# Mersenne primes and class field theory

Jansen, B.J.H.

# Mersenne primes and class field theory

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof.mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 18 december 2012
klokke 15:00 uur

door

Bastiaan Johannes Hendrikus Jansen
geboren te Gouda
in 1977

Samenstelling van de promotiecommissie

**Promotor**

prof.dr. H.W. Lenstra, Jr.

**Copromotor**

dr. B. de Smit

**Overige leden**

prof.dr. F. Beukers (Universiteit Utrecht)
prof.dr. S. J. Edixhoven
dr. F. Lemmermeyer (Universität Heidelberg)
prof.dr. P. Stevenhagen
prof.dr. Tijdeman

# Mersenne primes and class field theory

Bas Jansen

# Stellingen

**Stelling 1**
Zij $q$ een positief geheel getal. Laat $R_q$ de ring zijn gedefinieerd door

$$R_q = \bigcup_{\gcd(n,q)=1} \mathbb{Z}[\sqrt[n]{2}],$$

waar $n$ loopt over alle positieve gehele getallen relatief priem met $q$. Dan is er precies één ringhomomorfisme van $R_q$ naar $\mathbb{Z}/(2^q-1)\mathbb{Z}$.

**Stelling 2**
Zij $t \in \bigcup_{n\geq 1} \mathbb{Q}(\sqrt[n]{2})$. Dan is $((-54468-61952\sqrt{2})t^4+(-123904+435744\sqrt{2})t^3+(326808+371712\sqrt{2})t^2+(123904-435744\sqrt{2})t-54468-61952\sqrt{2})/(t^2+1)^2$ een universele startwaarde (zie Definition 2.5).

**Stelling 3**
Zij $q, n \in \mathbb{Z}_{>1}$, $q \equiv -1 \bmod n$ en $q > 2n-1$. Dan geldt $\left(\frac{\sqrt[n]{2}-1}{M_q}\right) = 1$ (zie Definition 2.4).

**Stelling 4**
Zij $n$ een positief geheel getal. Laat $\mathfrak{p}$ een priemideaal $\neq (0)$ zijn van $\mathbb{Z}[\sqrt[n]{2}]$ en laat $\mathfrak{P}$ een priemideaal van de ring van gehelen $\mathcal{O}$ van $\mathbb{Q}(\sqrt[n]{2})$ boven $\mathfrak{p}$ zijn. Dan is $\mathbb{Z}[\sqrt[n]{2}]/\mathfrak{p}$ isomorf met $\mathcal{O}/\mathfrak{P}$.

**Stelling 5**
Het kwadraat van 4103 kan als volgt worden bepaald.

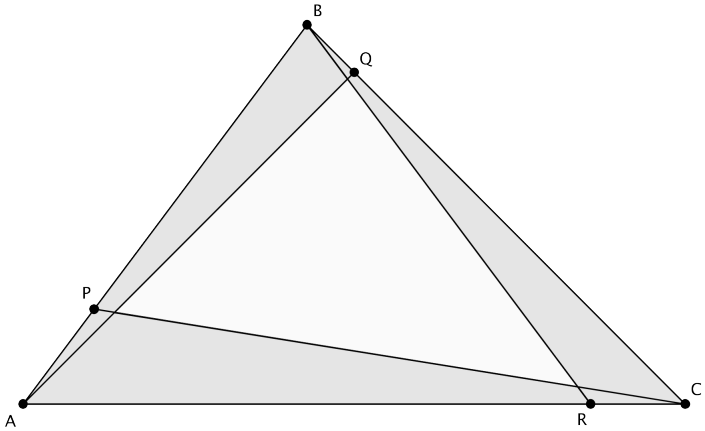
| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| I | vooraan per cijfer één punt plaatsen | . | . | . | . | 4 | 1 | 0 | 3 |
| II | een getal naar links schuiven tot het aantal | . | 4 | . | . | . | 1 | 0 | 3 |
| | punten links ervan gelijk is aan het aantal | . | 4 | . | . | 1 | 0 | . | 3 |
| | cijfers erin; dit herhalen tot het kwadraat | | | | | | | | |
| | van elk los getal eenvoudig te bepalen is | | | | | | | | |
| III | kwadrateren van de losse getallen uit II | 1 | 6 | . | 1 | 0 | 0 | . | 9 |
| IV | voor elk getal in II dat uit elkaar geschoven | | | | | | 6 | 0 | |
| | is in $x$ en $y$, het getal $2xy$ links van $y$ zetten | | | 8 | 2 | 4 | | | |
| | bv $2 \cdot 4 \cdot 103 = 824$ staat links van 103 | | | | | | | | |
| V | getallen uit III en IV optellen | 1 | 6 | 8 | 3 | 4 | 6 | 0 | 9 |

Het kwadraat van 4103 is 16834609. Deze methode werkt voor alle natuurlijke getallen.

