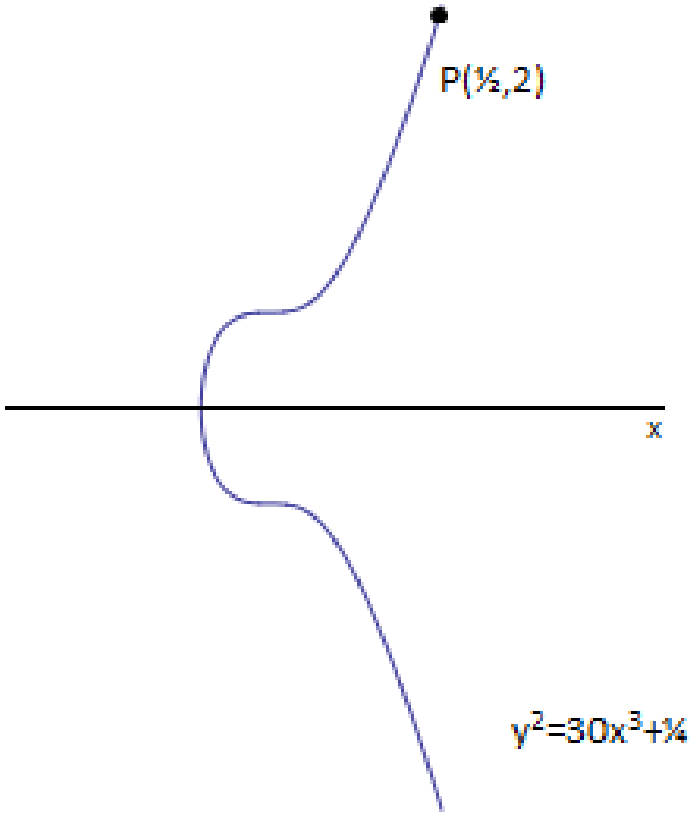
university of groningen

faculty of mathematics and natural sciences

Primality Testing



Bachelor's thesis

May 2, 2016

Student: P. A. van der Sluis

Primary supervisor: Prof. dr. J. Top

Secondary supervisor: Prof. dr. E.C. Wit

Abstract

This thesis discusses the primality of two types of numbers. In 1857, French mathematician Édouard Lucas stated that $2^{127} - 1$ was a prime number. In the 1930s, American mathematician Derrick Lehmer came up with a simple test for finding primes of the form $2^n - 1, n \in \mathbb{N}$. In this thesis I give a detailed proof of a more general version of this test, based on the unpublished notes from Jaap Top. After that, a part of the proof will be modified to make variations and find different prime tests. The second type of numbers are of the form $K_\ell := 3^{2^\ell} - 3^{2^{\ell-1}} + 1$. I will give an necessary and sufficient condition for primes of this form, but only proof the necessary part of it. This proof is based on elliptic curves. The last part of this thesis is used to discuss several important differences between the two tests.

Contents

1 Introduction

This thesis discusses the primality of two types of numbers: $M_n := 2^n - 1, n \in \mathbb{N}$ and M_n and $K_l := 3^{2^l} - 3^{2^{l-1}} + 1, l \in \mathbb{N}$.

1.1 Mersenne Numbers

The first type of numbers, M_n, are also called the Mersenne numbers. Observe that $M_1 = 1$ is not prime and $M_2 = 3$ is prime. For $n > 2$, one can first think about some necessary conditions on the number n. For example if n is a even number, we see that $2^n - 1 = (2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}} + 1)$, so since $n > 2$ both factors are larger then 1 and thus M_n is a composite number. To find a more strict condition on n, assume n is a composite number, say $n = ab$, with $a, b \neq 1$, $2^n - 1 = 2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-2)a} + 2^{(b-1)a})$. Since a and b are larger then 1, both factors are larger then 1 and hence M_n is composite. We conclude that n composite implies M_n composite. But for n prime, we cannot say directly whether $2^n - 1$ is prime. We see this since $M_3 = 7$ is prime but $M_{11} = 2047 = 23 \cdot 89$ is not. In section 2 a necessary and sufficient condition on n for the primality of M_n is stated and proved. This condition is the classical Lucas-Lehmer test, initiated by Lucas in 1856 and in 1878, and finalized by Lehmer in 1935.

1.2 The numbers K_ℓ

With $\omega := e^{2\pi i/3} \in \mathbb{C}$, the integers $K_\ell = 3^{2^\ell} - 3^{2^{\ell-1}} + 1$ can be written as $K_l = (3^{2^{l-1}} + \omega)(3^{2^{\ell-1}} + \overline{\omega})$. In Subsection 3.2 it will be explained that for an integer of the form $(3^m + \omega)(3^m + \overline{\omega})$ to be a prime number, a necessary condition is that m is a power of 2. We will present some details concerning a primality test using elliptic curves, which was introduced by Denomme and Savin in 2008.

2 Mersenne Numbers

In order to find a neseccary and sufficient condition for the primality of Mersenne numbers, we first define a recurrence relation.

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

Theorem 1. *M_n with $n > 2$ is a prime number if and only if $a_{n-2} \equiv 0 \bmod M_n$.*

The proof of this theorem is based on 4 lemmas. But before stating these, first state some definitions.

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

The proof of theorem 1 makes use of

$$G := Z(x^2 - 3y^2 - 1).$$

So G consists of pairs (a, b) satisfying $a^2 - 3b^2 = 1$.

Definition 2. *Let K be a field. Then*

$$G(K) := \{(x, y) \in K \times K| \quad x^2 - 3y^2 = 1\}$$

is an abelian group, with zero element $(1, 0)$ and group operation will be defined as follows:

$$(x_1, y_1) + (x_2, y_2) := (x_1x_2 + 3y_1y_2, x_1y_2 + x_2y_1).$$

It is not hard to show that $G(K)$ is indeed an abelian group. Every element $(x, y) \in G$ has an inverse, given by $(x, y)^{-1} = (x, -y)$. Note that $(x, y) \in G$ implies that $(x, -y) \in G$. Details are found in appendix A on page 22. The last thing we need to show is that the sum of every two elements of G is also an element of G. We know that

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 + 3y_1y_2, x_1y_2 + x_2y_1)$$

If we fill in this point in the polynomial, we get the following:

$$\begin{aligned}(x_1x_2 + 3y_1y_2)^2 - 3(x_1y_2 + x_2y_1) - 1 =& x_1^2x_2^2 + 6x_1x_2y_1y_2 + 9y_1^2y_2^2 - 3x_1^2y_1^2 \\ &+ 3x_1x_2y_1y_2 + 3x_2^2y_1^2 - 1 \\ =& x_1^2x_2^2 - 3x_1^2y_2^2 - 3x_2^2y_1^2 + 9y_1^2y_2^2 - 1 \\ =& (x_1^2 - 3y_1^2)(x_2^2 - 3y_2^2) - 1 \\ =& 0\end{aligned}$$

Thus $(x_1, y_1) + (x_2, y_2) \in G, \quad \forall (x_1, y_1), (x_2, y_2) \in G.$

The first lemma describes the relation between the recurrence relation and the group. Note that $(2, 1) \in G$.

