Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 1

Introduction

Background

One of the most famous mathematical texts is the *Elements*, written by Euclid 300 B.C.. This work consist of 13 books. In Definition 22 of book VII he defines a number to be perfect if the sum of its proper divisors equals the number itself. For example 6 is a perfect number, since $1 + 2 + 3 = 6$. Also 28 is perfect because $1 + 2 + 4 + 7 + 14 = 28$. Two other perfect numbers were known to the Greeks, namely 496 and 8128. These four perfect numbers could be found using the following theorem of Euclid: for any $q \in \mathbb{Z}_{>0}$ for which $2^q - 1$ is prime, the number $2^{q-1}(2^q - 1)$ is perfect (Euler (1707–1783) proved that every even perfect number is of this form). Hence finding even perfect numbers is equivalent to finding primes of the form $2^q - 1$ with $q \in \mathbb{Z}$. The fifth perfect number was found around 1456 by someone who remains unknown. Pietro Cataldi (1552–1626) found the next two perfect numbers. He also proved that $q \in \mathbb{Z}_{>0}$ is prime if $2^q - 1$ is prime. Marin Mersenne (1588–1648) claimed that

$$\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$$

is the list of all $q \in \mathbb{Z}_{>0}$ smaller than 258 for which $2^{q-1}(2^q - 1)$ is perfect. His claim is false only because $2^{67} - 1$ and $2^{257} - 1$ are composite and $2^{61} - 1$, $2^{89} - 1$ and $2^{107} - 1$ are prime. Nowadays, nevertheless, primes of the form $2^q - 1$ with $q \in \mathbb{Z}_{>0}$ are called *Mersenne primes*. Euler proved that $2^{31} - 1$ is prime by using a corollary of one of his theorems, namely prime divisors of $2^{31} - 1$ are 1 modulo 31. Until Edouard Lucas (1842–1891) no other Mersenne primes were found. By applying his very fast test, Lucas was able to show that $2^{127} - 1$ is prime. Later, Derrick Lehmer (1905–1991) extended Lucas's test. The main problem of the present thesis derives from the Lucas-Lehmer-test, which still produces the largest known primes nowadays (see appendix).

Theorem. *Let $q \in \mathbb{Z}_{>2}$ be an integer. Define $s_i \in \mathbb{Z}/(2^q - 1)\mathbb{Z}$ for $i \in \{1, 2, \ldots, q - 1\}$ by $s_1 = 4$ and $s_{i+1} = s_i^2 - 2$. Then $2^q - 1$ is prime if and only if $s_{q-1} = 0$.*

To illustrate the Lucas-Lehmer-test we will apply the test to $q = 5$. In the ring $\mathbb{Z}/31\mathbb{Z}$ we have

$$\begin{aligned} s_1 &= 4, \\ s_2 &= 4^2 - 2 = 14, \\ s_3 &= 14^2 - 2 = 194 = 8, \\ s_4 &= 8^2 - 2 = 62 = 0. \end{aligned}$$

Since $s_4 = 0$, we conclude that 31 is a Mersenne prime. Lehmer observed: if $s_{q-1} = 0$ and q is odd then s_{q-2} is either $+2^{(q+1)/2}$ or $-2^{(q+1)/2}$ (see Proposition 5.1). The Lehmer symbol $\epsilon(4, q) \in \{+1, -1\}$ is defined for $q \in \mathbb{Z}_{>0}$ odd for which $M_q = 2^q - 1$ is prime by $s_{q-2} = \epsilon(4, q)2^{(q+1)/2}$. From the example above we read that the Lehmer symbol $\epsilon(4, 5)$ is $+1$, since $s_3 = +2^3$. We can also start the Lucas-Lehmer-test with $s_1 = 10$ instead of $s_1 = 4$. As in the case $s = 4$ the Lehmer symbol $\epsilon(10, n) \in \{+1, -1\}$ is defined for $q \in \mathbb{Z}_{>0}$ odd for which M_q is prime by $s_{q-2} = \epsilon(10, q)2^{(q+1)/2}$. The following table shows the Lehmer symbols $\epsilon(4, q)$ and $\epsilon(10, q)$ for q up to 521.

