Mersenne primes of the form $x^2 + d \cdot y^2$

Bas Jansen

June 10, 2002

Contents

Introduction

Fermat's earliest interest in number theory grew out of the classical concept of a perfect number, one equal to the sum of all its proper divisors. Book IX of Euclid's *Elements* contains a proof that if $2^n - 1$ is prime, then $2^{n-1} \cdot (2^n - 1)$ is perfect. The Greeks had, however, only been able to discover four perfect numbers, $6, 28, 496$ and 8128, because it was difficult to determine the values of n for which $2^n - 1$ is prime. Fermat discovered three propositions that could help in this regard, propositions he communicated to Mersenne in a letter of June 1640. The first of these results was that if n is not itself prime, then $2^n - 1$ cannot be prime. The proof of this result just exhibited the factors: If $n = r \cdot s$, then

$$2^n - 1 = 2^{r \cdot s} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1).$$

The basic question therefore reduced to asking for which primes p is $2^p - 1$ prime. Such primes are today called Mersenne primes in honor of Fermat's favorite correspondent (I have quoted this from [Katz] page 458).

Definition 0.1 *Let $l \in \mathbb{N}$. The number $2^l - 1$ will be denoted by M_l. If M_l is prime we shall call M_l a Mersenne prime.*

The biggest known prime at the moment (March 2002) is the Mersenne prime $2^{13466917} - 1$. It is no coincidence that the biggest known prime at the moment is a Mersenne prime, because there is a very easy test, the Lucas-Lehmer test (see [Beukers] page 44), to check whether a number of the form $2^p - 1$ is prime or not.

David A. Cox has written a book about primes of the form $x^2 + d \cdot y^2$ (see [Cox]). In this paper we consider this for Mersenne primes, so the fundamental equation of this paper is

$$M_l = x^2 + d \cdot y^2, \tag{0.1}$$

with $x, y, d \in \mathbb{Z}_{\geq 0}$ and M_l a Mersenne prime.

Definition 0.2 *We define F_d to be the quadratic form $X^2 + d \cdot Y^2 \in \mathbb{Z}[X, Y]$. Let p be a prime. We shall say that p is represented by F_d if there is a tuple $(x, y) \in \mathbb{Z}^2_{\geq 0}$ such that $p = x^2 + d \cdot y^2$.*

Proposition 0.3 *Let M_l be a Mersenne prime. Let $d \in \mathbb{Z}_{\geq 0}$. Suppose that F_d represents M_l. Then there is a unique tuple $(x, y) \in \mathbb{Z}^2_{\geq 0}$ with the property $M_l = x^2 + d \cdot y^2$.*

Proof:
If $d = 0$ then clearly F_d does not represent M_l. If $d = 1$ then $x^2 + d \cdot y^2 \equiv 1 \bmod 4$, but since we have $M_l \equiv 3 \bmod 4$, we see that F_d does not represent M_l. Let $d > 1$. We know that $M_l \neq 2$. If $M_l \mid d$ then F_d does not represent M_l or $M_l = d$. In the last case it is clear that $(x, y) = (0, 1)$ is the unique tuple

in $\mathbb{Z}^2_{\geq 0}$ with $M_l = x^2 + d \cdot y^2$. Now we may assume that $M_l \nmid 2d$. But then M_l does not divide the conductor f of $\mathbb{Z}[\sqrt{-d}]$, because f obeys the relation $-4d = f^2 \Delta(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$. Suppose that (x, y) and (x', y') are tuples in $\mathbb{Z}^2_{\geq 0}$ with the property that $M_l = x^2 + d \cdot y^2 = (x')^2 + d \cdot (y')^2$. Since M_l does not divide f we know that M_l splits uniquely in two principal prime ideals in $\mathbb{Z}[\sqrt{-d}]$ (see [Cox] page 144), so we have that the element $x' + y'\sqrt{-d}$ is equal to, let's say, the element $(x + y\sqrt{-d}) \cdot u$ for a certain $u \in \mathbb{Z}[\sqrt{-d}]^* = \{\pm 1\}$. We get $x = x'u$, hence $x = x'$. Therefore we have $(x, y) = (x', y')$. This completes the proof.

Definition 0.4 *We call the unique tuple (x, y) in proposition (0.3) the F_d-solution of M_l.*

We will be concerned with two questions. The first most natural question to arise is: Can we decide for a given $d \in \mathbb{Z}_{>0}$ and a given Mersenne prime M_l whether or not F_d represents M_l? Suppose F_d represents M_l. Let (x, y) be the F_d-solution of M_l. Our second question is: What can we say about the divisibility of x or y by small primes (2 or 3)?

An illustration of both questions, which was implicitly the start of this paper, is the following table made by Franz Lemmermeyer.

$2^7 - 1 = 127 = 8^2 + 7 \cdot 3^2$
$2^{13} - 1 = 8191 = 48^2 + 7 \cdot 29^2$
$2^{19} - 1 = 524287 = 720^2 + 7 \cdot 29^2$
$2^{31} - 1 = 2147483647 = 43968^2 + 7 \cdot 5533^2$
$2^{61} - 1 = 2305843009213693951 = 910810592^2 + 7 \cdot 459233379^2$

In this table we see the first few nontrivial solutions of the equation $M_l = x^2 + 7 \cdot y^2$. Franz Lemmermeyer observed that x is divisible by 8 every time. That this is true in general was proved by Hendrik Lenstra and Peter Stevenhagen (see [LenSte]). The idea they used in the proof of their theorem can be generalized. One generalization leads to the following result.

Theorem 0.5 *Let $d = 2^n - 1$ be a squarefree integer with $2 \nmid n$. Let M_l be a Mersenne prime with $l \equiv 1 \bmod n$. Suppose that (x, y) is the F_d-solution of M_l then $8 \mid x$.*

Definition 0.6 *Let $0 < n < 38$ be an integer. We define A_n be the set of the first n Mersenne primes. We define $s_n(d)$ to be $\{M_l \in A_n | F_d \text{ represents } M_l\}$.*

This paper is divided in four chapters. In the first chapter we will look at the F_d-solution of M_l for $M_l \in s_{10}(d)$ and d between 0 and 48, and we will look at the numbers $\#s_{20}(d)$ for d between 0 and 48. We will observe some structure in our examples. Some of these structures are easy to prove, see proposition (1.1), and some are harder to prove, see for example proposition (3.6). In chapter two we will state a couple of theorems we use in chapter three and four. Keywords in chapter two are the Artin map, Hilbert class field, ray class field and ring class field. These class fields will help us to decide whether or not F_d represents M_l.

The knowledge of chapter two will be used to explain the numbers $\#s_{20}(d)$ we found in chapter one. Take for example $d = 14$. We get for this d the following nice result. Suppose that M_l is a Mersenne prime then

$$F_{14} \textit{ represents } M_l \Leftrightarrow l \equiv 1 \bmod 3.$$

The technique we used to prove the above statement will also be used in the proof of theorem (0.5) in chapter four.

I would like to thank my supervisor Bart de Smit and Peter Stevenhagen for their advice and suggestions.

Chapter 1

Numerical results

In this chapter we will look at the F_d-solution of M_l for $M_l \in s_{10}(d)$ and d between 0 and 48, and we will look at the numbers $\#s_{20}(d)$ for d between 0 and 48.

In Pari/GP, the well known computer algebra package (see [Cohen2] page 525), one can implement the algorithm of Cornacchia (see [Beukers] page 157 or [Cohen] page 34) to calculate the F_d-solution of M_l. The first ten Mersenne primes are $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{61}$ and M_{89}. The F_d-solution of M_l for $M_l \in s_{10}(d)$ and d between 0 and 48 are given below.

$d = 2$
$M_2 = (1)^2 + 2 \cdot (1)^2$

$d = 3$
$M_2 = (0)^2 + 3 \cdot (1)^2$
$M_3 = (2)^2 + 3 \cdot (1)^2$
$M_5 = (2)^2 + 3 \cdot (3)^2$
$M_7 = (2 \cdot 5)^2 + 3 \cdot (3)^2$
$M_{13} = (2 \cdot 23)^2 + 3 \cdot (3^2 \cdot 5)^2$
$M_{17} = (2 \cdot 181)^2 + 3 \cdot (3)^2$
$M_{19} = (2 \cdot 149)^2 + 3 \cdot (3 \cdot 127)^2$
$M_{31} = (2 \cdot 23081)^2 + 3 \cdot (3^4 \cdot 29)^2$
$M_{61} = (2 \cdot 9697 \cdot 77617)^2 + 3 \cdot (3^2 \cdot 11 \cdot 13 \cdot 89611)^2$
$M_{89} = (2 \cdot 601 \cdot 14456661997)^2 + 3 \cdot (3 \cdot 5^3 \cdot 1979 \cdot 13851631)^2$

$d = 6$
$M_3 = (1)^2 + 6 \cdot (1)^2$
$M_5 = (5)^2 + 6 \cdot (1)^2$
$M_7 = (11)^2 + 6 \cdot (1)^2$
$M_{13} = (29)^2 + 6 \cdot (5 \cdot 7)^2$
$M_{17} = (5 \cdot 71)^2 + 6 \cdot (29)^2$
$M_{19} = (349)^2 + 6 \cdot (7 \cdot 37)^2$

$M_{31} = (44029)^2 + 6 \cdot (3 \cdot 7 \cdot 281)^2$
$M_{61} = (47 \cdot 1321 \cdot 22027)^2 + 6 \cdot (5 \cdot 7 \cdot 7697863)^2$
$M_{89} = (7 \cdot 43 \cdot 77508521119)^2 + 6 \cdot (5 \cdot 173 \cdot 11087 \cdot 367867)^2$

$d = 7$
$M_3 = (0)^2 + 7 \cdot (1)^2$
$M_7 = (2^3)^2 + 7 \cdot (3)^2$
$M_{13} = (2^4 \cdot 3)^2 + 7 \cdot (29)^2$
$M_{19} = (2^4 \cdot 3^2 \cdot 5)^2 + 7 \cdot (29)^2$
$M_{31} = (2^6 \cdot 3 \cdot 229)^2 + 7 \cdot (11 \cdot 503)^2$
$M_{61} = (2^5 \cdot 79 \cdot 360289)^2 + 7 \cdot (3^2 \cdot 11 \cdot 4638721)^2$

$d = 14$
$M_7 = (1)^2 + 14 \cdot (3)^2$
$M_{13} = (71)^2 + 14 \cdot (3 \cdot 5)^2$
$M_{19} = (13 \cdot 43)^2 + 14 \cdot (3 \cdot 41)^2$
$M_{31} = (13 \cdot 3557)^2 + 14 \cdot (3 \cdot 271)^2$
$M_{61} = (5 \cdot 79 \cdot 223 \cdot 10859)^2 + 14 \cdot (3 \cdot 13 \cdot 47 \cdot 61 \cdot 2819)^2$

$d = 15$
$M_5 = (2^2)^2 + 15 \cdot (1)^2$
$M_{13} = (2^4)^2 + 15 \cdot (23)^2$
$M_{17} = (2^2 \cdot 89)^2 + 15 \cdot (17)^2$
$M_{61} = (2^5 \cdot 19 \cdot 43 \cdot 47609)^2 + 15 \cdot (3 \cdot 2477 \cdot 30223)^2$
$M_{89} = (2^3 \cdot 47 \cdot 739 \cdot 4147399)^2 + 15 \cdot (3^2 \cdot 4339 \cdot 8753 \cdot 18773)^2$

$d = 19$
$M_{19} = (2 \cdot 257)^2 + 19 \cdot (3^2 \cdot 13)^2$

$d = 22$
$M_5 = (3)^2 + 22 \cdot (1)^2$
$M_{19} = (3^2 \cdot 5 \cdot 7)^2 + 22 \cdot (139)^2$
$M_{31} = (7 \cdot 6619)^2 + 22 \cdot (3 \cdot 61)^2$
$M_{61} = (1518243299)^2 + 22 \cdot (3 \cdot 5 \cdot 7 \cdot 13 \cdot 4363)^2$
$M_{89} = (53 \cdot 13405371289)^2 + 22 \cdot (3 \cdot 103 \cdot 17158836061)^2$

$d = 23$
$M_{89} = (2^4 \cdot 59 \cdot 79 \cdot 6113 \cdot 28813)^2 + 23 \cdot (3 \cdot 5 \cdot 11 \cdot 16649 \cdot 1603769)^2$

$d = 27$
$M_5 = (2)^2 + 27 \cdot (1)^2$
$M_7 = (2 \cdot 5)^2 + 27 \cdot (1)^2$
$M_{13} = (2 \cdot 23)^2 + 27 \cdot (3 \cdot 5)^2$
$M_{17} = (2 \cdot 181)^2 + 27 \cdot (1)^2$
$M_{19} = (2 \cdot 149)^2 + 27 \cdot (127)^2$
$M_{31} = (2 \cdot 23081)^2 + 27 \cdot (3^3 \cdot 29)^2$

$M_{61} = (2 \cdot 9697 \cdot 77617)^2 + 27 \cdot (3 \cdot 11 \cdot 13 \cdot 89611)^2$
$M_{89} = (2 \cdot 601 \cdot 14456661997)^2 + 27 \cdot (5^3 \cdot 1979 \cdot 13851631)^2$

$d = 30$
$M_5 = (1)^2 + 30 \cdot (1)^2$
$M_{13} = (89)^2 + 30 \cdot (3)^2$
$M_{17} = (19^2)^2 + 30 \cdot (5)^2$
$M_{61} = (13 \cdot 53522947)^2 + 30 \cdot (11 \cdot 349 \cdot 64189)^2$
$M_{89} = (24014203778671)^2 + 30 \cdot (3^5 \cdot 11 \cdot 23 \cdot 19311737)^2$

$d = 31$
$M_5 = (0)^2 + 31 \cdot (1)^2$
$M_{31} = (2^3 \cdot 647)^2 + 31 \cdot (3^2 \cdot 919)^2$
$M_{61} = (2^4 \cdot 5 \cdot 43 \cdot 435983)^2 + 31 \cdot (3 \cdot 7 \cdot 2032909)^2$

$d = 38$
$M_{19} = (683)^2 + 38 \cdot (3 \cdot 13)^2$

$d = 39$
$M_{13} = (2^3 \cdot 5)^2 + 39 \cdot (13)^2$
$M_{19} = (2^2 \cdot 7 \cdot 23)^2 + 39 \cdot (53)^2$
$M_{31} = (2^3 \cdot 5503)^2 + 39 \cdot (7 \cdot 331)^2$
$M_{61} = (2^3 \cdot 5 \cdot 21609899)^2 + 39 \cdot (7 \cdot 11 \cdot 131 \cdot 19819)^2$

$d = 43$
$M_{13} = (2 \cdot 3 \cdot 13)^2 + 43 \cdot (7)^2$

$d = 46$
$M_7 = (3^2)^2 + 46 \cdot (1)^2$
$M_{19} = (271)^2 + 46 \cdot (3^2 \cdot 11)^2$
$M_{89} = (5 \cdot 23143 \cdot 168841333)^2 + 46 \cdot (3 \cdot 18229 \cdot 41528533)^2$

Some d's give a lot of solutions, for example $d = 3, 6, 27$, other d's a few and there are also a lot of d's without a solution. Now take a look at the divisibility of x or y by 2 or 3. For example take $d = 3$ then most y's are divisible by 3. For $d = 15$ we see that $4 \mid x$. The proposition below explains some of these observations. We will explain the other observations in chapter three.