Lemma 1. $2 \cdot (x \text{ coordinate of } 2^k(2,1)) = a_k$.

Proof. The proof of this lemma is done by induction. Note that for $k = 0$, both sides of the equation equal 4 and therefore the base step holds. For the inductive step, assume $2 \cdot (x \text{ coordinate of } 2^k(2,1)) = a_k$. For the righthand side we know $a_{k+1} = a_k^2 - 2$. For the lefthand side $2^{k+1}(2,1)) = 2 \cdot 2^k(2,1) = 2 \cdot (\frac{a_k}{2}, *)$. Since $(\frac{a_k}{2}, *)$ has to be an element of the group, we know that $(\frac{a_k}{2})^2 - 3\,*^2 - 1 = 0$, thus $3*^2 = (\frac{a_k}{2})^2 - 1$. Thus

$$2 \cdot (\frac{a_k}{2}, *) = (\frac{a_k^2}{4} + 3*^2, \mu) = (\frac{a_k^2}{4} + \frac{a_k^2}{4} - 1, \mu)$$

for some μ.

Therefore we conclude that

$$2 \cdot (x \text{ coordinate of } 2^{k+1}(2,1)) = 2 \cdot (x \text{ coordinate of } (\frac{a_k^2}{2} - 1, \mu) = 2 \cdot (\frac{a_k^2}{2} - 1) = a_{k+1}$$

which proves the lemma. □

2.1 Finding the square root of 6 in $\mathbb{F}_q$

Definition 3. *Let R be a ring.* $R^{*2} := \{x \in R^* | \exists y \in R : x = y^2\} \subset R^*$

For proving the next lemma, we want to find specific values for q such that $6 \in \mathbb{F}_q^{*2}$. We do this by expressing $\sqrt{6}$ in terms of roots of unity. This is done in analogy with the same problem over the complex numbers.

In $\mathbb{C}$, we want to find an element a such that $a^2 = 6$. Consider

$$\begin{array}{rcccl} \epsilon & := & e^{\frac{2\pi i}{3}} & = & -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \\ \beta & := & e^{\frac{2\pi i}{8}} & = & \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{-2} \\ \gamma := \epsilon\beta & := & e^{\frac{11\pi i}{12}} & = & \frac{1}{4}(-1 + \sqrt{-3})(\sqrt{2} + \sqrt{-2}) \end{array}$$

Eliminating the parenthesis will yield in a expression with $\sqrt{6}$ in it. Namely

$$\gamma = \frac{1}{4}(-\sqrt{2} - \sqrt{-2} + \sqrt{-6} + \sqrt{6})$$

Adding its complex conjugate to this, the complex parts will cancel out.

$$\gamma + \frac{1}{\gamma} = \frac{1}{2}(\sqrt{6} - \sqrt{2})$$

Note that $\beta + \frac{1}{\beta} = \sqrt{2}$. Therefore $2\gamma + \frac{2}{\gamma} + \beta + \frac{1}{\beta} = \sqrt{6}$. In this way we constructed the square root of $6 \in \mathbb{C}$.

Proposition 1. *If the characteristic of $\mathbb{F}_q$ is not equal to 2 or 3,* $6 \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv 1, 5, 19, 23 \bmod 24$.

Proof. Taking a similar approach as the complex numbers, consider $\Omega = \Omega_{\mathbb{F}_q}^{X^{24}-1}$, the splitting field of $X^{24}-1$. By definition of the splitting field, $\exists \alpha \in \Omega$: $ord(\alpha) = 24$. Thus $\alpha^{24} = 1, \alpha^{12} = -1$. Analogous to the complex numbers, consider

$$(2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3})^2 \tag{1}$$

When this expression equals 6, we have found the square root of 6.

$$\begin{aligned}(2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3})^2 &= 4\alpha^2 + \frac{4}{\alpha^2} + \alpha^6 + \frac{1}{\alpha^6} + 8 - 4\alpha^4 - \frac{4}{\alpha^2} - 4\alpha^2 - \frac{4}{\alpha^4} + 2 \\ &= \frac{\alpha^{12} - 4\alpha^{10} + 10\alpha^6 - 4\alpha^2 + 1}{\alpha^6}\end{aligned}$$

Since we know that α has order 24, $\alpha^{12} = -1$, thus $\alpha^{12} + 1 = (\alpha^4)^3 + 1 = 0$, therefore we may conclude that $(\alpha^4 + 1)(\alpha^8 - \alpha^4 + 1) = 0$. Since $ord(\alpha) = 24, \alpha^4 \neq -1$. Therefore $\alpha^8 = \alpha^4 - 1$. Combining these results, we see that expression 1 is equal to

$$\begin{aligned}\frac{-4\alpha^{10} + 10\alpha^6 - 4\alpha^2}{\alpha^6} &= \frac{-4\alpha^8 + 10\alpha^4 - 4}{\alpha^4} \\ &= \frac{-4\alpha^4 + 4 + 10\alpha^4 - 4}{\alpha^4} \\ &= \frac{6\alpha^4}{\alpha^4} \\ &= 6\end{aligned}$$

Therefore we may conclude that:

$$(2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3})^2 = 6$$

Now we are only interested in the question whether $\beta := 2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3} \in \mathbb{F}_q$. This is the case when it is a root of $x^q - x$. So we need to find all possibilities of q such that

$$2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3} = (2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3})^q \tag{2}$$

Note that $\beta^q = (2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3})^q = (2\alpha)^q + (\frac{2}{\alpha})^q - (\alpha^3)^q - (\frac{1}{\alpha^3})^q = 2\alpha^q + \frac{2}{\alpha^q} - (\alpha^q)^3 - \frac{1}{(\alpha^q)^3}$. Observe that if $q \equiv x \bmod 24$, it suffices to look whether β^x is equal to β, since every factor α^{24} is equal to 1.

By assumption, the characteristic is not equal to 2 or 3. Thus the only possibilities for q that are left are $q \equiv 1, 5, 7, 11, 13, 17, 19, 23 \bmod 24$. Note that if $q \equiv x \bmod 24$ satisfies the equation if and only if $q \equiv -x \bmod 24$ satisfy the equation. Since $\alpha^{24} = 1$, we know that for $q \equiv \pm 1 \bmod 24$, equation 2 holds.

