pdf, pages 197-200, 226-233.

[5] J.H. Silverman, *The arithmetic of elliptic curves*, Vol. 106. Springer Science & Business Media, 2009.

[6] J. Top, *Groepentheorie* http://www.math.rug.nl/~top/alg1.pdf, pages 109-116.

[7] J.H. Silverman, *An Introduction to the Theory of Elliptic Curves*, http://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf, slides 5-31.