Proposition 1.1 *Let $M_l \neq 3$ be a Mersenne prime. If $d \equiv 0, 1, 2, 4, 5 \bmod 8$ then F_d does not represent M_l. Suppose that F_d represents M_l. Let (x, y) be the F_d-solution of M_l. For the remaining cases of $d \bmod 8$ we have the following properties:*

$d \bmod 8$	*properties of* (x, y)
3	$2 \parallel x$
6	$2 \nmid x \cdot y$
7	$4 \mid x$

For the cases $d \equiv 1, 2 \bmod 3$ we have the following properties:

$d \bmod 3$	*properties of* (x, y)
1	*either* $3 \mid x$ *or* $3 \mid y$
2	$3 \mid y$

Proof:
Since we assumed that $M_l \neq 3$ we have $M_l \equiv -1 \bmod 8$. Because a square modulo 8 equals $0, 1, 4 \bmod 8$, we see from the equivalence $M_l \equiv -1 \equiv x^2 + d \cdot y^2 \bmod 8$, after we have checked all the possible combinations, that we have no solutions for $d \equiv 0, 1, 2, 4, 5 \bmod 8$. For $d \equiv 3 \bmod 8$ we see that $2 \parallel x$. If $d \equiv 6 \bmod 8$ then $2 \nmid x \cdot y$. And for $d \equiv 7 \bmod 8$ we see that $4 \mid x$. Suppose that $d \equiv 1 \bmod 3$, then $M_l \equiv 1 \equiv x^2 + d \cdot y^2 \equiv x^2 + y^2 \bmod 3$, so either $3 \mid x$ or $3 \mid y$. Suppose $d \equiv 2 \bmod 3$ then $M_l \equiv 1 \equiv x^2 + d \cdot y^2 \equiv x^2 - y^2 \bmod 3$, so $3 \mid y$. This completes the proof.

With proposition (1.1) we can exclude $d \equiv 0, 1, 2, 4, 5 \bmod 8$, if $d \neq 2$. For the case $d = 2$ we know by proposition (1.1) that F_2 represents M_l if and only if $M_l = 3 = 1^2 + 2 \cdot 1^2$. In the table below we see the numbers $\#s_{20}(d)$ for each d between 0 and 48.

d	2	3	6	7	11	14	15	19	22	23
$\#s_{20}(d)$	1	20	19	13	1	12	9	2	8	2

d	27	30	31	35	38	39	43	46	47
$\#s_{20}(d)$	18	9	5	0	2	7	3	6	1

For $d = 3, 7, 15$ we see that $|\#s_{20}(d) - \#s_{20}(2d)| \leq 1$. In chapter three we will prove for these d's that if M_l is a Mersenne prime not equal to d then F_d represents M_l if and only if F_{2d} represents M_l. In chapter three we will find criteria to decide whether or not F_d represents M_l, for d between 0 and 48. With these criteria we can explain the numbers $\#s_{20}(d)$ in the table above.

Let's take a look again at the F_d-solution of M_l for $M_l \in s_{10}(d)$ and d between 0 and 48, with the divisibility of x by 8 for $d = 7$ in mind. For $d = 15$ we already mentioned that $4 \mid x$. Now $7 = 2^3 - 1$ and $15 = 2^4 - 1$. The next odd power of two minus one is $2^5 - 1 = 31$ and if we check the divisibility of x by 2 for $d = 31$, we see that for our two nontrivial solutions we both have $8 \mid x$. The next M_l such that F_{31} represents M_l is M_{521} and also $8 \mid x$. After M_{521} the next two M_l's with F_{31} represents M_l are M_{4253} and M_{11213}. But for both F_{31}-solutions (x, y) of M_{4253} and (x, y) of M_{11213} we have $8 \nmid x$. Next we have $2^7 - 1 = 127$. The first nontrivial Mersenne prime M_l such that F_{127} represents M_l is M_{127}.

$M_{127} = 12831216340765303000^2 + 127 \cdot 208123802438146401^2$

The next one is M_{9689}. For both F_{127}-solutions (x, y) of M_{127} and (x, y) of M_{9689} we have $8 \mid x$. I did not found Mersenne primes which are represented by F_{2^9-1} or $F_{2^{11}-1}$. The first nontrivial Mersenne prime M_l such that $F_{2^{13}-1}$ represents M_l is M_{521}. For the $F_{2^{13}-1}$-solution (x, y) of M_{521} we have $8 \mid x$.

Theorem (4.2) will explain the divisibility of x by 8 for all these examples.

Chapter 2

Some class field theory

In this chapter we will state the theorems we use in chapter three and four. We will define Hilbert class field, the Artin map, ray class field and ring class field. When we have done this, we can build up the conditions, as in [Cox], for deciding whether a prime is of the form $x^2 + d \cdot y^2$ or not.

We will refer a lot to the book of Cox (see [Cox]), therefore we will use his less usual definition of a number field. We define a number field K to be a subfield of the complex numbers $\mathbb{C}$ which has finite degree over the rational numbers $\mathbb{Q}$. Let K and L be number fields. The ring of algebraic integers of K will be denoted by $\mathbb{Z}_K$. The disciminant of L/K will be denoted by $\Delta(L/K)$. The discrimant of a polynomial f will be denoted by $\Delta(f)$. Let α be an element of L. The minimal polynomial of α over K will be denoted by f_K^α. We denote the norm map from the fractional ideals of L to the fractional ideals of K by $\mathbf{N}_{L/K}$.

Ramification and discriminant

If you want to use class field theory, like we do, it is important to know which primes ramify. Therefore we will state some useful theorems about ramification.

Theorem 2.1 *Let L/K be an extension of number fields. Then a prime π of K ramifies in the extension $\mathbb{Z}_K \subset \mathbb{Z}_L$ if and only if it divides $\Delta(L/K)$.*

Proof: See [FT] page 126.

Theorem 2.2 *Let L/K be an extension of number fields. Suppose $L = K(\alpha)$ for an element $\alpha \in \mathbb{Z}_L$ then $\Delta(L/K) \mid \Delta(f_K^\alpha) \cdot \mathbb{Z}_K$.*

Proof: See [FT] page 121.

Theorem 2.3 *Given a tower of number fields $K \subset L \subset M$, we have the identity*

$$\Delta(M/K) = \boldsymbol{N}_{L/K}(\Delta(M/L)) \cdot \Delta(L/K)^{[M:L]}.$$

Proof: See [FT] page 126.

Theorem 2.4 *Let L and M be linearly disjoint extensions of a number field K, and suppose that $\Delta(L/K)$ and $\Delta(M/K)$ are coprime in $\mathbb{Z}_K$. Then we have $\mathbb{Z}_{LM} = \mathbb{Z}_L \cdot \mathbb{Z}_M$ and $\Delta(LM/K) = \Delta(L/K)^{[M:K]} \cdot \Delta(M/K)^{[L:K]}$.*

Proof: See [Lang] page 68.

Infinite primes

Finite primes of a number field K are just the maximal ideals of $\mathbb{Z}_K$, the ring of algebraic integers of K. The infinite primes are determined by the embedding of a number field into the complex numbers $\mathbb{C}$. We have two kind of infinite primes. A real infinite prime is an embedding $\sigma : K \to \mathbb{R}$ and a complex infinite prime is an unordered pair of complex conjugated embeddings $\sigma, \bar{\sigma} : K \to \mathbb{C}$ with $\sigma \neq \bar{\sigma}$. So $\mathbb{Q}$ has one prime at infinity and $K = \mathbb{Q}(\sqrt[3]{2})$ has two primes at infinity.

Let $K \subset L$ be number fields and φ, τ infinite primes in K, L respectively. We say τ lies above φ if and only if $\tau|_K = \varphi$. If this is the case, we will write $\tau|\varphi$. Each infinite prime φ of K gives rise to an absolute value on K. Indeed, let $\alpha \in K$ and let $|\cdot|$ the Euclidean distance function on $\mathbb{C}$. If φ is a real infinite prime, say φ is the imbedding $\sigma : K \to \mathbb{C}$, then we define $|\alpha|_\varphi$ to be $|\sigma(\alpha)|$. If φ is a complex infinite prime, say φ is the pair of complex conjugated embeddings $\sigma, \bar{\sigma} : K \to \mathbb{C}$, then we define $|\alpha|_\varphi$ to be $|\sigma(\alpha)|$. This is well defined since $|\sigma(\alpha)| = |\bar{\sigma}(\alpha)|$. Let φ be an infinite prime then we have the following absolute value on K

$$\alpha \mapsto |\alpha|_\varphi.$$

By K_φ we will mean the completion of K induced by the absolute value $|\cdot|_\varphi$. The field K_φ will be $\mathbb{R}$, whenever φ is a real infinite prime, or $\mathbb{C}$, whenever φ is a complex infinite prime. Now suppose that $\tau|\varphi$ and $K_\varphi \neq L_\tau$ then we say that φ ramifies in L.

Theorem 2.5 *Let $K \subset L$ be number fields. Let φ be an infinite prime of K and let τ be an infinite prime of L above φ. Then*

$$\sum_{\tau|\varphi} [L_\tau : K_\varphi] = [L : K].$$

Proof: See [Lang] page 39.

We give an example of theorem (2.5). Let ∞ be the infinite prime of $\mathbb{Q}$. Let τ be an infinite prime of $K = \mathbb{Q}(\sqrt[3]{2})$. Clearly τ lies above ∞. So we have using theorem (2.5)

$$\sum_{\tau|\infty} [K_\tau : \mathbb{Q}_\infty] = [\mathbb{R} : \mathbb{R}] + [\mathbb{C} : \mathbb{R}] = 1 + 2 = [K : \mathbb{Q}].$$

Now we can talk about unramified extensions.

2.1 Hilbert class field

We say that a number field L is unramified over a number field $K \subset L$ if every prime, finite or infinite, of K is unramified in L. We define $\overline{K}$ to be the algebraic closure of the number field K in $\mathbb{C}$.

Theorem 2.6 *For every number field K there exist a finite abelian unramified extension $H(K)$ in $\overline{K}$, such that if L is an unramified abelian extension of K in $\overline{K}$, then we have $L \subset H(K)$. Furthermore, we have $\mathrm{Cl}(K) \simeq \mathrm{Gal}(H(K)/K)$, where $\mathrm{Cl}(K)$ is the class group of K and $\mathrm{Gal}(H(K)/K)$ is the Galois group of $H(K)$ over K.*

Proof: See [Cox] page 106 and 109.

The field $H(K)$ is called the Hilbert class field of K. It is the maximal unramified abelian extension of K in $\overline{K}$. A theorem of Minkowski, see [Cohen] page 195, says that for every number field K different from $\mathbb{Q}$ we have $|\Delta(K/\mathbb{Q})|$, the absolute value of the discriminant of K over $\mathbb{Q}$, is bigger then 1. From theorem (2.6) we get that $\mathrm{Cl}(\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) \simeq \{id\}$, so the class number of $\mathbb{Q}$ is 1, and we rediscover the well known fact that $\mathbb{Z}$ is a unique factorization domain.

2.2 The Artin map

Theorem (2.6) says that there is an isomorphism between the class group $\mathrm{Cl}(K)$ and the Galois group $\mathrm{Gal}(H(K)/K)$. In this section we will give a canonical map. We will follow mainly [Lang].

Let L/K be a Galois extension of number fields with $G = \mathrm{Gal}(L/K)$. Let π be a finite prime of K and let ρ_1 and ρ_2 be primes of L above π. We know that there exist $\sigma \in G$ such that $\rho_1 = \sigma(\rho_2)$ (see [Lang] page 12). And if $\sigma \in G$ then $\sigma(\rho_1)$ lies above π. Let ρ be a prime above π in L. Let $G_\rho = \{\sigma \in G | \sigma(\rho) = \rho\}$ be the decomposition group of the prime ρ of L. We have $G_{\rho_1} = \sigma G_{\rho_2} \sigma^{-1}$ if $\rho_1 = \sigma(\rho_2)$. So if the Galois group G is abelian, then we have $G_{\rho_1} = G_{\rho_2}$. Since every element σ of G_ρ leaves ρ fixed and is the identity on $\mathbb{Z}_K/\pi$, the element σ induces an element $\bar{\sigma}$ of the Galois group of $\mathbb{Z}_L/\rho$ over $\mathbb{Z}_K/\pi$. This gives us a surjective group homomorphism (see [Lang] page 16)

$$G_\rho \to \mathrm{Gal}((\mathbb{Z}_L/\rho)/(\mathbb{Z}_K/\pi)),$$

given by

$$\sigma \longmapsto \bar{\sigma}.$$

The kernel of the homomorphism is called the inertia group and it is denoted by I_ρ. The fixed field of the decomposition group of a prime ρ is called the decomposition field of ρ. The fixed field of the inertia group of ρ is called the inertia field of ρ. These two fields have very nice properties. The decomposition field D of ρ is the smallest subfield of L containing K such that ρ is the only prime of L lying above the prime $\rho \cap D$ of D. The ramification index $e(\rho \cap D/\pi)$ and the residue index $f(\rho \cap D/\pi)$ are both equal to 1. The inertia field I of ρ is the smallest subfield of L containing K such that the prime $\rho \cap I$ is totally ramified in L. The ramification index $e(\rho/\pi)$ equals $[L : I]$ and the residue class degree $f(\rho/\pi)$ equals $[I : D]$.