q	3	5	7	13	17	19	31	61	89	107	127	521
$\epsilon(4, q)$	+	+	−	+	−	−	+	+	−	−	+	−
$\epsilon(10, q)$	−	−	−	+	+	+	+	+	+	+	+	+

In 1996 George Woltman (1957) conjectured a relation between the table for $s = 4$ and the table for $s = 10$, namely these tables show the same sign if and only if $q \equiv 5$ or 7 modulo 8 and $q \neq 5$. Four years later S.Y. Gebre-Egziabher proved the conjecture of Woltman (see [3]). Moreover he showed that one can also start the Lucas-Lehmer-test with the rational value $s = 2/3$ and that the sign table of $s = 2/3$ is easy to write down since the sign is '+' if and only if q is 1 modulo 4 and $q \neq 5$. Of course "2/3 modulo M_q" is defined by $(2 \bmod M_q)(3 \bmod M_q)^{-1}$. In this thesis we generalize these results of Gebre-Egziabher.

Main results

Define $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$. Let $q \in \mathbb{Z}_{>1}$ and recall $M_q = 2^q - 1$. For every $s \in K$ there exists a non-zero integer k_s such that for all $q \in \mathbb{Z}_{>1}$ with $\gcd(q, k_s) = 1$ we can define a natural ring homomorphism $\mathbb{Z}[s] \to \mathbb{Z}/M_q\mathbb{Z}$ (see first paragraph of Chapter 2). This ring homomorphism allows us to use starting values of K for the Lucas-Lehmer-test. We call $s \in K$ a universal starting value if s can be used as a starting value in the Lucas-Lehmer-test for almost all prime numbers q (see Definition 2.5). The elements $4, 10$ and $2/3$ of K are examples of universal starting values. A new example of a universal starting value is $s = \frac{238}{507} + \frac{160}{169} \cdot \sqrt{2}$. Example 2.7 gives an infinite family of universal starting values. Moreover we show in Chapter 2 how one can make more families of universal starting values (see Theorem 2.9).

For every universal starting value s we can study the Lehmer symbol $\epsilon(s,q)$ (see Definition 5.2). The following theorem is the first main result of this thesis.

Theorem. *Let $s \in K$. Suppose $4-s^2$ is a square in K^*. Then there exist positive integers l and m such that $\epsilon(s,p) = \epsilon(s,q)$ if $p,q \geq l$ and $p \equiv q \bmod m$. Moreover l and m are easy to compute by Theorem 7.5.*

Gebre-Egziabher's result for the universal starting value $s = 2/3$ described above follows from this theorem. Indeed, $4-(2/3)^2$ equals $(4\sqrt{2}/3)^2 \in K^{*2}$. Other examples are Corollary 7.3, Corollary 7.6, Corollary 7.7 and Corollary 7.8. More examples can easily be made by taking a equal to b in Theorem 2.9.

Next we will describe a generalisation of Gebre-Egziabher's result on the conjecture of Woltman for related pairs of potential starting values (see Definition 8.1). An example of a related pair of potential starting values is 4 and 10. The following theorem is the second main result of this thesis.

Theorem. *Let $s,t \in K$ be a related pair of potential starting values. Suppose $(2+\sqrt{2+s})(2+\sqrt{2+t})$ is a square in $K(\sqrt{2+s},\sqrt{2-s})^*$. Then there exist positive integers l and m such that $\epsilon(s,p)\cdot\epsilon(t,p) = \epsilon(s,q)\cdot\epsilon(t,q)$ if $p,q \geq l$ and $p \equiv q \bmod m$. Moreover l and m are easy to compute by Corollary 9.4.*

Since $(2+\sqrt{2+4})(2+\sqrt{2+10})$ equals $(\sqrt[4]{2}(1+\sqrt{2}+\sqrt{3}))^2 \in K(\sqrt{6},\sqrt{-2})^{*2}$, this theorem implies Woltman's conjecture. Other examples are Corollary 9.5 and Corollary 9.6.