For $q \equiv \pm 5$, we get

$$\begin{aligned}
\beta^q &= 2\alpha^5 + \frac{2}{\alpha^5} - \alpha^{15} - \frac{1}{\alpha^{15}} \\
&= 2\alpha^5 - 2\alpha^7 + \alpha^3 + \frac{1}{\alpha^3} \\
&= 2\alpha^5 - 2\alpha^3 + \frac{2}{\alpha} + \alpha^3 + \frac{1}{\alpha^3} \\
&= 2\alpha - \frac{2}{\alpha^3} + \frac{2}{\alpha} - \alpha^3 + \frac{1}{\alpha^3} \\
&= 2\alpha + \frac{2}{\alpha} - \alpha^3 - \frac{1}{\alpha^3} \\
&= \beta
\end{aligned}$$

Therefore if $q \equiv \pm 5 \bmod 24$, $6 \in \mathbb{F}_q^{*2}$

For $q \equiv \pm 7 \bmod 24$, we have

$$\begin{aligned}
\beta^q &= 2\alpha^7 + \frac{2}{\alpha^7} - \alpha^{21} - \frac{1}{\alpha^{21}} \\
&= 2\alpha^3 - \frac{2}{\alpha} - 2\alpha^5 + \alpha^9 + \frac{1}{\alpha^9} \\
&= 2\alpha^3 - \frac{2}{\alpha} - 2\alpha + \frac{2}{\alpha^3} + \alpha^5 - \alpha - \alpha^3 \\
&= 2\alpha^3 - \frac{2}{\alpha} - 2\alpha + \frac{2}{\alpha^3} + \alpha - \frac{1}{\alpha^3} - \alpha - \alpha^3 \\
&= -2\alpha - \frac{2}{\alpha} + \alpha^3 + \frac{1}{\alpha^3} \\
&= -\beta
\end{aligned}$$

Therefore if $q \equiv \pm 7 \bmod 24$, $6 \notin \mathbb{F}_q^{*2}$

For $q \equiv \pm 11 \bmod 24$, we have

$$\begin{aligned}
\beta^q &= 2\alpha^{11} + \frac{2}{\alpha^{11}} - \alpha^{33} - \frac{1}{\alpha^{33}} \\
&= \frac{2}{\alpha} - 2\alpha - \alpha^9 - \frac{1}{\alpha^9} \\
&= -2\alpha - \frac{2}{\alpha} + \frac{1}{\alpha^3} + \alpha^3 \\
&= -\beta
\end{aligned}$$

Therefore if $q \equiv \pm 11 \bmod 24$, $6 \notin \mathbb{F}_q^{*2}$ □

Lemma 2. *Let M_n be a prime number with n odd. Then $(2,1) \in G$ is not divisible by 2 in $G(\mathbb{F}_{M_n})$*

Proof. We want to know whether the element $(2,1)$ is divisible by 2, that is

$$\exists (x,y) \in G : (x,y) + (x,y) = (2,1)$$

If such point exists, it has to satisfy the following equations:

$$\begin{cases} x^2 - 3y^2 &= 1 \\ x^2 + 3y^2 &= 2 \\ 2xy &= 1 \end{cases}$$

Subtracting the first equation from the second, it follows that $6y^2 = 1$ and by proposition 1 there exists a solution in $G(\mathbb{F}_q)$ if and only if $6^{-1} \in \mathbb{F}_q^{*2}$. Note that $\mathbb{F}_q^{*2}$ is a group therefore it is sufficient to show that $6 \in \mathbb{F}_q^{*2}$

Considering the Mersenne numbers, we see that $M_n = 2^n - 1 \equiv (-1)^n - 1 \bmod 3$. For odd n, we see that $M_n \equiv 1 \bmod 3$. For $n \geq 3$, $8 | M_n + 1$. Therefore $M_n \equiv 7 \bmod 8$. Combining these two gives us that $M_n \equiv 7 \bmod 24$ for $n \geq 3$ and odd. Therefore we may apply proposition 1 and conclude that $(2,1)$ is not divisible by 2 in $G(\mathbb{F}_{M_n})$. □

2.2 Number of elements of $G(\mathbb{F}_{M_n})$

Let $\mathbb{F}_q$ be a finite field of cardinality q.

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

$$\#G(\mathbb{F}_q) = \begin{cases} q - 1 & \text{if } q \equiv 1, 11 \bmod 12 \\ q + 1 & \text{if } q \equiv 5, 7 \bmod 12 \end{cases}$$

Proof. To find $\#G(\mathbb{F}_q)$ for characteristics different than 2 or 3, we make a relation between $G(\mathbb{F}_q) \backslash \{(1,0)\}$ and the set of linear relations between y and x of the form $y = \gamma(x-1)$, $\gamma \in \mathbb{F}_q$. The latter set has q elements. We do this with the following map:

$$f : (a,b) \mapsto y = \frac{b}{a-1}(x-1)$$

$(1,0)$ is the only element in $G(\mathbb{F}_q)$ with x-coordinate 1, thus $a - 1 \neq 0$, and therefore this is a well defined map. To see whether the map is injective, we see if two different elements can be mapped to the same line. So assume $\frac{b}{a-1} = \frac{d}{c-1}$ This results in the following set of equations:

$$\begin{cases} a^2 - 3b^2 &= 1 \\ c^2 - 3d^2 &= 1 \\ b(c-1) &= d(a-1) \end{cases}$$

Combining the first and third equation, we get

$$\begin{aligned} & a^2 - 1 &&= \tfrac{3d^2(a-1)^2}{(c-1)^2} \\ \Rightarrow \quad & a + 1 &&= \tfrac{3d^2(a-1)}{(c-1)^2} \\ \Rightarrow \quad & a(1 - \tfrac{3d^2}{(c-1)^2}) &&= -1 - \tfrac{3d^2}{(c-1)^2} \\ \Rightarrow \quad & a &&= \tfrac{-(c-1)^2 - 3d^2}{(c-1)^2 - 3d^2} \end{aligned}$$

Since $3d^2 = c^2 - 1$, this implies

$$\begin{aligned} a &= \tfrac{-(c-1)^2 - c^2 + 1}{(c-1)^2 - c^2 + 1} \\ &= \tfrac{-(c-1) - c - 1}{(c-1) - c - 1} \\ &= \tfrac{-2c}{-2} \\ &= c \end{aligned}$$

By the third equation of the system $b = d$ thus the image is injective.