For the rest of this section we assume that π is a finite prime of K unramified in L. By the theory of finite fields there exists a unique element $\bar{\sigma}$ of $\mathrm{Gal}((\mathbb{Z}_L/\rho)/(\mathbb{Z}_K/\pi))$, called the Frobenius automorphism, that has the effect

$$\bar{\sigma}(x) \equiv x^{\mathbf{N}(\pi)} \bmod \rho \quad \forall x \in \mathbb{Z}_L.$$

So every unramified prime ρ above π of L gives us a unique element $\bar{\sigma}$ of $\mathrm{Gal}((\mathbb{Z}_L/\rho)/(\mathbb{Z}_K/\pi))$. And since π is unramified in L, we have $I_\rho = \{e\}$, so the map from G_ρ to $\mathrm{Gal}((\mathbb{Z}_L/\rho)/(\mathbb{Z}_K/\pi))$ is an isomorphism. Hence we get a unique element σ of $G_\rho \subset \mathrm{Gal}(L/K)$. We denote this unique element σ by $(\frac{\rho}{L/K})$.

For the rest of this section we assume that $K \subset L$ is an abelian extension of number fields. Since L/K is abelian and $(\frac{g(\rho)}{L/K}) = g(\frac{\rho}{L/K})g^{-1}$ for all $g \in G$ (see [Cox] page 107), we see that $(\frac{\rho}{L/K})$ only depends on π. Hence every unramified prime π of K induces an element of the Galois group of L/K. We denote this element by $(\frac{\pi}{L/K})$. Now we have a map from the prime ideals of K, which do not ramify in L, to $\mathrm{Gal}(L/K)$, given by

$$\pi \longmapsto (\frac{\pi}{L/K}).$$

We define the decomposition group of π, denoted by G_π, to be the decomposition group of a prime ρ in L above π. This is well defined since L/K is abelian. We define the Frobenius of π to be the unique element of G_π that induces the Frobenius automorphism of $\mathrm{Gal}((\mathbb{Z}_L/\rho)/(\mathbb{Z}_K/\pi))$.
Now in words the map above says: Every prime ideal π of K is send to the Frobenius of π.

We can extend our map by multiplicativity. Let $I_K(\Delta(L/K))$ be the group of fractional ideals of $\mathbb{Z}_K$ prime to $\Delta(L/K)$, so every prime ideal in $I_K(\Delta(L/K))$ is unramified in L. If $i \in I_K(\Delta(L/K))$ and $i = \prod \pi^{e_\pi}$, then we define

$$(\frac{i}{L/K}) = \prod (\frac{\pi}{L/K})^{e_\pi}.$$

Now we have a map,

$$I_K(\Delta(L/K)) \to \mathrm{Gal}(L/K), \tag{2.1}$$

the *Artin map*, which is actually a surjective homomorphism (see [Lang] page 199).

We are interested in the kernel of the Artin map. First we define a couple of important terms.

Definition 2.7 *Let K be a number field. A modules m of K is a formal product $m_0 \cdot m_\infty$ of finitely many finite primes m_0 and finitely many infinite real primes m_∞, with the real primes all different from each other.*

By $I_K(m)$ we will mean the group of all fractional ideals of K relative prime to m_0.

Definition 2.8 *Let K be a number field and m a modulus of K. We define $P_{K,1}(m)$ to be the subgroup of $I_K(m)$ generated by the principal ideals $\alpha \cdot \mathbb{Z}_K$, with $\alpha \in \mathbb{Z}_K$, satisfying $\alpha \equiv 1 \bmod m_0$ and $\sigma(\alpha) > 0$ for all infinite primes σ of K dividing m_∞. We define $\mathrm{Cl}_m(K)$ to be the group $I_K(m)/P_{K,1}(m)$.*

Let m be a modulus, such that every finite prime which ramifies in L, divides m. Then we have the Artin map

$$I_K(m) \twoheadrightarrow \mathrm{Gal}(L/K). \tag{2.2}$$

It is not in general true that the kernel of this map contains $P_{K,1}(m)$. But if we make a good choice for the modulus, this will be true. There is a "smallest" choice.

Theorem 2.9 *Let L/K be an abelian extension of number fields. Then there is a modulus $f = f(L/K)$ such that:*

(i) A prime of K, finite or infinite, ramifies in L if and only if it divides f.
(ii) Let m be a modulus divisible by all primes which ramify in L. Then the kernel of the Artin map $I_K(m) \to \mathrm{Gal}(L/K)$ contains $P_{K,1}(m)$ if and only if $f \mid m$.

Proof: See [Cox] page 162.

The $f(L/K)$ in theorem (2.9) is called the conductor of L/K. The following theorem gives us a good modulus.

Theorem 2.10 *Let $K \subset L$ be an abelian extension of number fields. Let $\Delta(L/K)$ be the relative discriminant of L over K. Let m_∞ be the formal product of all real infinite primes of K which ramify in L. Set $m = \Delta(L/K) \cdot m_\infty$. Then the Artin map induces a surjective group homomorphism*

$$Cl_m(K) \twoheadrightarrow Gal(L/K). \tag{2.3}$$

Proof: The conductor $f(L/K)$ divides $\Delta(L/K) \cdot m_\infty$ (see [Cohen2] page 158). So by theorem (2.9) the theorem follows.

2.3 Ray class field and ring class field

In the previous section we started with an extension of number fields L/K. Now we will go the other way around and start with a number field K and a modulus m of K.

Fix m, then we can search for abelian extensions L of K in $\overline{K}$, the algebraic closure of K in $\mathbb{C}$, with the following two properties:
1: Every prime of K, finite or infinite, which ramifies in L divides m.
2: $P_{K,1}(m)$ is contained in the kernel of the Artin map.

Let $\Omega_m(K)$ be the set of all abelian field extensions L of K which satisfy these two properties. Let $\Upsilon_m(K)$ be the set of all subgroups of $I_K(m)$ which contain $P_{K,1}(m)$. There is a canonical bijection $\beth$ between $\Omega_m(K)$ and $\Upsilon_m(K)$ induced by the Artin map. Indeed, given a field $L \in \Omega_m(K)$ then the kernel of the Artin map $I_K(m) \to Gal(L/K)$ is a group $H \in \Upsilon_m(K)$. And given a group $H \in \Upsilon_m(K)$ then the is a unique field $L \in \Omega_m(K)$ such that the kernel of the Artin map $I_K(m) \to Gal(L/K)$ is H (see [Cox] page 162). The bijection $\beth$ has the following nice property. Let $L_1, L_2 \in \Omega_m(K)$ then $L_1 \subset L_2$ if and only if $\beth(L_1) \supset \beth(L_2)$. Hence we have the following theorem.

Theorem 2.11 *There is a field $R_m(K) \in \Omega_m(K)$ such that for every $L \in \Omega_m(K)$, we have $L \subset R_m(K)$. Furthermore, the Artin map induces a group isomorphism*

$$\mathrm{Cl}_m(K) \to \mathrm{Gal}(R_m(K)/K).$$

Proof: Take $R_m(K) = \beth(P_{K,1}(m))$.

The field $R_m(K)$ is called the ray class field of K with modulus m. It is the maximal abelian extension of K in $\overline{K}$ with the property, that only primes of K, which divide the modulus m, ramify in $R_m(K)$ and every prime ideal of K in $P_{K,1}(m)$ is completely split in $R_m(K)$. The group $\mathrm{Cl}_m(K)$ is called the ray class group of K with modulus m. A basic result is that the number of elements of $\mathrm{Cl}_m(K)$ is finite (see [Cox] page 160), hence $R_m(K)$ is a finite extension of K. If we take $m = 1$, then $R_m(K) = H(K)$ and $\mathrm{Cl}_m(K) = \mathrm{Cl}(K)$, so we see that the ray class field is a generalization of the Hilbert class field.

The most important field of chapter three will be the ring class field. Let K be a quadratic number field and let O be an order of K. Set $m = [\mathbb{Z}_K : O]$. We define $P_{K,\mathbb{Z}}(m)$ to be the subgroup of $I_K(m)$ generated by the principal ideals $\alpha \cdot \mathbb{Z}_K$, with $\alpha \in \mathbb{Z}_K$, satisfying $\alpha \equiv a \bmod m$ for a number a with $gcd(a, m) = 1$. The field $\beth(P_{K,\mathbb{Z}}(m))$ is called the ring class field of the order O and we will denoted it by $Ri(O)$. Clearly the Artin map induces an isomorphism between $I_K(m)/P_{K,\mathbb{Z}}(m)$ and $\mathrm{Gal}(Ri(O)/K)$.

We have $m = [\mathbb{Z}_K : O] = 1, 2, 3, 4, 6$ if and only if $P_{K,1}(m) = P_{K,\mathbb{Z}}(m)$. And we have $P_{K,1}(m) = P_{K,\mathbb{Z}}(m)$ if and only if $R_m(K) = Ri(O)$. In chapter three we only need to calculate the ring class fields of orders O with $[\mathbb{Z}_K : O] = 1, 2, 6$. Hence we only need to calculate the ray class fields $R_m(K)$.

2.4 Calculating the ray class fields

In this section we will concentrate on calculating ray class fields of imaginary quadratic fields K. Our fields will be imaginary quadratic, therefore we may assume that our modulus $m = m_0$. We will give one way that might lead to the ray class field $R_m(K)$.

Let K be a number field and m a modulus. We want to find $R_m(K)$, the ray class field of K with modulus m. From theorem (2.11) we know that $\mathrm{Cl}_m(K)$ is isomorphic to $G = \mathrm{Gal}(R_m(K)/K)$. So if we know the number of elements of $\mathrm{Cl}_m(K)$ then we know $[R_m(K) : K]$. We have the following exact sequence

$$0 \to \mathbb{Z}_K^* \to (\mathbb{Z}_K/m)^* \twoheadrightarrow \mathrm{Cl}_m(K) \twoheadrightarrow I_K(m)/P_K(m) \to 0.$$

Hence we have

$$\#\mathrm{Cl}_m(K) = \#(I_K(m)/P_K(m)) \cdot \# im((\mathbb{Z}_K/m)^*),$$

where $im((\mathbb{Z}_K/m)^*)$ is the image of the homomorphism $\mathbb{Z}_K^* \to (\mathbb{Z}_K/m)^*$.

Theorem 2.12 *Let K be a number fields and m a modulus of K then*

$$\#\mathrm{Cl}_K = \# I_K(m)/P_K(m).$$

Proof: See [Janusz] page 112 and 113.

Now $\#\mathrm{Cl}_K$ is the class number h_K of K which can be calculated with methods explained in [Stewart] chapter 10 or looked up in a table (for example [Koch] page 246). We also get from the exact sequence above

$$\# im((\mathbb{Z}_K/m)^*) = \#(\mathbb{Z}_K/m)^*/\# im(\mathbb{Z}_K^*),$$

where $im(\mathbb{Z}_K^*)$ is the image of the homomorphism $\mathbb{Z}_K^* \to (\mathbb{Z}_K/m)^*$. Using the Chinese remainder theorem and the fact that

$$\#(\mathbb{Z}_K/\pi^{e_\pi})^* = (\mathbf{N}(\pi) - 1) \cdot (\mathbf{N}(\pi))^{(e_\pi - 1)}$$

(see [Cohen2] page 189) we see that the number of elements of $(\mathbb{Z}_K/m)^*$ is $\prod_{\pi_i} (\mathbf{N}(\pi_i) - 1) \cdot (\mathbf{N}(\pi_i))^{(e_{\pi_i} - 1)}$, with $m = \pi_1^{e_{\pi_1}} \cdots \pi_n^{e_{\pi_n}}$ the prime decomposition of m. Combining what we have done so far we get:

$$\#\mathrm{Cl}_m(K) = \{h_K \cdot \prod_{\pi_i | m} (\mathbf{N}(\pi_i) - 1) \cdot (\mathbf{N}(\pi_i))^{(e_{\pi_i} - 1)}\} / \#(im(\mathbb{Z}_K^*)). \qquad (2.4)$$

Theorem 2.13 *Let K be a number field and $R = R_m(K)$ the ray class field of K with modulus m. Let L be an abelian extension of K with conductor $f = f(L/K)$. If $f \mid m$ then*

$$L \subset R$$

Proof: See [Cox] page 163.

For the fields L of theorem (2.13) we know that only primes of K dividing m may ramify in L. So if we find a field L which is abelian over K and the only primes which ramify are primes dividing m, then we only need to check that $f(L/K) \mid m$. This leads us to calculating the conductor. But first we remark that the Hilbert class field of K is contained in $R_m(K)$. Indeed $f(H(K)/K) = 1$. Genus theory gives us a part of the Hilbert class field of an imaginary quadratic field.

Theorem 2.14 *Let K be an imaginary quadratic field with discriminant d_K. Let $p_1, \ldots, p_r$ be the odd primes dividing d_K. Set $p_i^* = (-1)^{(p_i-1)/2} \cdot p_i$. Then*

$$K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*}) \subset H(K),$$

with $H(K)$ the Hilbert class field of K.

Proof: See [Cox] page 121.

The field $K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*})$ is called the genus field of K.
Let's go back to the conductor. Another very useful theorem is the following.