**Stelling 6**
Zij $m \in \mathbb{Z}_{>0}$, $H_m = \{1/n \in \mathbb{Q} : n \in \mathbb{Z}_{>m}\}$ en $V$ de verzameling van alle eindige deelverzamelingen van $H_m$. Definieer de functie $f : V \to \mathbb{Q}_{>0}$ door $f : W \mapsto \sum_{x \in W} x$. Dan is voor elke $x \in \mathbb{Q}_{>0}$ het aantal elementen van $f^{-1}(x)$ oneindig.

**Stelling 7**
Als bij een constructie met passer en liniaal het tekenen van een lijn of cirkel één euro kost, dan kun je een hoek van 15 graden construeren voor vijf euro.

**Stelling 8**
De oppervlakte van een driehoek ABC met punten P, Q en R op zijden AB, BC en CA respectievelijk zodat $\frac{\text{AP}}{\text{PB}} = \frac{1}{3}$, $\frac{\text{BQ}}{\text{QC}} = \frac{1}{6}$ en $\frac{\text{CR}}{\text{RA}} = \frac{1}{7}$ is twee keer zo groot als de oppervlakte ingesloten door de lijnstukken AQ, BR en CP (zie figuur).




De oppervlakte van driehoek ABC is twee keer zo groot als de oppervlakte van de lichtgrijze driehoek in het midden.

# Abstract

Mersenne numbers are positive integers of the form $M_q = 2^q - 1$ with $q \in \mathbb{Z}_{>1}$. If a Mersenne number is prime then it is called a Mersenne prime. The Lucas-Lehmer-test is an algorithm that checks whether a Mersenne number is a prime number. The test is based on the following theorem.

**Theorem** (Lucas-Lehmer-test). *Let $q \in \mathbb{Z}_{>1}$ and 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 one has $s_{q-1} = 0$ if and only if $M_q$ is prime and the Jacobi symbols $\left(\frac{s-2}{M_q}\right)$ and $\left(\frac{-s-2}{M_q}\right)$ are both* 1.

In practice one applies the Lucas-Lehmer-test only if $q$ is a prime number, because $2^q - 1$ is composite if $q$ is composite. To apply the Lucas-Lehmer-test one chooses a value $s \in \mathbb{Z}/M_q\mathbb{Z}$ for which $\left(\frac{s-2}{M_q}\right) = \left(\frac{-s-2}{M_q}\right) = 1$ holds. Then to find out whether $M_q$ is prime, it suffices to calculate $s_{q-1}$ and verify whether it is zero.

Familiar values that one can use for $q \neq 2$ are $s = (4 \bmod M_q)$ and $s = (10 \bmod M_q)$. If $q$ is odd we can use the less familiar value $s = (2 \bmod M_q)(3 \bmod M_q)^{-1}$, which is denoted by $s = (2/3 \bmod M_q)$. Two examples of new values that can be used if $q$ is odd are

$$s = \left(\frac{626}{363} \bmod M_q\right) \text{ and } s = \left(\frac{238}{507} + \frac{160}{169}\sqrt{2} \bmod M_q\right)$$

where $(\sqrt{2} \bmod M_q)$ is defined to be $(2^{(q+1)/2} \bmod M_q)$. The condition on $q$ guarantees that $(2^{(q+1)/2} \bmod M_q)$ and the inverses of $(363 \bmod M_q)$, $(507 \bmod M_q)$ and $(169 \bmod M_q)$ are well-defined. In this thesis we will give a formula that produces infinitely many values in the field $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ that, when suitably interpreted modulo $M_q$, can be used to apply the Lucas-Lehmer-test.