Let $s \in K$. If for only finitely many $q \in \mathbb{Z}_{>1}$ the Lehmer symbol $\epsilon(s,q)$ is defined, then the two theorems above trivially hold. This is the case when there are only finitely many Mersenne primes or s is a starting value for only finitely many $q \in \mathbb{Z}_{>1}$ (for example $s=5$ is not a starting value for any q). One might wonder if the two theorems above allow a converse for universal starting values if one assumes that there are infinitely many Mersenne primes. We were able to prove a weaker theorem (see two theorems below) by assuming a stronger hypothesis on Mersenne primes. We call this hypothesis the working hypothesis.

The working hypothesis roughly says that the only restrictions for Frobenius symbols of Mersenne primes in a finite Galois extension of $\mathbb{Q}$ come from abelian extensions of K. Let $L = \mathbb{Q}(\zeta_8, \sqrt[8]{5})$. The precise statement of the working hypothesis for the extension $L/\mathbb{Q}$ is: for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ with $\sigma|_{\mathbb{Q}(\zeta_8)}$ the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}))$ there are infinitely many Mersenne primes M_p such that the Frobenius symbol of M_p in the extension $L/\mathbb{Q}$ equals the conjugacy class of σ in $\mathrm{Gal}(L/\mathbb{Q})$. This statement is partly motivated by the fact that the Artin symbol of the prime ideal $(\sqrt[n]{2^p}-1)$ in the abelian extension $\mathbb{Q}(\zeta_8,\sqrt{5})/\mathbb{Q}(\sqrt{2})$ is non-trivial. There are no other conditions for the Frobenius symbol of M_p in $L/\mathbb{Q}$ that we can come up with. The following two theorems can been seen as the converses of the two main results above.

Theorem. *Let $s \in K$ be a universal starting value. Suppose $4-s^2$ is not a square in K^* and suppose that there exist positive integers l and m such that*

$\epsilon(s,p) = \epsilon(s,q)$ *if* $p,q \geq l$ *and* $p \equiv q \bmod m$. *Then the working hypothesis is false.*

Theorem. *Let* $s,t \in K$ *be a related pair of potential starting values and suppose both* s *and* t *are universal starting values. Suppose* $(2+\sqrt{2+s})(2+\sqrt{2+t})$ *is a not a square in* $K(\sqrt{2+s},\sqrt{2-s})^*$ *and suppose that there exist positive integers* l *and* m *such that* $\epsilon(s,p)\cdot\epsilon(t,p) = \epsilon(s,q)\cdot\epsilon(t,q)$ *if* $p,q \geq l$ *and* $p \equiv q \bmod m$. *Then the working hypothesis is false.*

Sketch of the proofs of the main results

Denote the Jacobi symbol by $\left(\frac{\cdot}{\cdot}\right)$ (see [1, §1, page 16]). Let $q \in \mathbb{Z}_{>1}$ and $M_q = 2^q - 1$. Let $s \in \mathbb{Z}/M_q\mathbb{Z}$. Define $s_i \in \mathbb{Z}/M_q\mathbb{Z}$ for $i \in \{1,2,\ldots,q-1\}$ by $s_1 = s$ and $s_{i+1} = s_i^2 - 2$. Then we have

$$s_{q-1} = 0 \Longleftrightarrow M_q \text{ is prime and } \left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$$

(see Theorem 2.1). In the proof of Theorem 2.1 we show that

$$s_{q-1} = 0 \Longrightarrow R = (\mathbb{Z}/M_q\mathbb{Z})[x]/(x^2 - sx + 1) \text{ is a field.}$$

From the definition of R one easily deduces the equalities

$$s_{i+1} = s_i^2 - 2 = x^{2^i} + x^{-2^i} \tag{1.1}$$

in R (see proof of Theorem 2.1). Suppose $s_{q-1} = 0$. Then the Lehmer symbol $\epsilon(s,q)$ is defined and R is a field. Equation (1.1) enables us to link the Lehmer symbol to the Frobenius automorphism $\mathrm{Frob} : x \mapsto x^{M_q}$ in an extension R' of R which contains an element y such that $y^8 = x$ (see proof of Theorem 5.6). Indeed, in R' we have

$$\epsilon(s,q)2^{\frac{q+1}{2}} = s_{q-2} = x^{2^{q-3}} + x^{-2^{q-3}} = y^{2^q} + y^{-2^q} = \mathrm{Frob}(y)y + \mathrm{Frob}(y^{-1})y^{-1}.$$