Theorem 2.15 *Let L/K be an abelian extension of number fields. Suppose that the prime π of K is tamely ramified in L then*

$$\pi \parallel f(L/K).$$

Furthermore, if π is a prime of K which is unramified in L then

$$\pi \nmid f(L/K).$$

Proof: See [Cohen2] page 149 and [Janusz] page 188 and 189.

Theorem (2.15) does not tell us what to do if π is wildly ramified. There will be one case in chapter three, namely the case $d = 27$, where we have to deal with a wildly ramified prime. Fortunately, we find in [Janusz] chapter *VI* a general method to calculate the conductor. We can use this method in particular in the case where π is wildly ramified. The theorem below is the main key and it uses local fields. We will define local fields first. Let π be a finite prime of the number field K. We denote by K_π the completion of K with respect to the absolute value $|\cdot|_\pi$ (see [Lang] page 36 for more detail). The field K_π is called a local field.

Theorem 2.16 *Let L/K be an abelian extension of number fields. Let π be a prime of K which ramifies in L then*

$$\pi^b \parallel f(L/K),$$

where b is the smallest integer such that $1 + \pi^b \mathbb{Z}_{K_\pi} \subseteq \boldsymbol{N}_\pi(L_\beta^*)$, with β a prime of L above π and $\mathbb{Z}_{K_\pi}$ the closure of $\mathbb{Z}_K$ in K_π.

Proof: See [Janusz] page 188 and 189.

With the theory above we can handle our examples.

Chapter 3

Criteria for solvability

In this chapter we will give a criterion to decide whether or not F_d represents p. When we have done this we will look at the special cases where p is a Mersenne prime and d lies between 0 and 48. With the criteria we get for these special cases, we can explain the numbers $\#s_{20}(d)$, we got in the table of chapter one.

3.1 Primes of the form $x^2 + d \cdot y^2$

In [Cox] we find a sufficient and necessary condition to know for a fixed $d \in \mathbb{Z}_{>0}$ when we can write a prime as $x^2 + d \cdot y^2$ for certain $x, y \in \mathbb{Z}_{\geq 0}$. We will discuss the idea of how this can be done and state the theorems we use. The most easy case is the following.

Theorem 3.1 *Let $d \equiv 1, 2 \bmod 4$ be a positive squarefree integer. Let p be an odd prime not dividing d. Suppose that the class number of $\mathbb{Q}(\sqrt{-d})$ equals 1, then*

$$F_d \textit{ represents } p \Leftrightarrow (\frac{-d}{p}) = 1.$$

Proof:
"$\Rightarrow$": Because $p \nmid d$ and $p = x^2 + d \cdot y^2$, we get $-d \cdot y^2 \equiv x^2 \bmod p$ so $(\frac{-d}{p}) = 1$.
"$\Leftarrow$": If $(\frac{-d}{p}) = 1$ and $p \neq 2$ then p splits in $\mathbb{Q}(\sqrt{-d})$, say $p\mathbb{Z}_K = \pi\bar{\pi}$. Because $h(\mathbb{Q}(\sqrt{-d})) = 1$, we know that π and $\bar{\pi}$ are principal. And because $d \equiv 1, 2 \bmod 4$ is a positive squarefree integer, we have $\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})} = \mathbb{Z}[\sqrt{-d}]$. So we have let's say $\pi = (x + y \cdot \sqrt{-d})$ and $\bar{\pi} = (x - y \cdot \sqrt{-d})$. Hence we have $p\mathbb{Z}_K = \pi\bar{\pi} = (x + y \cdot \sqrt{-d})(x - y \cdot \sqrt{-d}) = (x^2 + d \cdot y^2)$. From this we see that $p = x^2 + d \cdot y^2$. This completes the proof.

From the proof of theorem (3.1) it is clear that we need to make sure that the prime ideals above p in $K = \mathbb{Q}(\sqrt{-d})$ are generated by elements of the form $x \pm y \cdot \sqrt{-d}$ in order to be able to write p as $x^2 + d \cdot y^2$ for certain $x, y \in \mathbb{Z}_{\geq 0}$. In theorem (3.1) this was done by two assumptions. From the assumption $h_K = 1$ we get that every ideal is a principal ideal. Combining this with the assumption $d \equiv 1, 2 \bmod 4$ is positive and squarefree, we get that every ideal is generated by an element in $\mathbb{Z}[\sqrt{-d}]$.

Note that in theorem (3.1) we can change $(\frac{-d}{p}) = 1$ with p splits completely in $\mathbb{Q}(\sqrt{-d})$. First we will make a generalization of theorem (3.1) by dropping the assumption $h(K) = 1$. The Hilbert class field of K will be used for this.

Theorem 3.2 *Let $d \equiv 1, 2 \bmod 4$ be a positive squarefree integer. Let p be an odd prime not dividing d. Then we have*

$$F_d \textit{ represents } p \Leftrightarrow p \textit{ splits completely in } H(K),$$

where $H(K)$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-d})$.

Proof:
"$\Rightarrow$": The prime p does not ramify in K, because p does not divide the discriminant of K over $\mathbb{Q}$, which is $-d$ or $-4d$. And since $p = x^2 + d \cdot y^2$ we have $p\mathbb{Z}_K = \pi\bar{\pi}$ with let's say $(x + y\sqrt{-d}) = \pi \neq \bar{\pi} = (x - y\sqrt{-d})$. Using theorem (2.6) we get $(\frac{\pi}{H(K)/K}) = (\frac{\bar{\pi}}{H(K)/K}) = 1$, hence π splits completely in $H(K)$ and $\bar{\pi}$ splits completely in $H(K)$. We conclude that p splits completely in $H(K)$.
"$\Leftarrow$": Since p splits completely in $H(K)$ we have $p\mathbb{Z}_K = \pi\bar{\pi}$ with $\pi \neq \bar{\pi}$ and $(\frac{\pi}{H(K)/K}) = (\frac{\bar{\pi}}{H(K)/K}) = 1$. Using theorem (2.6) we get π and $\bar{\pi}$ are principal ideals. We have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-d}]$, since $d \equiv 1, 2 \bmod 4$ and $d > 0$ is squarefree. Therefore we have $x, y \in \mathbb{Z}$ with $p\mathbb{Z}_K = \pi \cdot \bar{\pi} = (x + y \cdot \sqrt{-d}) \cdot (x - y \cdot \sqrt{-d}) = (x^2 + d \cdot y^2)$. From this we see that $p = x^2 + d \cdot y^2$. This completes the proof.

In the theorem below we give a more elementary way of saying that p splits completely in $H(K)$.

Theorem 3.3 *Let $d \equiv 1, 2 \bmod 4$ be a positive squarefree integer. Then there is a monic irreducible polynomial $f = f_{\mathbb{Q}}^{\alpha}(x)$ of degree $[H(K) : K]$ in $\mathbb{Z}[x]$, with $K = \mathbb{Q}(\sqrt{-d})$ and $H(K)$ the Hilbert class field of K, such that if p is an odd prime neither dividing d nor $\Delta(f)$, then*

$$F_d \textit{ represents } p \Leftrightarrow (\frac{-d}{p}) = 1 \textit{ and } f \equiv 0 \bmod p \textit{ has an integer solution .}$$

Furthermore, f may be taken to be the minimal polynomial of a real algebraic integer α for which $H(K) = K(\alpha)$.

Proof:
We will work in the following fields $\mathbb{Q} \subset K \subset H(K)$ and $L = \mathbb{R} \cap H(K)$. Let τ be complex conjugation. Because $\tau(H(K))$ is unramified over $\tau(K) = K$ we see that $\tau(H(K)) \subset H(K)$, by theorem (2.6). Therefore $H(K)$ is Galois over $\mathbb{Q}$. The fixed field of the subgroup generated by τ is contained in $\mathbb{R}$, so this field is L and $[H(K) : L] = 2$. Let α be an algebraic integer such that $L = \mathbb{Q}(\alpha)$ and let $f = f_{L/\mathbb{Q}}^{\alpha}$ be the minimal polynomial of α over $\mathbb{Q}$. Because the compositum of

L and K is $H(K)$, the polynomial f can also be seen as the minimal polynomial of $H(K)$ over K.
"$\Rightarrow$": Suppose that $p = x^2 + d \cdot y^2$. Since p is an odd prime not dividing d, we have using (3.2) that p splits completely in $H(K)$ and $(\frac{-d}{p}) = 1$. Thus p splits completely in L. And with the Kummer-Dedekind theorem (see [Cohen] page 299) we see that $f \equiv 0 \bmod p$ has an integer solution.
"$\Leftarrow$": Suppose that $(\frac{-d}{p}) = 1$ then p splits in K, let's say $p\mathbb{Z}_K = \pi\bar{\pi}$. Because $(\mathbb{Z}_K/\pi) \cong \mathbb{F}_p$ we see $f \equiv 0 \bmod \pi$ has a solution. And because $H(K)/K$ is Galois and p does not divide $\Delta(f)$, we see that π splits completely in $H(K)$. With the same argument we get $\bar{\pi}$ splits completely in $H(K)$. We conclude that p splits completely in $H(K)$. Hence using theorem (3.2) we get F_d represents p. This completes the proof.

There are only finite p's excluded in theorem (3.3). For these p's one can use the algorithm of Cornacchia to check whether or not p is represented by F_d. For all other p's one has to find the polynomial f of theorem (3.3). In [Cox] we find a systematic method, which uses modular functions and complex multiplication, to calculate f.

Next we will drop the assumption $d \equiv 1, 2 \bmod 4$ and d squarefree. The problem will be that the principal ideals of $\mathbb{Q}(\sqrt{-d})$ do not have to be generated by an element of the form $x + y \cdot \sqrt{-d}$. We will use the ring class field of $\mathbb{Z}[\sqrt{-d}]$ for this problem.

Theorem 3.4 *Let d be a positive integer. Let p be an odd prime not dividing d. Then we have*

$$F_d \text{ represents } p \Leftrightarrow p \text{ splits completely in } Ri(\mathbb{Z}[\sqrt{-d}]),$$

where $Ri(\mathbb{Z}[\sqrt{-d}])$ is the ring class field of the order $\mathbb{Z}[\sqrt{-d}]$ of $\mathbb{Q}(\sqrt{-d})$.

Proof:
Let $K = \mathbb{Q}(\sqrt{-d})$ and let $O = \mathbb{Z}[\sqrt{-d}]$. We have $\mathbb{Z}_K = \mathbb{Z} + m\mathbb{Z}_K$, where $m = [\mathbb{Z}_K : O]$ (see [Cox] page 133). We also have $\Delta(O) = -4d = m^2\Delta(K/\mathbb{Q})$.
"$\Rightarrow$": Since $\Delta(K/\mathbb{Q}(\sqrt{-d})) \mid 4d$ we see that p, our odd prime not dividing d, does not ramify in K. And since $p = x^2 + d \cdot y^2$ we have $p\mathbb{Z}_K = \pi\bar{\pi}$ with let's say $(x + y\sqrt{-d}) = \pi \neq \bar{\pi} = (x - y\sqrt{-d})$. Because p does not divide m we see that $\pi, \bar{\pi} \in P_{K,\mathbb{Z}}(m)$. Hence we get $(\frac{\pi}{Ri(O)/K}) = (\frac{\bar{\pi}}{Ri(O)/K}) = 1$. So π splits completely in $Ri(O)$ and $\bar{\pi}$ splits completely in $Ri(O)$. We conclude that p splits completely in $Ri(O)$.
"$\Leftarrow$": Since p splits completely in $Ri(O)$ we have $p\mathbb{Z}_K = \pi\bar{\pi}$ with $\pi \neq \bar{\pi}$ and $(\frac{\pi}{Ri(O)/K}) = (\frac{\bar{\pi}}{Ri(O)/K}) = 1$. Hence π and $\bar{\pi}$ are elements of $P_{K,\mathbb{Z}}(m)$. Therefore we have $x, y \in \mathbb{Z}$ with $p\mathbb{Z}_K = \pi \cdot \bar{\pi} = (x + y \cdot \sqrt{-d}) \cdot (x - y \cdot \sqrt{-d}) = (x^2 + d \cdot y^2)$. From this we see that $p = x^2 + d \cdot y^2$. This completes the proof.

We want to give a more elementary way of saying that p splits completely in $Ri(O)$ in case where $Ri(O)$ equals $R_m(K)$.

Theorem 3.5 *Let d be a positive integer. Let $R_m(K)$ be the ray class field of $K = \mathbb{Q}(\sqrt{-d})$ with modulus $m = [\mathbb{Z}_K : \mathbb{Z}[\sqrt{-d}]]$. Suppose that the integer $m \in \{1, 2, 3, 4, 6\}$. Then there is a minimal monic irreducible polynomial $f = f^{\alpha}_{\mathbb{Q}}(x)$ of $R_m(K) \cap \mathbb{R}$ over $\mathbb{Q}$ in $\mathbb{Z}[x]$, such that if an odd prime p divides neither d nor the discriminant of f, then*

$$F_d \text{ represents } p \Leftrightarrow (\frac{-d}{p}) = 1 \text{ and } f \equiv 0 \bmod p \text{ has an integer solution.}$$

Furthermore, f may be taken to be the minimal polynomial of a real algebraic integer α for which $R_m(K) = K(\alpha)$.