Lehmer observed in the case $s_{q-1} = 0$ with $q$ odd that $s_{q-2}$ is either $+2^{(q+1)/2}$ or $-2^{(q+1)/2}$. In that case we define *the Lehmer symbol* $\epsilon(s, q) \in \{+1, -1\}$ by $s_{q-2} = \epsilon(s, q)2^{(q+1)/2}$. The main object of study in this thesis is the Lehmer symbol. At the moment the fastest way to calculate the sign $\epsilon(s, q)$ in the case $s = (4 \bmod M_q)$ for a Mersenne prime $M_q$ is to calculate the sequence $s_1, s_2, \ldots, s_{q-2}$. In 2000 however S.Y. Gebre-Egziabher showed that in the case $s = (2/3 \bmod M_q)$ and $q \neq 5$ we have $\epsilon(s, q) = 1$ if and only if

$q \equiv 1 \bmod 4$. The first main result of this thesis yields a similar result for every $s \in K$ with the property that $4 - s^2$ is a square in $K$. That includes the result of Gebre-Egziabher, since for $s = 2/3$ one has $4 - s^2 = (4\sqrt{2}/3)^2$. Another example is the following theorem.

**Theorem A.** *Let $q \in \mathbb{Z}_{>1}$ with $q \neq 2, 5$ be such that $M_q$ is prime. Let $s = (\frac{626}{363} \bmod M_q)$. Then $\epsilon(s, q) = 1$ if and only if $q \equiv 1$, 7, 9 or 13 $\bmod 20$.*

In 1996 G. Woltman conjectured that for $q \neq 2, 5$ the equation

$$\epsilon(4 \bmod M_q, q) \cdot \epsilon(10 \bmod M_q, q) = 1$$

holds if and only if $q \equiv 5$ or 7 $\bmod 8$. Woltman's conjecture was proved four years later by Gebre-Egziabher. A generalization of this theorem is the second main result of this thesis. It gives sufficient conditions for two values $s$ and $t$ in $K$ to give rise to a relation similar to Woltman's conjecture. These conditions are awkward to state, but they are similar to the conditions on $s$ in the first main result. The second main result implies the following theorem.

**Theorem B.** *Let $s = \frac{1108}{529}$ and $t = \frac{5476}{529}$. Then*

$$\epsilon(s \bmod M_q, q) \cdot \epsilon(t \bmod M_q, q) = 1 \text{ if and only if } q \equiv 3, 4, 6, 9 \text{ or } 10 \bmod 11.$$

In the proofs of both main results we express the Lehmer symbol $\epsilon(s, q)$, for $s \in K$ interpretable in the ring $\mathbb{Z}/M_q\mathbb{Z}$ in the manner suggested above, in terms of the Frobenius symbol of a Mersenne prime $2^q - 1$ in a certain number field depending *only* on $s$. Then we can use the Artin map from class field theory to control the Frobenius symbol and hence the Lehmer symbol.

It is of interest to know whether the converses of both main results hold. Thus, if $s \in K$ is such that $\epsilon(s \bmod M_q, q)$ is a "periodic" function of $q$ as in Theorem A, is $4 - s^2$ necessarily a square in $K$? This is currently beyond proof, but we will formulate a *working hypothesis* that implies an affirmative answer. Given a finite Galois extension of $\mathbb{Q}$, the working hypothesis tells us which conjugacy classes in the Galois group appear infinitely many times as the Frobenius symbol of a Mersenne prime. A strong necessary condition arises from the Artin map and the splitting behavior of Mersenne primes in the fields $\mathbb{Q}(\sqrt[n]{2})$ for $n \in \mathbb{Z}_{>0}$. The working hypothesis states that this condition is also sufficient. Restricted to abelian extensions of $\mathbb{Q}$, the working hypothesis may be reformulated as follows: for every pair of relatively prime integers $a, b \in \mathbb{Z}_{>0}$ there are infinitely many prime numbers $q$ with $q \equiv a \bmod b$ such that $2^q - 1$ is a Mersenne prime. One might view this as Dirichlet's "theorem" for Mersenne primes.

Assuming the working hypothesis, we can prove that for the value $s = 4$ there do not exist positive integers $m$ and $n$ with the property that for any $p, q \in \mathbb{Z}_{>m}$ with $M_p$ and $M_q$ prime and $p \equiv q \bmod n$ one has $\epsilon(4, p) = \epsilon(4, q)$. The same applies to any $s \in K$ for which $4 - s^2$ is not a square in $K$. We prove a similar statement for the second main result assuming the working hypothesis.

# Contents