Next we study this Frobenius symbol in an extension of global fields. Let M_p be a Mersenne prime. Let $s \in K = \bigcup_{n=1}^{\infty}\mathbb{Q}(\sqrt[n]{2})$ be a universal starting value such that s is a starting value for p. Let L_s be the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}(s)$ and let $K_s = L_s \cap K = \mathbb{Q}(\sqrt[n]{2})$. Note that a zero of f_s has the same algebraic properties as the element $y \in R'$ above. The equation in R' above shows that the Frobenius symbol of the prime ideal $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$ of K_s in L_s/K_s determines the Lehmer symbol $\epsilon(s,p)$. In the case $4 - s^2 \in K^{*2}$ the extension L_s/K_s is abelian. Hence we can determine the Frobenius symbol of $\mathfrak{m}_p$ easily via the Artin map. The integers l and m of the first main result stated above can be calculated using the conductor of L_s/K_s.

Next we describe the outline of the second main result. Let M_p be a Mersenne prime. Let $s,t \in K$ be a related pair of potential starting values and suppose that both s and t are universal starting values such that both s and t

are starting values for p. Let $L_{s,t} = L_s L_t$ and let $K_{s,t} = L_{s,t} \cap K = \mathbb{Q}(\sqrt[n]{2})$. The subgroup of $\mathrm{Gal}(L_{s,t}/K_{s,t})$ generated by the Frobenius symbol of any prime ideal of $L_{s,t}$ above of the prime ideal $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$ of $K_{s,t}$ in $L_{s,t}/K_{s,t}$ determines the product of Lehmer symbols $\epsilon(s,p) \cdot \epsilon(t,p)$. In the case that $(2+\sqrt{2+s})(2+\sqrt{2+t})$ is a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$ we can study this subgroup in an abelian extension of $K_{s,t}$. We can use the Artin symbol of $\mathfrak{m}_p$ to determine the subgroup and hence the value of $\epsilon(s,p) \cdot \epsilon(t,p)$. Similarly as above the conductor of this abelian extension of $K_{s,t}$ can be used to calculate the integers l and m in the second main result described above.

Overview of the chapters

In Chapter 2 we treat the Lucas-Lehmer-test and create families of universal starting values.

In Chapter 3 we define potential starting values $s \in K$ and show that if s is a starting value for some odd positive integer q, then s is a potential starting value. Potential starting values have some properties of universal starting values but their definition does not depend on Mersenne numbers.

In Chapter 4 we construct for potential starting values $s \in K$ a Galois extension and we define a map λ_s that maps certain elements of this Galois group to a sign. This map λ_s allows us to express the Lehmer symbol in terms of the Frobenius symbol

In Chapter 5 we make a connection between the Lehmer symbol $\epsilon(s,p)$ and the Frobenius symbol via a commutative diagram with the map λ_s.

In Chapter 6 we state the sufficient properties of the Artin map and we prove a theorem to estimate conductors.

In Chapter 7 we apply the connection made in Chapter 5 and the Artin map in order to prove the first main result of this thesis.

In Chapter 8 we construct a Galois extension for a related pair of potential starting values and we define a map $\lambda'_{s,t}$ that maps certain elements of this Galois group to a sign.

In Chapter 9 we make a connection between the product of two Lehmer symbols $\epsilon(s,p) \cdot \epsilon(t,p)$ and the Frobenius symbol via a commutative diagram with the map $\lambda'_{s,t}$. We use this diagram to prove the second main result of this thesis.

In Chapter 10 we introduce the working hypothesis for abelian extension over $\mathbb{Q}$.

In Chapter 11 we state the working hypothesis and reformulate it so that it can easily be applied in the next Chapter.

In Chapter 12 we prove, assuming the working hypothesis, the converse of the two main results of this thesis.