Proof:
Let $O = \mathbb{Z}[\sqrt{-d}]$. Since $[\mathbb{Z}_K : \mathbb{Z}[\sqrt{-d}]] = 1, 2, 3, 4, 6$ we have $Ri(O) = R_K(m)$. We will work in the following fields $\mathbb{Q} \subset K \subset R_m(K)$ and $L = \mathbb{R} \cap R_m(K)$. Let τ be complex conjugation. Because $\tau(R_m(K))$ is an abelian extension of K with conductor $\tau(m) = m$ we see that $\tau(R_m(K)) \subset R_m(K)$, by theorem (2.11). Therefore $R_m(K)$ is Galois over $\mathbb{Q}$. The fixed field of the subgroup generated by τ is contained in $\mathbb{R}$, so this field is L and $[R_m(K) : L] = 2$. Let α be an algebraic integer such that $L = \mathbb{Q}(\alpha)$ and let $f = f^{\alpha}_{L/\mathbb{Q}}$ be the minimal polynomial of α over $\mathbb{Q}$. Because the compositum of L and K is $R_m(K)$, the polynomial f can also be seen as the minimal polynomial of $R_m(K)$ over K.
"$\Rightarrow$": Suppose that $p = x^2 + d \cdot y^2$. Since p is an odd prime not dividing d, we have using (3.4) that p splits completely in $R_m(K)$ and $(\frac{-d}{p}) = 1$. Thus p splits completely in L. And with the Kummer-Dedekind theorem (see [Cohen] page 299) we see that $f \equiv 0 \bmod p$ has an integer solution.
"$\Leftarrow$": Suppose that $(\frac{-d}{p}) = 1$ then p splits in K, let's say $p\mathbb{Z}_K = \pi\bar{\pi}$. Because $(\mathbb{Z}_K/\pi) \cong \mathbb{F}_p$ we see $f \equiv 0 \bmod \pi$ has a solution. And because $R_m(K)/K$ is Galois and p does not divide $\Delta(f)$, we see that π splits completely in $R_m(K)$. With the same argument we get $\bar{\pi}$ splits completely in $R_m(K)$. We conclude that p splits completely in $R_m(K)$. Hence using theorem (3.4) we get F_d represents p. This completes the proof.

If you want to know how to find the polynomial f in theorem (3.5) then you might want to read the text after the proof of theorem (3.3).

In chapter one we mentioned that for $d = 3, 7, 15$ we have $|\#s_{20}(d) - \#s_{20}(2d)| \leq 1$. For the cases $d = 3, 15$ the following proposition will be used to prove that if $d \neq M_l$ then F_d represents M_l if and only if F_{2d} represents M_l.

Proposition 3.6 *Let $d \equiv 3 \bmod 4$ be a positive squarefree integer. Suppose that $L = R_2(\mathbb{Q}(\sqrt{-d}))(\sqrt{2}) = H(\mathbb{Q}(\sqrt{-2d}))$. Let M_l be a Mersenne prime unramified in L then*

$$F_d \text{ represents } M_l \Leftrightarrow F_{2d} \text{ represents } M_l.$$

Proof:
We have $M_l = (\sqrt{2}^l - 1) \cdot (\sqrt{2}^l + 1)$, so M_l splits in $\mathbb{Q}(\sqrt{2})$. We want to use

theorem (3.4). The prime M_l is unramified in L, so we have $M_l \nmid 2d$. We have $[\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})} : \mathbb{Z}[\sqrt{-d}]] = 2$, because $d \equiv 3 \bmod 4$ is a positive squarefree integer. Using the fact that M_l splits in $\mathbb{Q}(\sqrt{2})$ and theorem (3.4) we get: F_d represents M_l if and only if M_l splits completely in $R_2(\mathbb{Q}(\sqrt{-d}))(\sqrt{2})$. We have $[\mathbb{Z}_{\mathbb{Q}(\sqrt{-2d})} : \mathbb{Z}[\sqrt{-2d}]] = 1$, so with theorem (3.4) we get: F_{2d} represents M_l if and only if M_l splits completely in $H(\mathbb{Q}(\sqrt{-2d}))$. By assumption we have $R_2(\mathbb{Q}(\sqrt{-d}))(\sqrt{2}) = H(\mathbb{Q}(\sqrt{-2d}))$, so the theorem follows. This completes the proof.

The next proposition will be used in the proof of theorem (4.1) and in chapter three. In the proof of this proposition we will use the following theorem.

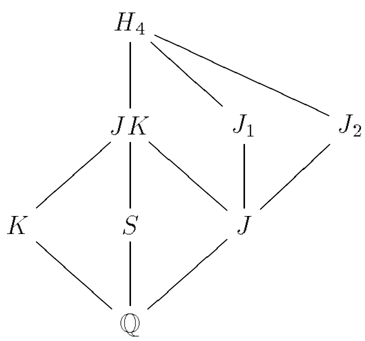
Theorem 3.7 *Let K be an imaginary quadratic field. Then an Abelian extension L of K is generalized dihedral over $\mathbb{Q}$, if and only if L is contained in a ring class field of K.*

Proof: See [Cox] page 191.

So if L is contained in a ring class field of K then we know that L over $\mathbb{Q}$ is Galois. And the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to $\mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$, where the nontrivial element τ of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(L/K)$ via conjugation by τ and this action sends every element of $\mathrm{Gal}(L/K)$ to its inverse.

Proposition 3.8 *Let $d \equiv 3 \bmod 4$ be a squarefree positive integer. Suppose that there exists a cyclic extension H_4 of $S = \mathbb{Q}(\sqrt{-2 \cdot d})$, with $[H_4 : S] = 4$, $H_4 \subset H(S)$ and $\sqrt{2} \in H_4$. Let M_l be a Mersenne prime. Suppose that $l \equiv 1 \bmod 2n$, where n is equal to the order of 2 in the group $(\mathbb{Z}/d)^*$, then M_l splits completely in H_4.*

Proof:
Let $K = \mathbb{Q}(\sqrt{-d})$ and let $J = \mathbb{Q}(\sqrt{2})$. Because $\sqrt{2}$ is an element of H_4, we have that J is contained in H_4. From the final part of theorem (3.7) it follows that $\mathrm{Gal}(H_4/\mathbb{Q})$ is isomorphic to the dihedral group with 8 elements. So there are two conjugated field extensions of J, say J_1 and J_2, contained in H_4. We have the following field diagram.



The discriminant of JK over J is $-d$. To see this use theorem (2.4) on the extensions K and J of $\mathbb{Q}$ and the fact that $d \equiv 3 \bmod 4$ to calculate the ring of algebraic integers $\mathbb{Z}_{JK}$. Then one sees that $\mathbb{Z}_{JK}$ is a free module over $\mathbb{Z}_J$, so one can easily calculate the discriminant $\Delta(JK/J)$. The discriminants $\Delta(J_1/J)$ and $\Delta(J_2/J)$ must be relative prime. To see this suppose that the discriminants were not relative prime. Then we would have a prime of J which would be ramified in J_1 and J_2. This prime would also be ramified in JK, because $\Delta(H_4/JK) = 1$. But then the inertia field of this prime equals J, which cannot be the case since $\Delta(H_4/JK) = 1$. Using theorem (2.3) on the extension $J \subset JK \subset H_4$ and theorem (2.4) on the linearly disjoint extension J_1 and J_2 of J we get $-d = \Delta(J_1/J)\Delta(J_2/J)$. Now take $v_l = \frac{\sqrt{2}^l-1}{\sqrt{2}-1}$ and $\tilde{v}_l = \frac{\sqrt{2}^l+1}{\sqrt{2}+1}$ (note $v_l \cdot \tilde{v}_l = M_l = 2^l - 1$). Using the fact that l is odd we see that v_l and $\tilde{v}_l$ are both elements of $\mathbb{Z}_J$. Because $l \equiv 1 \bmod 2n$ we have $\sqrt{2}^l \equiv \sqrt{2} \bmod (d)\mathbb{Z}_J$. Hence $v_l \equiv \tilde{v}_l \equiv 1 \bmod (d)\mathbb{Z}_J$ and also $\forall\, \sigma \in \mathrm{Gal}(J/\mathbb{Q})$ we have $\sigma(v_l) > 0$ and $\sigma(\tilde{v}_l) > 0$, because l is odd implies $\sigma(\sqrt{2}^l \pm 1)\sigma(\sqrt{2} \pm 1) > 0$. In other notation we have:

$$v_l \equiv \tilde{v}_l \equiv 1 \bmod (d)\mathbb{Z}_J \quad \wedge \quad \forall\, \sigma \in \mathrm{Gal}(J/\mathbb{Q}) \text{ we have } \sigma(v_l) > 0 \text{ and } \sigma(\tilde{v}_l) > 0.$$

Using the Chinese remainder theorem, $\Delta(J_1/J)$ and $\Delta(J_2/J)$ are coprime, we get:

$$v_l \equiv \tilde{v}_l \equiv 1 \bmod (\Delta(J_1/J))\mathbb{Z}_J \ \wedge \ v_l \equiv \tilde{v}_l \equiv 1 \bmod (\Delta(J_2/J))\mathbb{Z}_J \ \wedge$$
$$\forall\, \sigma \in \mathrm{Gal}(J/\mathbb{Q}) \text{ we have } \sigma(v_l) > 0 \text{ and } \sigma(\tilde{v}_l) > 0.$$

Now we apply the Artin map and theorem 2.10. This gives:

$$\left(\frac{(v_l)}{J_i/J}\right) = \left(\frac{(\tilde{v}_l)}{J_i/J}\right) = e \text{ for } i \in \{1, 2\},$$

because v_l and $\tilde{v}_l$ are in the kernel. The Galois group of H_4/J is isomorphic to $\mathrm{Gal}(J_1/J) \times \mathrm{Gal}(J_2/J)$. So:

$$\left(\frac{(v_l)}{H_4/J}\right) = \left(\frac{(\tilde{v}_l)}{H_4/J}\right) = e.$$

So M_l splits completely in H_4. This completes the proof.

The following proposition will be used for the cases $d = 14$ and $d = 46$ in the next section.

Proposition 3.9 *Let $p \equiv 3 \bmod 4$ be a prime. Suppose that $\mathrm{Cl}(\mathbb{Q}(\sqrt{-2p}))$ is isomorphic to the cyclic group with four elements. Let M_l be a Mersenne prime. Suppose that $l \equiv 1 \bmod 2n$, where n is equal to the order of 2 in the group $(\mathbb{Z}/p)^*$, then F_{2p} represents M_l.*

Proof:
From proposition (3.8) we know that M_l splits completely in $H(\mathbb{Q}(\sqrt{-2p}))$. Then we apply theorem (3.2). This completes the proof.

3.2 The cases with d between 0 and 48.

In this section we will apply the theory of the previous section to decide whether or not F_d represents M_l, where M_l is a Mersenne prime and where d lies between 0 and 48.

For the cases $d \equiv 0, 1, 2, 4, 5 \bmod 8$, with $d \neq 2$, we have F_d doesn't represent M_l (see proposition (1.1)). We will deal with the remaining cases below.

The case $d = 2$.

From proposition (1.1) we get: Suppose that M_l is a Mersenne prime then F_d represents M_l if and only if

$$l = 2.$$

The case $d = 3$.

For $d = 3$ we have $m = 2$ (see theorem (3.5)). Because the class number of $K = \mathbb{Q}(\sqrt{-3})$ is 1, we have that the ray class group of K is $\mathrm{Cl}_2(K) = I_K(2)/P_{K,1}(2) = P_K(2)/P_{K,1}(2)$. Because $\frac{1+\sqrt{-3}}{2} \bmod 2\mathbb{Z}_K$ is clearly in the kernel of the surjective group homomorphism $(\mathbb{Z}_K/2)^* \twoheadrightarrow P_K(2)/P_{K,1}(2)$, we see that the group $P_K(2)/P_{K,1}(2)$ is trivial. So $R_2(K) = K$. Now $M_l = 2^l - 1$, so $M_l \equiv -1 \bmod 4$. If $l = 2$ then we have the solution $3 = 0^2 + 3 \cdot 1^2$. Suppose $l \neq 2$ then $(\frac{-3}{M_l}) = (\frac{-1}{M_l})(\frac{3}{M_l}) = (-1)(-(\frac{M_l}{3})) = 1$. With theorem (3.5) we get: Suppose that M_l is a Mersenne prime then F_3 represents M_l.

The case $d = 6$.

Suppose $d = 6$. Then we have $K = \mathbb{Q}(\sqrt{-6})$. The class number of K is 2. So we get $[H(K) : K] = 2$. Using theorem (2.14) we have that $K(\sqrt{-3}) = K(\sqrt{2})$ is unramified over K, so $H(K) = K(\sqrt{2})$. But now we have $R_2(\mathbb{Q}\sqrt{-3})(\sqrt{2}) = H(\mathbb{Q}(\sqrt{-6}))$. Using proposition (3.6) we get the following result: Suppose that M_l is a Mersenne prime then F_6 represents M_l if and only if

$$l \neq 2.$$

The case $d = 7$.

The next d is $d = 7$. The class number of $K = \mathbb{Q}(\sqrt{-7})$ is 1 and $m = 2$. So $\mathrm{Cl}_2 = P_K(2)/P_{K,1}(2)$. Again we have the surjective homomorphism $(\mathbb{Z}_K/2)^* \twoheadrightarrow P_K(2)/P_{K,1}(2)$. But 2 splits in K so $(\mathbb{Z}_K/2)^*$ has only one element. Therefore $R_2(K) = K$. Take $M_l = 2^l - 1$ with $l \neq 2, 3$. Then $(\frac{-7}{M_l}) = (\frac{-1}{M_l})(-(\frac{M_l}{7})) = (\frac{M_l}{7})$. Now $(\frac{M_l}{7}) = 1$ if and only if $l \equiv 1 \bmod 3$. With theorem (3.5) we get: Suppose that M_l is a Mersenne prime then F_7 represents M_l if and only if

$$l \equiv 1 \bmod 3 \textit{ or } l = 3.$$

The case $d = 11$.