Conversely,

$$f^{-1}(\quad y = t(x-1) \quad) = \{(a,b) | a^2 - 3b^2 = 1, a \neq 1, t = \frac{b}{a-1}\}$$

Combining these gives

$$\begin{aligned} a^2 - 3t^2(a-1)^2 - 1 = 0 \\ (a-1)(a+1-3t^2(a-1)) = 0 \end{aligned}$$

Since $a \neq 1$, the second factor has to be equal to zero, thus

$$a(1 - 3t^2) + 1 + 3t^2 = 0$$

Filling this in gives us the unique a and b satisfying this set of equations, therefore the inverse is defined as follows:

$$f^{-1} : y = t(x-1) \mapsto (\frac{3t^2+1}{3t^2-1}, \frac{2t}{3t^2-1})$$

A little care is required when $3^{-1} \in G(\mathbb{F}_q)^{*2}$, since the inverse isn't well defined in that case, because the relation $y = \pm 3^{-1}(x-1)$ can not be mapped to an element of $G(\mathbb{F}_q) \backslash \{(1,0)\}$. Therefore

$$\#G(\mathbb{F}_q)\backslash\{(1,0)\} = \begin{cases} q & \text{if } 3^{-1} \notin G(\mathbb{F}_q)^{*2} \\ q-2 & \text{if } 3^{-1} \in G(\mathbb{F}_q)^{*2} \end{cases}$$

Thus we want to know whether $3 \in \mathbb{F}_q^{*2}$.

Considering the same technique as on page 6, we want to see when $3 \in \mathbb{F}_q^{*2}$. Consider $\Omega = \Omega_{\mathbb{F}_q}^{x^{12}-1}$. Let $\alpha \in \Omega$ be the element of order 12. Thus $\alpha^{12} = 1$,

$\alpha^6 = -1$. Therefore $(\alpha^2+1)(\alpha^4-\alpha^2+1) = 0$ and $\alpha^4 - \alpha^2 + 1 = 0$ because $\alpha^2 \neq -1$. So

$$\begin{aligned}(\alpha + \frac{1}{\alpha})^2 &= \alpha^2 + 2 + \frac{1}{\alpha^2} \\ &= \alpha^2 + 2 - \alpha^4 \\ &= \alpha^4 + 1 + 2 - \alpha^4 \\ &= 3\end{aligned}$$

Now we want to find all q that satisfy

$$(\alpha + \frac{1}{\alpha})^q = \alpha + \frac{1}{\alpha} \tag{3}$$

Note that the only values for q mod 12 that are possible are $\pm 1, \pm 5$. All the others cannot occur because the characteristic has to be 2 or 3 in that case. Consider the four cases that are left.

$q \equiv 1 \bmod 12$
Trivial. Satisfies condition 3.

$q \equiv 5 \bmod 12$
$(\alpha + \frac{1}{\alpha})^q = \alpha^5 + \frac{1}{\alpha^5} = -\frac{1}{\alpha} - \alpha$. So this does not satisfy condition 3.

$q \equiv 7 \bmod 12$
$(\alpha + \frac{1}{\alpha})^q = \alpha^7 + \frac{1}{\alpha^7} = -\alpha - \frac{1}{\alpha}$ So it does not satisfy condition 3.

$q \equiv 11 \bmod 12$
$(\alpha + \frac{1}{\alpha})^q = \alpha^{11} + \frac{1}{\alpha^{11}} = \frac{1}{\alpha} + \alpha$. So it does satisfy condition 3.

Therefore we may conclude that:

$$\#G(\mathbb{F}_q) = \begin{cases} q-1 & \text{if } q \equiv 1, 11 \bmod 12 \\ q+1 & \text{if } q \equiv 5, 7 \bmod 12 \end{cases}$$

□

Corollary 1. *Assume M_n is prime and $n \geq 3$. $\#G(\mathbb{F}_{M_n}) = M_n + 1 = 2^n$.*

Proof. This is a direct consequence of lemma 3 and the fact that $M_n \equiv 7 \bmod 24$ thus $M_n \equiv 7 \bmod 12$ □

2.3 Determining the elements of order 4 in $G(K)$.

The next lemma describes the elements of order 4 in the group $G(K)$. If the characteristic of K is equal to 2, all elements except the unit are of order 2. If the characteristic is not equal to 2, an element of order two must satisfy the

following equations:

$$\begin{cases} x^2 + 3y^2 & = 1 \\ 2xy & = 0 \\ x^2 - 3y^2 & = 1 \\ (x, y) & \neq (1, 0) \end{cases}$$

It follows easily that only $(-1, 0)$ satisfies this set of equations.

Now we want to find elements of order 4 in $G(K)$. If the characteristic is 2 or 3, we clearly have no elements of order 4. Note that in characteristic 3, we also have no elements with x-coordinate 0. For elements of order 4 in characteristic different than 2 or 3, we state the following lemma.

Lemma 4. *Let $a \in G(K)$. If the characteristic of K is not equal to 2, the order of a is 4 if and only if the x-coordinate of a equals 0.*

Proof. For finding elements of order 4, thus $(u, v) + (u, v) = (-1, 0)$, we need to solve the following set of equations.

$$\begin{cases} u^2 - 3v^2 & = -1 \\ u^2 + 3v^2 & = 1 \\ 2uv & = 0 \end{cases}$$

By a simple calculation it follows that the only elements of order 4 are the elements $(0, \pm\frac{1}{\sqrt{3}})$.
The other way around. Assume a has an x-coordinate equal to 0. Since a is an element of the group $G(K)$ we have $3y^2 = 1$ and therefore the y-coordinate of a is equal to $\pm\frac{1}{\sqrt{3}}$ and in both cases a is an element of order 4. □

Now that the four lemmas are stated and proved, one can prove the Mersenne primality condition.

Proof of theorem 1. Assume M_n is prime, $n > 2$. Since $2^n - 1 \equiv (-1)^n - 1 \equiv 0 \bmod 3$ for n even, we may conclude that n is odd. Therefore the characteristic of $G(\mathbb{F}_{M_n})$ is not equal to 2. Note that in the proof of lemma 4 we saw that $(-1, 0)$ is the only element of order 2. By corollary 1 we have that $\#G(\mathbb{F}_{M_n}) = 2^n$ and therefore $G(\mathbb{F}_{M_n}) \simeq \mathbb{Z}/2^n\mathbb{Z}$. By lemma 2, we have that $(2, 1)$ is not divisible by 2, thus this element generates the group and has order 2^n. Therefore $2^{n-2}(2, 1)$ has order 4. By lemma 4 we have that the x-coordinate equals 0 and therefore by lemma 1 we can conclude that $a_{n-2} \equiv 0 \bmod M_n$.
Assume $a_{n-2} \equiv 0 \bmod M_n$. If $p|M_n$, then $a_{n-2} \equiv 0 \bmod p$. Note that $p = 2$ implies that M_n is even which is not possible. Since the characteristic is not 2, by lemma 4 we have that there is an element of order 4. Therefore the characteristic is not 3 and thus n is odd. In $G(\mathbb{F}_p)$ we get thus that $2^{n-2}(2, 1) = (0, \pm\frac{1}{\sqrt{3}})$. Thus by lemma 1, $2^{n-2}(2, 1)$ has order 4 in $G(\mathbb{F}_p)$. Therefore $(2, 1)$ has order 2^n. Since the order of an element is a divisor of the number of elements in the

group, we get that $2^n \leq \#G(\mathbb{F}_p)$. In the proof of lemma 3 we saw that the maximum possible numbers of elements in the group is $p+1$, so

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

Which implies $p \geq 2^n - 1 = M_n$. Therefore M_n is prime.

□

3 Primality of K_ℓ

In the next section another primality test is described. The proof of the test involves elliptic curves, but the theorem itself is stated without them. Let $K_\ell := 3^{2^\ell} - 3^{2^{\ell-1}} + 1$ and $f(x) := \frac{-30x^3-1}{90x^2}$.

For $n > 1$ we write f^n for the composition $f \circ f \circ \ldots \circ f$ (composing f n times).

Theorem 2. *K_ℓ is prime if and only if $f^{2^\ell-1}(\frac{1}{2}) \equiv 0 \bmod K_\ell$ (and $f(\frac{1}{2}) \bmod K_\ell$, $f^2(\frac{1}{2}) \bmod K_\ell, \ldots, f^{2^\ell-1}(\frac{1}{2}) \bmod K_\ell$ are all well-defined).*

As remarked above, the proof of this statement uses elliptic curves. An introduction to the theory of such curves is, e.g., the textbook [8] written by J. Tate and J. Silverman. An elliptic curve over a field K (of characteristic $\neq 2$) is a curve E given by an equation $y^2 = ax^3 + bx^2 + cx + d$, with $a, b, c, d \in K$ satisfying the condition that $ax^3 + bx^2 + cx + d$ is a polynomial of degree 3 without multiple zeros. Moreover, one adds a point O 'at infinity'. The set $E(K)$ consisting of all points on the curve with $x, y \in K$ together with the point O is in fact an abelian group. Here O is the unit element, the inverse of any point $(x, y) \in E(K)$ is the point $(x, -y)$, and $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ precisely when (x_1, y_1), (x_2, y_2), $(x_3, -y_3)$ are the intersection points of E with a line.

3.1 Part of the proof of the theorem

To prove this theorem, we first state another theorem that almost directly implies theorem 2. Let $E : y^2 = 30x^3 + \frac{1}{4}$, which defines an elliptic curve over the field K provided the characteristic of K is not 2 and not 3 and not 5. Moreover, assume $\omega := \frac{-1+\sqrt{-3}}{2} \in K$. This is an element of order 3 in the group K^*. Note that $K_\ell = k_\ell \bar{k_\ell}$ with $k_\ell = -1 - 3^{2^{\ell-1}}\omega$. Here K_ℓ is regarded as an element of the prime field of K, so it is $K_\ell \bmod p$ in case the characteristic is $p > 0$. Moreover, $\bar{k_\ell}$ means that ω is replaced by ω^2 (which is the complex conjugate of ω in case $K \subset \mathbb{C}$). Furthermore we define $\rho : E \to E, (x, y) \mapsto (\omega x, y)$. This is a homomorphism $E(K) \to E(K)$ in case $\omega \in K$.

Theorem 3. *$P := (\frac{1}{2}, 2)$ is a point on the elliptic curve E. K_ℓ is prime if and only if*

$$(\rho - \rho^2)^{2^\ell-1} \cdot P \equiv (0, \pm\frac{1}{2}) \bmod k_\ell.$$

In this thesis, I will not give a proof of the "only if" part. For a complete proof see the article of Silverberg[3] or the article of Denomme and Savin[5] Before proving the theorem, some useful propositions are stated and proved.

Proposition 2. *$K_\ell \in \mathbb{Z}$ is prime if and only if $k_\ell \in \mathbb{Z}[\omega]$ is irreducible.*

Proof. Assume $K_\ell \in \mathbb{Z}$ is prime. Assume there exist $a, b \in \mathbb{Z}[\omega]$ such that $k_\ell = a \cdot b$. Then $K_\ell = k_\ell \cdot \bar{k_\ell} = a \cdot \bar{a} \cdot b \cdot \bar{b}$. Note that $a \cdot \bar{a} \in \mathbb{Z}$ and $b \cdot \bar{b} \in \mathbb{Z}$. Since

K_ℓ is prime by assumption, $a \cdot \bar{a} = 1$ or $b \cdot \bar{b} = 1$. Therefore a or b is unit and therefore k_ℓ is irreducible.
The other way around, assume k_l is irreducible. Since $\mathbb{Z}[\omega]$ is Euclidean and therefore a principal ideal domain, this implies that $(k_\ell) \subset \mathbb{Z}[\omega]$ is a maximal ideal and therefore $\frac{\mathbb{Z}[\omega]}{k_\ell}$ is a field. By Proposition 3, this field has $N(k_\ell) = K_\ell = p^n$ elements, for some p prime and $n \in \mathbb{Z}$. Since $p|K_\ell$, we get

$$3^{2^\ell} - 3^{2^{\ell-1}} + 1 \equiv 0 \bmod p$$

Define $x := 3^{2^{\ell-1}}$, for convenience. Now $x^2 - x + 1 \equiv 0 \bmod p$ which implies $x^3 + 1 = (x+1)(x^2 - x + 1) \equiv 0 \bmod p$. Therefore $x^6 \equiv 1 \bmod p$. We know therefore that the order of $x \bmod p \in \{1, 2, 3, 6\}$. The order of x equal to 1 implies that $x = 1$, hence $1 = x^2 - x + 1 = 0$ in $\mathbb{F}_p$. This contradicts the fact that p is prime. The order of x equal to 2 implies that $x = -1$, hence $x^2 - x + 1 = 3 = 0$ in $\mathbb{F}_p$. This contradicts the fact that $K_\ell \equiv 1 \bmod 3$. Order 3 contradicts the fact that $x^3 \equiv -1 \bmod p$. Therefore $ord(x) = ord(3^{2^{l-1}}) = 6$. Therefore $6|p-1$. And thus $p \equiv 1 \bmod 6$.
Note that