Take $d = 11$. Then $K = \mathbb{Q}(\sqrt{-11})$. The class number of K is 1 and 2 is inert in K. So using (2.4) we get that $[R_2(K) : K] = 3$. From the discriminant $\Delta(K/\mathbb{Q}) = -11$ and the modulus 2 we know that only the primes 2 and 11 of $\mathbb{Q}$ ramify in $R_2(K)$. Let's take a look at the field $L = R_2(K) \cap \mathbb{R}$ of degree 3 over $\mathbb{Q}$. We know that only 2 is totally ramified in L, because the modulus of $R_2(K)$ over K is 2 and $R_2(K)$ over K is Galois. From theorem (3.7) we get that the Galois group of $R_2(K)$ over $\mathbb{Q}$ is the S_3, therefore $R_2(K)$ is the Galois closure of L over $\mathbb{Q}$. Suppose that 11 is unramified in L, then 11 would be unramified in all the conjugates of L and therefore unramified in $R_2(K)$, which is not the case. From this we see that the different of $L/\mathbb{Q}$ only has the factors π_2^2 and π_{11}, with π_2 the prime above 2 and π_{11} the ramified prime above 11 (see [Koch] page 33 for the theory about different and ramification). Because K is contained in $R_2(K)$ and we know the factors of the different, we get $\Delta(L/\mathbb{Q}) = -44$. In [Cohen] page 509 we find an irreducible polynomial of degree 3 with discriminant -44, namely $f(x) = x^3 - x^2 - x - 1$. Let α be a zero of $f(x)$. Then $S = \mathbb{Q}(\alpha)(\sqrt{-11})$ is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Only the prime 2 of K ramifies totally in S. The conductor of S/K is therefore 2, see theorem (2.15). So from theorem (2.13) we get $S = R_2(K)$. We have $(\frac{-11}{M_l}) = (\frac{M_l}{11})$. Because $M_l = 2^l - 1$ is prime we have l is prime so $l \equiv 1, 3, 7, 9 \bmod 10$. This implies that $M_l \equiv 1, 7, 6, 5 \bmod 11$ respectively. But only $1, 5 \bmod 11$ are square. From theorem (3.5) we get: Suppose that M_l is a Mersenne prime then F_{11} represents M_l if and only if

$$l \equiv \pm 1 \bmod 5 \ \wedge \exists x \in \mathbb{Z} \ with \ x^3 - x^2 - x - 1 \equiv 0 \bmod M_l.$$

The case $d = 14$.

The next d is $d = 14$. The class group of $K = \mathbb{Q}(\sqrt{-14})$ is cyclic of degree four. We want to use proposition (3.9). The order of 2 in $(\mathbb{Z}/7)^*$ is three. From $(\frac{-14}{M_l}) = (\frac{2}{M_l})(\frac{-7}{M_l}) = (\frac{-7}{M_l}) = 1$ we get that $l \equiv 1 \bmod 3$ assuming that F_{14} represents M_l (see $d = 7$). But since $l \neq 2$ is prime we have $l \equiv 1 \bmod 6$. So with proposition (3.9) we get: Suppose that M_l is a Mersenne prime then F_{14} represents M_l if and only if

$$l \equiv 1 \bmod 3.$$

The case $d = 15$.

Take $d = 15$. Then the class number of $K = \mathbb{Q}(\sqrt{-15})$ is 2 and 2 splits in K. Using 2.4 we get $[I_K(2) : P_{K,1}(2)] = 2$. Now we can use theorem (2.14) to see that $R_2(K) = K(\sqrt{5})$. From $(\frac{-15}{M_l}) = (\frac{M_l}{5})$, we see that l has to be equivalent to 1 modulo 4 assuming that F_{15} represents M_l. And because the minimal polynomial of $R_2(K)/K$ is $x^2 - 5$ we see that this condition is enough to write M_l as $x^2 + 15 \cdot y^2$. So with theorem (3.5) we get: Suppose that M_l is a Mersenne prime then F_{15} represents M_l if and only if

$$l \equiv 1 \bmod 4.$$

The case $d = 19$.

Take $d = 19$. This one looks just like $d = 11$. Now $h_K = 1$ and 2 is inert in $K = \mathbb{Q}(\sqrt{-19})$. So we have to find a irreducible polynomial $f(x)$ with discriminant $-4 \cdot 19$. In [Cohen] page 509 we find $f(x) = x^3 - 2x - 2$. From the other condition $(\frac{-19}{M_l}) = (\frac{-1}{M_l})(-(\frac{M_l}{19})) = (\frac{M_l}{19}) = 1$, we get $l \equiv \pm 1 \bmod 18$ after some calculations. This gives: Suppose that M_l is a Mersenne prime then F_{19} represents M_l if and only if

$$l \equiv \pm 1 \bmod 9 \wedge \exists x \in \mathbb{Z} \textit{ with } x^3 - 2x - 2 \equiv 0 \bmod M_l.$$

The case $d = 22$.

Take $d = 22$. The class number of $K = \mathbb{Q}(\sqrt{-22})$ is 2. By theorem (2.14) we have that $H(K) = K(\sqrt{-11}) = K(\sqrt{2})$. Because $M_l \equiv -1 \bmod 8$ we have $(\frac{2}{M_l}) = 1$, so the polynomial $x^2 - 2 \equiv 0 \bmod M_l$ has an integer solution. By theorem (3.3) we only need to check $(\frac{-22}{M_l}) = (\frac{-1}{M_l})(\frac{2}{M_l})(\frac{11}{M_l}) = (-1)(1)(-(\frac{M_l}{11})) = (\frac{M_l}{11})$. Because $M_l = 2^l - 1$ is prime we have l is prime so $l \equiv 1, 3, 7, 9 \bmod 10$. This implies that $M_l \equiv 1, 7, 6, 5 \bmod 11$ respectively. But only $1, 5 \bmod 11$ are square. This gives use: Suppose that M_l is a Mersenne prime then F_{22} represents M_l if and only if

$$l \equiv \pm 1 \bmod 5 \textit{ or } l = 5.$$

The case $d = 23$.

Take $d = 23$. Then $h_K = 3$ and 2 splits in $K = \mathbb{Q}(\sqrt{-23})$. So $R_2(K) = H(K)$. We can use the same arguments of $d = 11$. We have to find an irreducible polynomial of degree 3 with discriminant -23. Now $f(x) = x^3 + x^2 - 1$ is such a polynomial (see [Cohen] page 509). From $(\frac{-23}{M_l}) = (\frac{M_l}{23}) = 1$ we get $l \equiv 1, 2, 5, 7, 8 \bmod 11$. This gives us: Suppose that M_l is a Mersenne prime then F_{23} represents M_l if and only if

$$l \equiv 1, 2, 5, 7, 8 \bmod 11 \ \wedge \exists x \in \mathbb{Z} \textit{ with } x^3 + x^2 - 1 \equiv 0 \bmod M_l.$$

The case $d = 27$.

Take $d = 27$. Then $m = 6$ and $h_K = 1$, with $K = \mathbb{Q}(\sqrt{-3})$. The units of $\mathbb{Z}_K$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$, with $\omega = \frac{-1+\sqrt{-3}}{2}$. Because we have an isomorphism from $\mathbb{Z}_K^*$ to $(\mathbb{Z}_K/3\mathbb{Z}_K)^*$ and the prime 2 of $\mathbb{Q}$ is inert in K, we get $\#(\mathrm{Cl}_6(K)) = 3$ (see (2.4)). So we have to find an abelian extension L of K with conductor 6 and $[L : K] = 3$. Take $L = K(\sqrt[3]{2})$, then clearly L is an abelian extension of K and $[L : K] = 3$. Because the discriminant of $x^3 - 2$ is $-108 = -2^3 \cdot 3^3$

we have that only 2 and 3 ramify in L. Now we will calculate the conductor f of L over K. Using theorem (2.15) we get $2 \parallel f$. Now $\sqrt{-3}$ is not tamely ramified so we have to use theorem (2.16). The ring of algebraic integers of L is $\mathbb{Z}_L = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}, \sqrt[3]{2}]$. So the ring of integers of the local field $\mathbb{Q}_3(\sqrt{-3}, \sqrt[3]{2})$ is $B = \mathbb{Z}_3[\sqrt{-3}, \sqrt[3]{2}]$. Let $\beta = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \in B^*$ with $a, b, c \in A$ then $N(\beta) = a^3 - 2b^3 - 6abc + 4c^3 \in A^*$ with $A = \mathbb{Z}_3[\sqrt{-3}]$ the ring of integers of the local field $\mathbb{Q}_3(\sqrt{-3})$ and $N = \mathbf{N}_{\sqrt{-3}}$ the local norm. So we have $(A^*)^3 \subset N(B^*)$. We will show that $(A^*)^3 = \pm 1 + \sqrt{-3}^4 A$. Let $\alpha \in A^*$ then $\alpha = \pm 1 + \sqrt{-3}n$ with $n \in A$. Now $\alpha^3 = (\pm 1) + (n^3 - n)\sqrt{-3}^3 + (\pm 1)n^2\sqrt{-3}^4$, but $\sqrt{-3} \mid n^3 - n$ because $n^3 \equiv n \bmod \sqrt{-3}$. So $(A^*)^3 \subset \pm 1 + \sqrt{-3}^4 A$. Let $x \in \pm 1 + \sqrt{-3}^5 A$. We will use Hensel's lemma (see [Lang] page 42) to show that $x \in (A^*)^3$. Therefore we have to prove that the polynomial $f(X) = X^3 \mp x$ has a zero in A. But $|f(1)| \leq |\sqrt{-3}^5| < |3 \cdot 2|^2 = |f'(1)|^2$, so with Hensel's lemma we get $\pm 1 + \sqrt{-3}^5 A \subset (A^*)^3 \subset \pm 1 + \sqrt{-3}^4 A$. But $2^3 = -1 + \sqrt{-3}^4 \notin \pm 1 + \sqrt{-3}^5 A$ and $[\pm 1 + \sqrt{-3}^4 A : \pm 1 + \sqrt{-3}^5 A] = 3$, hence $(A^*)^3 = \pm 1 + \sqrt{-3}^4 A \subset N(B^*)$. Let $(a, b, c) = a^3 - 2b^3 - 6abc + 4c^3$. Take $(a, b, c) = (\pm 1, \pm\sqrt{-3}, 0)$ then we see that $\pm 1 + \sqrt{-3}^3 + \sqrt{-3}^5$ and $\pm 1 - \sqrt{-3}^3 - \sqrt{-3}^5$ are elements of $N(B^*)$, so $\pm 1 \pm \sqrt{-3}^3 \in N(B^*)$, hence $\pm 1 + \sqrt{-3}^3 A \subset N(B^*)$. Taking $(0, 0, \pm 1)$ and $(0, \pm 1, 0)$ we see that $\pm 1 \pm \sqrt{-3}^2 \in N(B^*)$, hence $\pm 1 + \sqrt{-3}^2 A \subset N(B^*)$. Because $\pm 1 + \sqrt{-3}A = A^*$ and $\sqrt{-3}$ is ramified in L we get $\pm 1 + \sqrt{-3}^2 A = N(B^*)$ so $(\sqrt{-3}^2) \parallel f$, thus $f = 6$. So $L = R_6(K)$. If $M_l > 27$, which must be the case if F_{27} represents M_l, then we have $(\frac{-3}{M_l}) = 1$. For cyclic groups of order n we know that there is a unique subgroup of order d if $d \mid n$. Let $l \neq 2, 3$. Then $3 \mid M_l - 1$ so there exist a unique subgroup of index 3 in $\mathbb{F}_{M_l}^*$, namely $(\mathbb{F}_{M_l}^*)^3$. The order of the subgroup generated by 2 is l. Because $l \neq 3$ we have $3 \mid \frac{p-1}{l}$ so $2 \in (\mathbb{F}_{M_l}^*)^3$. Hence $x^3 - 2 \equiv 0 \bmod M_l$ always has a solution if $l \neq 2, 3$. From theorem (3.5) we get: Suppose that M_l is a Mersenne prime then F_{27} represents M_l if and only if

$$l \neq 2, 3.$$

Now we are able to prove the following observation made in chapter one.

Theorem 3.10 *Let $M_l > 7$ be a Mersenne prime. Let (x, y) be the F_3-solution of M_l then $3 \mid y$.*

Proof:
If $M_l > 7$ then $l > 3$ so F_{27} represents M_l, see case $d = 27$. Let (x', y') be the F_{27}-solution of M_l then $(x', 3y')$ is the F_3-solution of M_l. From proposition (0.3) we get that $(x', 3y') = (x, y)$. Hence we have $3 \mid y$. This completes the proof.

The case $d = 30$.

Take $d = 30$. The class number of $K = \mathbb{Q}(\sqrt{-30})$ is 4. With theorem (2.14) we get $H(K)$. But $H(K) = R_2(\mathbb{Q}(\sqrt{-15})(\sqrt{2})$ so from proposition (3.6) we get:

Suppose that M_l is a Mersenne prime then F_{30} represents M_l if and only if

$$l \equiv 1 \bmod 4.$$

The case $d = 31$.

Take $d = 31$. Then $h_K = 3$ and 2 is splits in $K = \mathbb{Q}(\sqrt{-31})$. The number of elements of $\mathrm{Cl}_2(K)$ is 3. So $R_2(K) = H(K)$. So we have to find an irreducible polynomial of degree 3. The polynomial $f(x) = x^3+x^2+1$ is such a polynomial. Hence we get: Suppose that M_l is a Mersenne prime then F_{31} represents M_l if and only if

$$l \equiv 1, 3 \bmod 5 \ \wedge \exists x \in \mathbb{Z} \ with\ x^3 + x^2 + 1 \equiv 0 \bmod M_l \ or\ l = 5.$$

The case $d = 35$.

Take $d = 35$. Then $h_K = 2$ and 2 is inert in $K = \mathbb{Q}(\sqrt{-35})$. The number of elements of $\mathrm{Cl}_2(K)$ is 6. To find $R_2(K)$ we find two subfields of $R = R_2(K)$. First using theorem (2.14) we get $H(K) = K(\sqrt{5}) \subset R$. Using the same arguments as with $d = 11$ we find the other field. Hence we get: Suppose that M_l is a Mersenne prime then F_{35} represents M_l if and only if

$$l \equiv 1 \bmod 12 \ \wedge \exists x \in \mathbb{Z} \ with\ x^3 + 2x - 2 \equiv 0 \bmod M_l.$$

The case $d = 38$.