$$\frac{\mathbb{Z}[\omega]}{(p)} = \frac{\mathbb{F}_p[x]}{(x^2 + x + 1)},$$

and $x^2 + x + 1 \in \mathbb{F}_p[x]$ is reducible because $p \equiv 1 \bmod 6$. From [6], it follows that p is reducible in $\mathbb{Z}[\omega]$. Write $p = u \cdot \alpha_1 \cdot \alpha_2 \cdots \alpha_t$, with $t \geq 2$, $u \in \mathbb{Z}[\omega]^*$, and α_i irreducible. Now

$$K_\ell = k_\ell \cdot \bar{k_\ell} = p^n = u^n \cdot \alpha_1^n \cdot \alpha_2^n \cdots \alpha_t^n$$

but since k_ℓ and $\bar{k_\ell}$ are irreducible, their product consists of exactly 2 irreducible factors. Therefore p^n consists of two irreducible factors and thus $t = 2$ and $n = 1$. Therefore we conclude that K_ℓ is prime. □

Proposition 3. *Consider* $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(x^2 - ax - b)$, *with* $\alpha = x \bmod (x^2 - ax - b)$ *for some* $a, b \in \mathbb{Z}$. *For any* $(n, m) \in \mathbb{Z}$ *with* $(n, m) \neq (0, 0)$ *one has*

$$\#\frac{\mathbb{Z}[\alpha]}{(n + m\alpha)} = |N(n + m\alpha)|.$$

Proof. Consider the additive group of $\mathbb{Z}[\alpha]$. The map $f : \mathbb{Z}[\alpha] \to \mathbb{Z}^2, \quad c + c\alpha \mapsto (c, d)$ is a group isomorphism. The subgroup $(n + m\alpha)$ is generated by $n + m\alpha$ and $(n + m\alpha) \cdot \alpha = n\alpha + ma\alpha + mb$. These generators are mapped under f to (n, m) and $(mb, n + ma)$, respectively. Now

$$\frac{\mathbb{Z}^2}{(n, m)\mathbb{Z} + (mb, n + ma)\mathbb{Z}} \simeq \frac{\mathbb{Z}[\alpha]}{(n + m\alpha)}$$

As seen in [1], if

$$det \begin{pmatrix} n & m \\ mb & n + ma \end{pmatrix} \neq 0$$

the number of elements of $\frac{\mathbb{Z}^2}{(n,m)\mathbb{Z}+(mb,n+ma)\mathbb{Z}}$ is equal to the absolute value of this determinant. Thus

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

□

Proof of theorem 3. $\Leftarrow$: Suppose p is a prime divisor of K_ℓ. From the proof of Proposition 2 we know $p \equiv 1 \bmod 6$, hence $p = \pi\overline{\pi}$ for some irreducible $\pi \in \mathbb{Z}[\omega]$. Then $\mathbb{Z}[\omega]/(\pi) =: \mathbb{F}_p$ is a finite field with p elements. We have the homomorphism $\rho : E(\mathbb{F}_p) \to E(\mathbb{F}_p), (x,y) \mapsto (\omega x, y)$. Then $(\rho^2 + \rho + id)(x,y) = (\omega^2 x, y) + (\omega x, y) + (x,y) = O$ for every $(x,y) \in E$. Thus $\rho^2 = -\rho - id$. Consider a point $Q := (x,y) \in E$. Note that

$$\begin{aligned} x =& 0 \\ \iff & \\ \rho(Q) =& \quad Q \\ \iff & \\ (1-\rho)(Q) =& \quad O \\ \iff & \\ (\rho - \rho^2)(Q) =& \quad O. \end{aligned}$$

Note that $\rho - \rho^2 = \rho - (-\rho - id) = 2\rho + id$; the calculation above shows that the kernel of this map consists of O together with the points $(x,y) \in E$ with $x = 0$, i.e., the points $(0, \pm\frac{1}{2})$. Consider the map

$$f : \mathbb{Z}[\omega] \to E(\mathbb{F}_p), \quad n + m\omega \mapsto (n + m\rho)P$$

This is a homomorphism of $\mathbb{Z}[\omega]$-modules, hence its kernel is an ideal in $\mathbb{Z}[\omega]$. Since $\mathbb{Z}[\omega]$ is euclidean, the kernel is of the form (α). Recall that $(2\rho + id) \cdot (0, \pm\frac{1}{2}) = O$. By assumption $(2\rho + id)^{2^{\ell}-1} \cdot P = (0, \pm\frac{1}{2}) \in E(\mathbb{F}_p)$, hence $(2\rho + id)^{2^\ell} \cdot P = O$.

We see that $(2\omega+1)^{2^\ell} \in ker(f) = (\alpha)$ and $(2\omega+1)^{2^\ell - 1} \notin ker(f)$. Note that $2\omega + 1$ is irreducible in $\mathbb{Z}[\omega]$ because $N(2\omega + 1) = 3$.

Now we are going to find the decomposition in irreducible factors of (α). Since $\alpha | (2\omega+1)^{2^\ell}$ and $2\omega+1$ is irreducible, it follows that $\alpha = (2\omega+1)^k, \quad k \leq 2^l$. But from $(2\omega + 1)^{2^\ell - 1} \notin (\alpha)$, it follows that $2^\ell - 1 < k$. Combining these inequalities, we get $k = 2^\ell$ and thus $ker(f) = ((2\omega + 1)^{2^\ell})$. As a result,

$$f(\mathbb{Z}[\omega]) = \mathbb{Z}[\rho]P \simeq \frac{\mathbb{Z}[\omega]}{((2\omega+1)^{2^\ell})}.$$

From Proposition 3, one finds

$$\#E(\mathbb{F}_p) \geq \#f(\mathbb{Z}[\omega]) = \#\frac{\mathbb{Z}[\omega]}{((2\omega+1)^{2^l})} = N((2\omega+1)^{2^l}) = 3^{2^l}.$$

Applying the Hasse bound[2], we get that $\#E(\mathbb{F}_p) \leq (\sqrt{p}+1)^2$. So

$$(\sqrt{p}+1)^2 =\geq \#E(\mathbb{F}_p) \geq 3^{2^\ell} \geq 3^{2^\ell} - 3^{2^{\ell-1}} + 1 = K_\ell$$

Thus $\sqrt{p}+1 \geq \sqrt{K_\ell}$, which implies $p > \sqrt{K_\ell}$ provided $\ell > 1$. In case $\ell \leq 1$ the number K_ℓ is certainly a prime, and for $\ell > 1$ we showed that the condition of the theorem implies that every possible prime divisor of K_ℓ is larger than $\sqrt{K_\ell}$, which also implies that K_ℓ is prime. □

3.2 The particular form of K_ℓ

One may wonder why our K_ℓ has this particular form. Why a power of 2 for example? The proof of Proposition 2 shows that $3^{2n} - 3^n + 1$ is prime if and only if $3^n + \omega \in \mathbb{Z}[\omega]$ is irreducible.

Proposition 4. *$3^n + \omega$ is not irreducible in case n has prime divisors other then 2 and 3.*

Proof. The following identity plays an important role in the next proof. For n odd, we have

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1}) \tag{4}$$

If $n = pa$ for some prime $p > 3$, then

$$(3^a)^p + \omega^{1+3m} = 3^n + \omega = (3^a)^p + (\omega^{-1})^{2+3m}$$

for all $m \in \mathbb{N}$.

We pick m such that either $1+3m = p$, or $2+3m = p$ depending on p mod 3. Then by equation 4, k_ℓ is divisible by $3^a + \omega^{\pm 1}$ which completes the proof. □

Proposition 5. *For each $k \in \mathbb{N}, 3^{3^k} + \omega$ is not irreducible.*

Proof. Note

$$3^{2a+1} + \omega = ((1 - 2 \cdot 3^a)\omega + 1 - 3^a)((1 + 2 \cdot 3^a)\omega + 1 + 3^a))$$

For $a := \frac{3^k-1}{2}$, which is a natural number since 3^k is odd, this shows the proposition.

□

To conclude, if we want to generate a prime number of the form $k_\ell \cdot \bar{k_\ell}$, where $k_\ell := 3^n + \omega$, we have the necessary condition that n is of the form $n := 2^i \cdot 3^j$ with $i \geq 1$. For example the case $n = 6$ results is a prime number $3^{12} - 3^6 + 1 = 530713$. However in this text we restrict to the numbers where $j = 0$.

4 Generating primes

Now that we have found primality conditions, one may want to apply this conditions to find prime numbers. Here is some Maple code to find these kind of primes and some examples of the primes generated by this code.

With a simple algorithm that calculates the values of $a_{n-2} \bmod M_n$, we can easily find large prime numbers.

Listing 1: Finding Mersenne Primes

```
for n from 2 to 4500 do
  Mn := (2^n-1);
  A:= 4;
  for i from 1 to (n-2) do
    A:= (A^2-2) mod Mn;
  end do
  if A=0
    then print(n);
  end if
end do:
```

After a few iterations we already find some prime numbers. We see that M_n is prime for $n = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423$. Note that $2^{4423} - 1 \approx 10^{1331}$. The found prime number thus already has more than thousand decimal digits.

For the numbers K_ℓ, the condition we have found is not very easy to calculate. Therefore we adjust the test a bit to make it easier to calculate with. As one can see in appendix B, we have $(\rho - \rho^2)(x, y) = (\frac{-\frac{1}{3}x^3 - \frac{1}{90}}{x^2}, \xi)$ with ξ such that the point is in E. To implement the condition of theorem 3, one iterates $f(x) = \frac{-\frac{1}{3}x^3 - \frac{1}{90}}{x^2}$. Then $f^{2^l-1}(\frac{1}{2}) \equiv 0 \bmod K_l$ implies K_l is prime. We convert this to the following algorithm to find prime numbers.

```
for l to 8 do
  Kl := 3^(2^l)-3^(2^(l-1))+1;
  x := 1/2;
  for n to 2^l-1 do
    x := `mod`((-(1/3)*x^3-1/90)/x^2, Kl)
    end do;
  if x = 0 then
    print(l)
  end if
end do
```

With this algorithm we found 3 primes, namely $K_1 = 7$, $K_2 = 73$ and $K_3 = 6481$.

5 Results

One may wonder whether this test can be used to find prime large prime numbers efficiently. Do these tests even generate infinitely many prime numbers? The following tests have run for 20 minutes each on a regular computer. See the results below

Prime	Digits of largest found number	computation time
M_{4423}	≈ 1331	20 min
K_3	4	20 min

6 Explanation of the results

One may wonder why the test for Mersenne primes generate a significantly more primes than the K_ℓ test. In this section some plausible arguments are given for this results.

Definition 4. *Let $\pi(x)$ denote the number of primes lower or equal to x.*

Theorem 4 (Prime Number Theorem)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{x} \ln(x) = 1$$

For the proof of the Prime Number Theorem and further reading, see [7]. This is equivalent to saying that $\pi(x)$ behaves asymptotically the same as $\frac{x}{\ln x}$,

$$\pi(x) \approx \frac{x}{\ln x}$$

Consider the interval $[1, \ldots, x]$, if we take a number random in this interval, the probability that this number is prime is roughly $\frac{1}{\ln x}$. With a little abuse of the random choosing, we pick K_ℓ from the interval $[1, \ldots, K_\ell]$. The probability that this is prime is $\frac{1}{\ln K_\ell}$. Thus the expected number of primes of the form K_ℓ is

$$\sum_{\ell=0}^{\infty} \frac{1}{\ln K_\ell} \approx 0.975\cdots .$$

We already found 3 primes K_ℓ which is more that the expected number based on the above heuristics. Unfortunately, we cannot prove that no more such primes exist. As mentioned before, the exponents of K_ℓ do not necessary involve only a pure power of two. It can also be of the form $3^{2^k 3^{\ell-1}} - 3^{2^{k-1} 3^{\ell-1}} + 1$. When using the same approximation for the number of prime numbers, we find a slightly higher expected number, since that sum will also converge. Thus this yield also in a finite amount of prime numbers. We conclude that most likely the method for finding primes of the form K_ℓ will not produce large prime numbers.
In contrast to the Mersenne numbers, where the exponent is quite simple, we

suspect that this method will produce infinite number of prime numbers. If we consider the same infinite sum for the Mersenne numbers, we see that

$$\sum_p \frac{1}{\ln M_p} = \sum_p \frac{1}{\ln 2^p - 1} \geq \sum_p \frac{1}{\ln 2^p} = \frac{1}{\ln 2} \sum_p \frac{1}{p}$$

where we sum over all prime numbers p. This is a diverging sum, as was proven by Euler in 1744. See a modified proof of this this argument in [4]. So one expects that an infinite number of Mersenne primes exist.