Take $d = 38$. Then $h_K = 6$ with $K = \mathbb{Q}(\sqrt{-38})$. We have to find two unramified abelian extensions of K of degree 2 and 3. The first one $K(\sqrt{2})$ we find using theorem (2.14). The second one is an extension of K of degree three. The polynomial $f(x) = x^3 - x^2 - 2x - 2$ has discriminant $-152 = -2^3 \cdot 19$. Let α be a zero of f. The Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $L = K(\alpha)$ because it contains $\sqrt{-152} = 4 \cdot \sqrt{-38}$. Only 2 and 19 ramify in L. We know from the discriminant of f that 2 and 19 are not totally ramified in $\mathbb{Q}(\alpha)$, else $2^2 \parallel \Delta(\mathbb{Q}(\alpha)/\mathbb{Q})$ and/or $19^2 \parallel \Delta(\mathbb{Q}(\alpha)/\mathbb{Q})$. Because L/K is Galois we have $e(\beta/\pi) = 1, 3$, with β a prime in L above a prime π in K. Hence L over K is unramified. So L is our field. From $d = 19$ we know that $(\frac{-38}{M_l}) = 1$ if and only if $l \equiv \pm 1 \bmod 9$. Hence we get: Suppose that M_l is a Mersenne prime then F_{38} represents M_l if and only if

$$l \equiv \pm 1 \bmod 9 \wedge \ \exists x \in \mathbb{Z} \ with\ x^3 - x^2 - 2x - 2 \equiv 0 \bmod M_l.$$

The case $d = 39$.

Take $d = 39$. Then $\mathrm{Cl}(K)$ is the cyclic group with four elements and 2 splits in $K = \mathbb{Q}(\sqrt{-39})$. So $R_2(K) = H(K)$. By theorem (3.5) we know that $\mathrm{Gal}(H(K)/\mathbb{Q})$ is the dihedral group with eight elements. We will use the idea of proposition (3.8). So we have to find two irreducible polynomials in $\mathbb{Q}(\sqrt{13})[x]$ such that the product of there discriminants is -3. Take $f_1(x) =$

$x^2 + (1 + (\frac{1+\sqrt{13}}{2}))x + (1 + (\frac{1+\sqrt{13}}{2}))$ and $f_2(x) = x^2 + (\frac{1+\sqrt{13}}{2})x + 1$. Then $\Delta(f_1)\Delta(f_2) = -(\frac{1+\sqrt{13}}{2}) \cdot -(\frac{1-\sqrt{13}}{2}) = -3$. From $(\frac{-39}{M_l}) = (\frac{M_l}{13}) = 1$ we get $l \equiv 1 \bmod 3$. So if $l \equiv 1 \bmod 3$ then M_l splits in $\mathbb{Q}(\sqrt{13})$. But we also want that the primes above M_l, say π and $\bar{\pi}$, split in $H(K)$. Because $H(K)$ over $\mathbb{Q}$ is Galois we have: M_l splits in $H(K)$ if and only if $l \equiv 1 \bmod 3$ and both equivalence relations $x^2 \equiv -(\frac{1\pm\sqrt{13}}{2}) \bmod \pi$ have solutions. A homomorphism from $\mathbb{Z}[\sqrt{13}]$ to $\mathbb{F}_{2^l-1}$ has as kernel π or $\bar{\pi}$. The element $\sqrt{13}$ can be mapped to $\pm x$, with $x^2 \equiv 13 \bmod M_l$. So $-\frac{1\pm\sqrt{13}}{2}$ will be mapped to $-\frac{1\pm x}{2}$, no matter which map we choose. It follows that $x^2 \equiv -(\frac{1\pm\sqrt{13}}{2}) \bmod \pi$ have solutions is equivalent with $(\frac{-\frac{1\pm x}{2}}{M_l}) = 1$. Since $(\frac{-\frac{1-x}{2}}{M_l})(\frac{-\frac{1+x}{2}}{M_l}) = (\frac{-3}{M_l}) = (\frac{M_l}{3}) = 1$ if and only if $l \equiv 1 \bmod 3$, we get: Suppose that M_l is a Mersenne prime then F_{39} represents M_l if and only if

$$l \equiv 1 \bmod 3 \;\wedge\; (\frac{-1+\sqrt{13}}{M_l}) = 1.$$

Note that $\sqrt{13} \in \mathbb{F}_{M_l}$ since $l \equiv 1 \bmod 3$ implies $(\frac{13}{M_l}) = 1$.

The case $d = 43$.

Take $d = 43$. Then $h_K = 1$ and 2 is inert in $K = \mathbb{Q}(\sqrt{-43})$. Using the same arguments as with $d = 11$ we get: Suppose that M_l is a Mersenne prime then F_{43} represents M_l if and only if

$$l \equiv \pm 1, \pm 2 \bmod 7 \;\; \wedge \exists x \in \mathbb{Z} \; with \; x^3 + x^2 - x - 3 \equiv 0 \bmod M_l.$$

The case $d = 46$.

Take $d = 46$. Then $\mathrm{Cl}(K)$ is the cyclic group with four elements, $K = \mathbb{Q}(\sqrt{-46})$. Clearly $\sqrt{2} \in H(K)$ so we can use proposition (3.9). So we already have: Suppose that M_l is a Mersenne prime then F_{46} represents M_l if

$$l \equiv 1 \bmod 11.$$

We will construct the two distinct conjugated subfields of $H(K)$ containing $\mathbb{Q}(\sqrt{2})$. With the proof of proposition (3.8) in mind we need to find two polynomials in $\mathbb{Q}(\sqrt{2})[x]$ such that the product of there discriminants is -23. Take $f_1(x) = x^2 + (1-\sqrt{2})x + (-1+\sqrt{2})$ and $f_2(x) = x^2 + (1+\sqrt{2})x + (-1-\sqrt{2})$. Now $\Delta(f_1)\Delta(f_2) = (7-6\sqrt{2})(7+6\sqrt{2}) = -23$. We know that $M_l = x^2 + 46 \cdot y^2$ if and only if M_l splits completely in $H(K)$. Clearly M_l splits in $\mathbb{Q}(\sqrt{2})$, say $M_l = \pi\bar{\pi}$. Because $H(K)$ over $\mathbb{Q}$ is Galois we have: $M_l = x^2 + 46 \cdot y^2$ if and only if π and $\bar{\pi}$ split in J_1 and J_2 (J_1 and J_2 the two field extensions of $\mathbb{Q}(\sqrt{2})$ corresponding to f_1 and f_2) if and only if both equivalence relations $x^2 \equiv 7 \pm 6\sqrt{2} \bmod \pi$ have solutions. A homomorphism from $\mathbb{Z}[\sqrt{2}]$ to $\mathbb{F}_{2^l-1}$ has as kernel π or $\bar{\pi}$. The element $\sqrt{2}$ can be mapped to $\pm 2^{\frac{l+1}{2}}$. The element $7 \pm 6\sqrt{2}$ will be mapped to $7 \pm 6 \cdot 2^{\frac{l+1}{2}}$, no matter which map we choose. It follows that $x^2 \equiv 7 \pm 6\sqrt{2} \bmod \pi$

have solutions is equivalent with $(\frac{7\pm 6\cdot 2^{\frac{l+1}{2}}}{M_l}) = 1$. From $(\frac{-46}{M_l}) = 1$ we get $l \equiv 1,2,5,7,8 \bmod 11$ (see $d=23$). Because $(\frac{-23}{M_l}) = (\frac{7-6\cdot 2^{\frac{l+1}{2}}}{M_l})(\frac{7+6\cdot 2^{\frac{l+1}{2}}}{M_l})$ we get: Suppose that M_l is a Mersenne prime then F_{46} represents M_l if and only if

$$l \equiv 1,2,5,7,8 \bmod 11 \ \wedge l \neq 2 \ \wedge (\frac{7-6\cdot\sqrt{2}}{M_l}) = 1.$$

Note that $\sqrt{2} \in \mathbb{F}_{M_l}$ since $l \neq 2$ implies $(\frac{2}{M_l}) = 1$.

The case $d = 47$.

Take $d = 47$. Then $h_K = 5$ and 2 splits in $K = \mathbb{Q}(\sqrt{-47})$. In [Cohen2] page 539 we find our polynomial $f(x) = x^5 - 2x^4 + 2x^3 - x^2 + 1$. Further $(\frac{-47}{M_l}) = 1$ if and only if $l \equiv 1,2,3,6,10,12,14,15,16,18,19 \bmod 23$. Hence we get: Suppose that M_l is a Mersenne prime then F_{47} represents M_l if and only if

$$\begin{gathered} l \equiv 1,2,3,6,10,12,14,15,16,18,19 \bmod 23 \ \wedge \\ \exists x \in \mathbb{Z} \ with \ x^5 - 2x^4 + 2x^3 - x^2 + 1 \equiv 0 \bmod M_l. \end{gathered}$$

Discussion

If we look at the numbers $\#s_{20}(d)$, for d between 0 and 48 (see the table in chapter one), and the polynomials, which occur in the criteria for these d's, then it seems to be possible to predict more or less the degree of these polynomials when the numbers $\#s_{20}(d)$ are given. In the table below we compare the numbers $\#s_{20}(d)$, for d between 0 and 48, and the degree of polynomials, which occur in the criteria for these d's. We have excluded all d's with $d \equiv 0,1,2,4,5 \bmod 8$. The d's and the numbers $\#s_{20}(d)$ are ordered in such a way that the first d appearing corresponds with the first $\#s_{20}(d)$ appearing, the second d appearing corresponds with the second $\#s_{20}(d)$ appearing, and so on.

d	degree of polynomial	$\#s_{20}(d)$
3,6,7,14,15,22,27,30	1	20,19,13,12,9,8,18,9
39,46	2	7,6
11,19,23,31,35,38,43	3	1,2,2,5,0,2,3
47	5	1

The number $\#s_{20}(31) = 5$ in the table above is large compared with the other numbers $\#s_{20}(d)$ that have a polynomial degree of 3. Of course if d is a Mersenne prime then F_d represents d, since $d = 0^2 + d\cdot 1^2$. So for $d = 31$ we get the Mersenne prime M_5 in $s_{20}(31)$ for free. We also get another Mersenne prime in $s_{20}(31)$ for free, namely M_{31}. The following theorem, proved by Peter Stevenhagen, explains why $M_{31} \in s_{20}(31)$.

Theorem 3.11 *Let M_l be a Mersenne prime with $l \equiv 3 \bmod 4$. Then F_l represents M_l.*

Proof:
We have $M_3 = 2^2 + 3 \cdot 1^2$, so we may assume that $l \neq 3$. Because M_l is prime we have l is prime. Let ζ_l be a primitive l^{th} root of unity. Let $S = \mathbb{Q}(\zeta_l)$ and let $K = \mathbb{Q}(\sqrt{-l})$. We know that there is only one prime, namely l, of $\mathbb{Z}$ that ramifies in S, and it is totally ramified (see [Lang] page 73). The Galois group of S over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/(l-1)\mathbb{Z}$, hence S contains a unique quadratic extension of $\mathbb{Q}$. The discriminant of this extension over $\mathbb{Q}$ can only be divisible by l. Since $l \equiv 3 \bmod 4$ we get $K \subset S$. The minimal polynomial of ζ_l over $\mathbb{Q}$ is

$$f(x) = \frac{x^l - 1}{x - 1} = \prod_{i=1}^{l-1} x - \zeta_l^i.$$

So $M_l = f(2)$ is equal to the norm $N_{S/\mathbb{Q}}(2 - \zeta_l)$. Hence we have $M_l \mathbb{Z}_K = \pi\bar{\pi}$ with let's say $\pi = (N_{S/K}(2 - \zeta_l))$ and $\bar{\pi} = (\overline{N_{S/K}(2 - \zeta_l)})$. From

$$N_{S/K}(2 - \zeta_l) \equiv N_{S/K}(\zeta_l) \equiv \zeta_l^i \bmod 2\mathbb{Z}_K$$

for a certain integer i and the fact that K does not contain any l^{th} root of unity unequal to 1 (here we use $l \neq 3$), we get $N_{S/K}(2 - \zeta_l) \equiv 1 \bmod 2\mathbb{Z}_K$. And since $\mathbb{Z}[\sqrt{-l}] = \mathbb{Z} + 2\mathbb{Z}_K$ we get $N_{S/K}(2 - \zeta_l) \in \mathbb{Z}[\sqrt{-l}]$. With the same argument we see $\overline{N_{S/K}(2 - \zeta_l)} \in \mathbb{Z}[\sqrt{-l}]$. Hence we have $x, y \in \mathbb{Z}$ with

$$M_l \mathbb{Z}_K = \pi\bar{\pi} = (x^2 + l \cdot y^2).$$

We conclude that F_l represents M_l. This completes the proof.

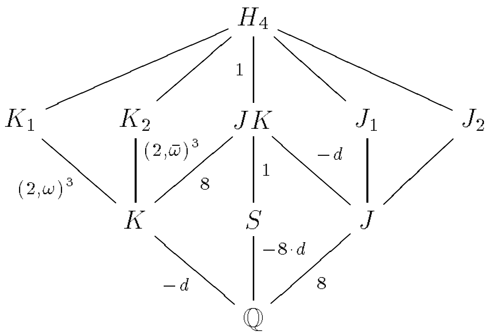
Chapter 4

Main theorem

In this chapter we will prove the main theorem. It will be an consequence of the following theorem.

Theorem 4.1 *Let $d \equiv 7 \bmod 24$ be a squarefree positive integer. Suppose that there exists a cyclic extension H_4 of $S = \mathbb{Q}(\sqrt{-2 \cdot d})$, with $[H_4 : S] = 4$, $H_4 \subset H(S)$ and $\sqrt{2} \in H_4$. Let $M_l = 2^l - 1$ be a Mersenne prime. Suppose that $l > 3$ and $l \equiv 1 \bmod 2n$, where n is equal to the order of 2 in the group $(\mathbb{Z}/d)^*$. Suppose that (x, y) is the F_d-solution of M_l then $8 \mid x$.*

Proof:
From theorem (3.5) we know that the Galois group of $H_4/\mathbb{Q}$ is the dihedral group with 8 elements. After we have calculated some discriminants we get the following diagram.



The numbers between the field extensions are the relative discriminants. With $K = \mathbb{Q}(\sqrt{-d})$, $S = \mathbb{Q}(\sqrt{(-d)2})$, $J = \mathbb{Q}(\sqrt{2})$, $\omega = \frac{1+\sqrt{-d}}{2}$, $\bar{\omega} = \frac{1-\sqrt{-d}}{2}$. Note that 2 splits in K as $(2, \omega)(2, \bar{\omega})$.
Now we will calculate the relative discriminants.
All the discriminants of the subfields of JK are easy to be found. Using theorem (2.3) on the extensions $K \subset JK \subset H_4$, we get $\Delta(H_4/K) = 8^2$. Also from theorem (2.3) we know that $\Delta(K_i/K) \mid 8^2$ for $i \in \{1, 2\}$. Suppose that $\Delta(K_1/K)$

and $\Delta(K_2/K)$ aren't coprime then there is a prime π of K dividing both discriminants. But π will also divide $\Delta(JK/K)$, so the inertia field of a prime in M above π will be K. This means that π has ramification index 4 in M, which cannot be the case, cause $\Delta(M/JK) = 1$. So $\Delta(K_1/K)$ and $\Delta(K_2/K)$ are coprime. Now we can use theorem (2.4). We get $\Delta(K_1/K) \cdot \Delta(K_2/K) = 8$. But since they were coprime and K_1 and K_2 are conjugated, we have $\Delta(K_1/K) = (2, \omega)^3$ and $\Delta(K_2/K) = (2, \bar{\omega})^3$. Let $\Delta = \Delta(K_1/K)$.

Now using theorem 2.10 we have the surjective homomorphism:

$$\mathrm{Cl}_\Delta(K) \twoheadrightarrow \mathrm{Gal}(K_2/K).$$

The group $P_K(\Delta)/P_{K,1}(\Delta)$ is a subgroup of $\mathrm{Cl}_\Delta(K)$ and contains the principal prime ideal $\pi = (x + \sqrt{-d} \cdot y)$ of K. Because $d \equiv 1 \bmod 3$ we have that the prime 3 of $\mathbb{Q}$ is inert in J and K and splits in S, so the decomposition field of a prime β in H_4 above 3 is S. We conclude that the prime $3\mathbb{Z}_K$ of K doesn't split in K_1. And therefore $P_K(\Delta)/P_{K,1}(\Delta)$ maps surjective on $\mathrm{Gal}(K_1/K)$. Clearly the map from $(\mathbb{Z}_K/\Delta)^*$ to $P_K(\Delta)/P_{K,1}(\Delta)$ is surjective. The group $(\mathbb{Z}_K/\Delta)^*$ is isomorphic to the group $(\mathbb{Z}/8\mathbb{Z})^*$. To see this, note that $(2, \omega)^3(2, \bar{\omega})^3 = (8)$. Now we have the following group homomorphisms:

$$(\mathbb{Z}/8\mathbb{Z})^* \cong (\mathbb{Z}_K/\Delta)^* \twoheadrightarrow P_K(\Delta)/P_{K,1}(\Delta) \twoheadrightarrow \mathrm{Gal}(K_1/K).$$

Because $(\alpha) = (-\alpha)$, it follows that $\{\pm 1\}$ is contained in the kernel of the first arrow. But $\#((\mathbb{Z}/8)^*) = 4 = \#((\mathbb{Z}_K/\Delta)^*)$ and the first arrow is surjective, so the kernel of the first arrow equals $\{\pm 1\}$. Therefore $P_K(\Delta)/P_{K,1}(\Delta)$ has two elements. So:

$$(\mathbb{Z}/8\mathbb{Z})^* \cong (\mathbb{Z}_K/\Delta)^* \twoheadrightarrow P_K(\Delta)/P_{K,1}(\Delta) \cong \mathrm{Gal}(K_1/K).$$

We know from proposition (3.8) that M_l is completely split in H_4, so $(\frac{(\pi)}{K_1/K}) = e$. Hence we get that $\pi = (x + y\sqrt{-d})$ is the identity element in $P_K(\Delta)/P_{K,1}(\Delta)$, thus $x + y\sqrt{-d} \equiv \pm 1 \bmod \Delta$. Because $d \equiv -1 \bmod 8$ we see using proposition (1.1) that $4 \mid x$. We have assumed that $l > 3$, so $M_l \equiv -1 \equiv x^2 + d \cdot y^2 \bmod 32$. But since $4 \mid x$ we have

$$\begin{gathered} d \cdot y^2 \equiv -1 \bmod 16 \Rightarrow (y \cdot \sqrt{-d})^2 \equiv 1 \bmod 16 \Rightarrow \\ y \cdot \sqrt{-d} \equiv \pm 1 \bmod 8 \Rightarrow y \cdot \sqrt{-d} \equiv \pm 1 \bmod \Delta. \end{gathered}$$

Using the isomorphism $(\mathbb{Z}/8\mathbb{Z})^* \cong (\mathbb{Z}_K/(\Delta)^*$ we see that there is $\epsilon \in \{\pm 1\}$ such that $x \pm 1 \equiv \epsilon \bmod 8$. We know that $4 \mid x$, hence $8 \mid x$. This completes the proof.

To prove the main theorem we have to construct the field H_4.

Theorem 4.2 *Let $d = 2^n - 1$ be a squarefree integer with $2 \nmid n$. Let M_l be a Mersenne prime with $l \equiv 1 \bmod n$. Suppose that (x, y) is the F_d-solution of M_L then $8 \mid x$.*

Proof:
The case $n = 1$ gives $d = 1$ and by proposition (1.1) we have no solution. If we take $n = 3$ then we take $H_4 = H(\mathbb{Q}(\sqrt{-14}))$, because $\mathrm{Cl}(\mathbb{Q}(\sqrt{-14}))$ is the cyclic group with four elements, and use theorem (4.1).

Now we may assume that $n > 3$. We only need to check that we can satisfy the assumptions of theorem (4.1). From $d = 2^n - 1$ and $n > 3$ we get $d \equiv -1 \bmod 8$ and $l > 3$. And from $d = 2^n - 1$ and $2 \nmid n$ we get $d \equiv 1 \bmod 3$. The order of 2 in $(\mathbb{Z}/(2^n - 1))^*$ is n and also $2 \nmid n$ so we have $l \equiv 1 \bmod 2n$. We only need to prove that H_4 exist. We will construct H_4. First we will build up the following field diagram and calculate the relative discriminant between the fields. Our result will be:

$$
\begin{tikzcd}
 & & M \arrow[lld, dash] \arrow[ld, dash] \arrow[d, dash, "1"'] \arrow[rd, dash] \arrow[rrd, dash] & & \\
K_1 \arrow[rd, dash] & K_2 \arrow[d, dash] & JK \arrow[ld, dash, "8"] \arrow[d, dash, "1"] \arrow[rd, dash, "-d"] & J_1 \arrow[d, dash, "\alpha"] & J_2 \arrow[ld, dash, "\bar{\alpha}"] \\
 & K \arrow[rd, dash, "-d"'] & S \arrow[d, dash, "-8\cdot d"] & J \arrow[ld, dash, "8"] & \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$

With $\alpha = 1+\sqrt{2}^n$, $\bar{\alpha} = 1-\sqrt{2}^n$, $M = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\bar{\alpha}})$, $J = \mathbb{Q}(\sqrt{2})$, $S = \mathbb{Q}(\sqrt{(-d)2})$, $J_1 = J(\sqrt{\alpha})$, $J_2 = J(\sqrt{\bar{\alpha}})$, $\omega = \frac{1+\sqrt{-d}}{2}$, $\bar{\omega} = \frac{1-\sqrt{-d}}{2}$, $K = \mathbb{Q}(\omega)$, $K_1 = K(\sqrt{\omega})$ and $K_2 = K(\sqrt{\bar{\omega}})$.
Now we construct this field diagram.
Take $K = \mathbb{Q}(\omega)$, with $\omega = \frac{1+\sqrt{-d}}{2}$. This is an extension of $\mathbb{Q}$ with discriminant $-d$, cause $d \equiv 1 \bmod 4$ and d is squarefree. Now we make $K_1 = K(\sqrt{\omega})$. The norm of ω equals $\frac{d+1}{4} = 2^{n-2}$. Because 2^{n-2} is not a square we see that K_1 is a quadratic extension of K. The element $\sqrt{\omega}$ is a root of the polynomial $f(x) = x^4 - x^2 + 2^{n-2}$, hence $f(x)$ is irreducible. But also $\bar{\omega}$ is a root of $f(x)$, so K_2 is also quadratic extension of K. All the roots of $f(x)$ are in the compositum of K_1 and K_2, so $N = K_1K_2$ is Galois over $\mathbb{Q}$. We have $\sqrt{\omega} \cdot \sqrt{\bar{\omega}} = \sqrt{2} \cdot 2^{(n-3)/2}$, with $\frac{n-3}{2} \in \mathbb{N}$, cause $2 \nmid n$ and $n > 4$. So we have $J = \mathbb{Q}(\sqrt{2}) \subset N$. Therefore the compositum of J and K is contained in N and $S = \mathbb{Q}(\sqrt{(-d)2})$ is contained in N. The discriminant of J over $\mathbb{Q}$ equals 8, so we know that only 2 ramifies in J. Now take $J_1 = J(\sqrt{\alpha})$. Clearly there is a prime dividing d which ramifies in J_1, so $J \subsetneq J_1$. With the same argument we have $J \subsetneq J_2$. The compositum $M = J_1J_2$ contains $(\frac{\sqrt{\alpha}\pm\sqrt{\bar{\alpha}}}{2})^2$, which equals ω or $\bar{\omega}$. So we get $M = N$.

All fields in the picture are now constructed. Now we will calculate the relative discriminants.
The discriminant of S over $\mathbb{Q}$ equals $-d \cdot 8$. Using theorem (2.4) we find the ring of algebraic integers of JK. Then we see that $\mathbb{Z}_{JK}$ is a free module over $\mathbb{Z}_J$ and $\mathbb{Z}_K$. This gives us the relative discriminant of JK over K and the relative

discriminant of JK over J.

The field J has class number 1. The elements α and $\bar{\alpha}$ are coprime in J, because if there were not coprime then there would exist a prime π dividing both and also $1+\sqrt{2}^n+1-\sqrt{2}^n = 2$, but this can not be the case as $\gcd(2^n-1, 2) = 1$. So the ramification index of a prime of J in M is at most 2. From the polynomials $x^2 - x \pm \sqrt{2}^{n-4}$, with discriminant α (corresponding to $-$) and discriminant $\bar{\alpha}$ (corresponding to $+$), we get using theorem (2.2) that $\Delta(J_1/J) \mid 1+\sqrt{2}^n$ and $\Delta(J_2/J) \mid 1-\sqrt{2}^n$. Now we see that every prime of J which ramifies in M will do this already in JK. So we have $\Delta(M/JK) = 1$. Hence we can take $H_4 = M$. This completes the proof.

The case $n = 3$ is treated in a paper of H.W. Lenstra, Jr. and P. Stevenhagen (see [LenSte]). The proof above is a generalization of their idea, but the construction is distinct in the sense that it doesn't apply for $n = 3$. For $n = 3$ our field M will be $\mathbb{Q}(\sqrt{-1+\sqrt{2}^3}, \sqrt{-1-\sqrt{2}^3})$. If we would take that M, so $M = \mathbb{Q}(\sqrt{-1+\sqrt{2}^n}, \sqrt{-1-\sqrt{2}^n})$, then 2 will totally ramify in the corresponding J_1 of M if $n > 3$. So we could not use theorem 2.10 with the nice discriminant $1+\sqrt{2}^n$ of J_1/J.

Another possible theme for further investigation is the following. We look at Mersenne primes of the form $x^2+d\cdot y^2$. More generally one might look at primes $\frac{n^l-1}{n-1}$ of the form $x^2+d\cdot y^2$. Such a prime splits in $\mathbb{Q}(\sqrt{n})$ as $\frac{\sqrt{n}^l-1}{\sqrt{n}-1} \cdot \frac{\sqrt{n}^l+1}{\sqrt{n}+1}$. Now one can use the argument of proposition (3.8) to prove that $\frac{n^l-1}{n-1}$ splits completely in the field H_4, if such a field exists. With the same kind of arguments used in the proof of theorem (4.1) one might be able to prove that x (or y) is always in the same congruence class modulo $\Delta(\mathbb{Q}(\sqrt{n})/\mathbb{Q})$.

References

[*Beukers*]: Frits Beukers, Getaltheorie voor Beginners, Epsilon uitgave, Utrecht, 1999.
[*Cohen*]: Henri Cohen, A course in computational algebraic number theory, Springer-Verlag, 1993.
[*Cohen2*]: Henri Cohen, Advanced topics in computational number theory, Springer-Verlag, 2000.
[*Cox*]: David A. Cox, Primes of the form $x^2 + n \cdot y^2$, pure and applied mathematics, Wiley interscience, 1989.
[*FT*]: A. Fröhlich and M.J. Taylor, Algebraic number theory, Cambridge University Press, 1991.
[*Janusz*]: Gerald J. Janusz, Algebraic number theory, pure and applied mathematics (volume 55), Academic press New York and London, 1973.
[*Katz*]: Victor J. Katz, A history of mathematics (second edition), Addison-Wesley, 1998
[*Koch*]: Helmut Koch, Algebraic number theory, Springer-Verlag, 1997.
[*Lang*]: Serge Lang, Algebraic number theory (second edition), Springer-Verlag, New York, 1994.
[*LenSte*]: H.W. Lenstra Jr. and P. Stevenhagen, Artin reciprocity and Mersenne primes, 2000.
[*Stewart*]: I.N. Stewart and D.O. Tall, Algebraic number theory (second edition), Chapman and Hall/CRC, 2000.