7 Conclusion

In conclusion, we have found and proven primality conditions for the numbers M_n and K_ℓ. When we used them to find large prime numbers, we found two main differences between the two tests: M_n from which we suspect that it will generate infinite prime numbers and K_ℓ from which we suspect that if will generate a finite amount of prime numbers. Further research can be done to find theorems that support this conjecture. In the proof of the Mersenne primality condition, we only used that $M_n \equiv 7 \bmod 24$. We can adjust our arguments easily to generate primes of other forms. One may perform research on these kind of numbers.

A The group $G := Z(x^2 - 3y^2 - 1)$

To prove that $G := Z(x^2 - 3y^2 - 1) \subset \mathbb{A}^2$ is a algebraic abelian group, we check whether it satisfies the four group properties.

(G1)

Let $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in G$. Now

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1x_2 + 3y_1y_2, x_1y_2 + x_2y_1) + (x_3, y_3)$$

$$= (x_1x_2x_3+3x_1y_2y_3+3y_1x_2y_3+3y_1y_2x_3, 3y_1y_2y_3+x_1x_2y_3+x_1y_2x_3+y_1x_2x_3)$$

On the other hand:

$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1, y_1) + (x_2x_3 + 3y_2y_3, x_2y_3 + x_3y_2)$$

$$= (x_1x_2x_3+3x_1y_2y_3+3y_1x_2y_3+3y_1y_2x_3, 3y_1y_2y_3+x_1x_2y_3+x_1y_2x_3+y_1x_2x_3)$$

Therefore $\forall x, y, z \in G, \quad (x + y) + z = x + (y + z)$.

(G2)

$(1, 0)$ Is the additive unit since

$$\forall (x, y) \in G, \qquad (x, y) + (1, 0) = (x \cdot 1 + 3 \cdot y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y)$$

(G3)

To see that $(x, -y)$ is actually the inverse of $(x, y) \in G$, consider $(x, y) + (x, -y) = (x^2-3y^2, xy-xy) = (1, 0)$, since (x, y) is a zero of the polynomial $x^2 - 3y^2 - 1$.

(G4)

$$(x_1, y_1) + (x_2, y_2) := (x_1x_2 + 3y_1y_2, x_1y_2 + x_2y_1)$$
$$= (x_2x_1 + 3y_2y_1, x_2y_1 + x_1y_2) = (x_2, y_2) + (x_1, y_1)$$

Since G is defined by a polynomial and addition and taking the inverse are maps given by polynomials, G is algebraic.

B Magma

The following commands are used to find a sufficient condition for finding K_l primes. The following code shows that $(\rho - \rho^2)(x, y) = (\frac{-\frac{1}{3}x^3 - \frac{1}{90}}{x^2}, \xi)$.

```
> Q:=Rationals();
> Pol<x>:=PolynomialRing(Q);
> K<w>:=ext<Q | x^2+x+1>;
> F<a>:=FunctionField(K);
> PF<T>:=PolynomialRing(F);
> L<b>:=ext<F | T^2-30*a^3-1/4>;
> E:=EllipticCurve([L!0,L!225]);
> P:=E![30*a,30*b];
> rho:=map<E->E | A :-> [w*A[1],A[2],A[3]]>;
> rho(P)-rho(rho(P));
((-10*a^3 - 1/3)/a^2 : (1/3*(20*w + 10)*a^3 + 1/9*(-4*w - 2))/a
    ^3*b : 1)
> Pt:=rho(P)-rho(rho(P));
> Pt[1]/30;
(-1/3*a^3 - 1/90)/a^2
```

Which produce the following result

```
(-1/3*a^3 - 1/90)/a^2
```

C Proof that $\mathbb{Z}[\omega]$ is Euclidean

$\mathbb{Z}[\omega]$ is Euclidean if

$$\forall a, b \in \mathbb{Z}[\omega], b \neq 0, \quad \exists q, r \in \mathbb{Z}[\omega] \text{ such that: } a = qb + r, \text{ with } |r|^2 < |b|^2$$

with the map $|\cdot|^2 : \mathbb{Z}[\omega] \to \mathbb{Z}_{\geq 0}$ defined as in [6].

Proposition 6. *$\mathbb{Z}[\omega]$ is Euclidean*

Proof. Write $a, b \in \mathbb{Z}[\omega]$ as $n + m\omega, k + l\omega$, respectively and assume $b \neq 0$. Then

$$\frac{a}{b} = \frac{n + m\omega}{k + l\omega} = \frac{(n + m\omega)(\overline{l + l\omega})}{|k + l\omega|^2} = \alpha + \beta\omega$$

for some $\alpha, \beta \in \mathbb{Q}$. Now pick $x \in \mathbb{Z}$ such that $|\alpha - x| \leq \frac{1}{2}$ and $y \in \mathbb{Z}$ such that $|\beta - y| \leq \frac{1}{2}$. Now if we take $q := x + y\omega \in \mathbb{Z}[\omega]$, then

$$\frac{a}{b} = q + \xi + \eta\omega$$

where $|\xi|, |\eta| \leq \frac{1}{2}$. Take $r := b(\xi + \eta\omega) = a - bq \in \mathbb{Z}[\omega]$. Then

$$|r|^2 = |b|^2|\xi + \eta\omega|^2 = |b|^2(\xi^2 - \xi\eta + \eta^2) \leq \frac{3}{4}|b|^2 < |b|^2$$

Therefore we may conclude that $\mathbb{Z}[\omega]$ is Euclidean with respect to the norm map $|\cdot|^2 : \mathbb{Z}[\omega] \to \mathbb{Z}_{\geq 0}$.

□

Bibliography

[1] J. Top, *Groepentheorie*. http://www.math.rug.nl/∼top/alg1.pdf, pages 105–119.

[2] J.H. Silverman, *An Introduction to the Theory of Elliptic Curves*. http://www.math.rug.nl/∼top/BenC.pdf, pages 49–69.

[3] A. Silverberg, *Some remarks on primality proving and elliptic curves*. 2014, pages 427–436.

[4] J. Top, http://www.math.rug.nl/∼top/lectures/carrousel8.pdf.

[5] R. Denomme, G. Savin, *Elliptic curve primality tests for Fermat and related primes*, Journal of Number Theory. 2008, pages 2398 – 2412.

[6] B. van Geemen, H.W. Lenstra, F. Oort, J.Top, *Algebraïsche Structuren*. http://www.math.rug.nl/∼top/dic.pdf, pages 90–91, 200–201.

[7] Dorian Goldfeld, *THE ELEMENTARY PROOF OF THE PRIME NUMBER THEOREM: AN HISTORICAL PERSPECTIVE*. http://www.math.columbia.edu/∼goldfeld/ErdosSelbergDispute.pdf.

[8] J. Tate and J. Silverman, *Rational Points on Elliptic Curves*. ISBN 978-1-4419-3101-6, 1992.