Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 7

Periodicity

In this chapter we combine the results of the previous chapters to prove the main theorem of this thesis, that is: for a fixed well-chosen value $s \in K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ the Lehmer symbol $\epsilon(s,p)$ is "periodic in the variable p".

Main theorem for rational starting values

The first example of a starting value for which the Lehmer symbol $\epsilon(s,p)$ is periodic in p is given by the following theorem of S.Y. Gebre-Egziabher.

Theorem 7.1. *Let $p \in \mathbb{Z}_{>2}$ and let $M = 2^p - 1$ be prime. Then*

$$\epsilon(2/3, p) = 1 \Leftrightarrow p \equiv 1 \bmod 4 \quad \textit{and} \quad p \neq 5.$$

This theorem of Gebre-Egziabher follows almost immediately from Theorem 7.2 below. For this theorem we recall that $P(s)$ is the set of $p \in \mathbb{Z}_{>2}$ such that $2^p - 1$ is prime and s is a starting value for p (see just before Definition 5.2). Let $s \in \mathbb{Q}$ and write $s = \frac{c_s}{d_s}$ with $c_s, d_s \in \mathbb{Z}$ and $\gcd(c_s, d_s) = 1$. Let $r_s = \prod_{q \mid d_s} q$ where the product is taken over all prime numbers $q \neq 2$ that divide d_s. Define w_s to be the multiplicative order of $(2 \bmod r_s)$ in $(\mathbb{Z}/r_s\mathbb{Z})^*$.

Theorem 7.2. *Let $s \in \mathbb{Q}$ such that $4 - s^2$ is a square in $\mathbb{Q}(\sqrt{2})^*$. Then for all $p, q \in P(s)$ we have*

$$\epsilon(s,p) = \epsilon(s,q) \text{ if } p, q \geq 13 \text{ and } p \equiv q \bmod (2 \cdot w_s).$$

To see how Theorem 7.2 implies Theorem 7.1, take $s = \frac{2}{3}$. Then

$$4 - s^2 = 32/9 = (4\sqrt{2}/3)^2,$$

so Theorem 7.2 applies to $s = \frac{2}{3}$. We have $r_s = 3$ and $w_s = 2$. Hence by Theorem 7.2 above for all $p, q \in P(s)$ such that $p, q \geq 13$ we have $\epsilon(s,p) = \epsilon(s,q)$ if $p \equiv q \bmod 4$. After we calculate $\epsilon(2/3, p)$ for $p = 3, 5, 7, 13, 19$, Theorem 7.1 follows.

Another example that illustrates Theorem 7.2, is the following corollary. Recall the definition of bad prime of Chapter 2.

Corollary 7.3. *Let $s = \frac{626}{363}$. Then s is a universal starting value with the set of bad primes equal to $\{2\}$. Furthermore we have*

$$\epsilon(s,p) = 1 \text{ if and only if } p \equiv 1, 7, 9 \text{ or } 13 \bmod 20.$$

Proof. Let $s = \frac{626}{363}$. The elements $s-2 = 10^2 \cdot 11^{-2} \cdot -3^{-1}$ and $-s-2 = (2\sqrt{2} \cdot 13)^2 \cdot 11^{-2} \cdot -3^{-1}$ equal -3 in the multiplicative group $\mathbb{Q}(\sqrt{2})^*/\mathbb{Q}(\sqrt{2})^{*^2}$. For $u = 3, 5, 11$ and 13 the order of $(2 \bmod p)$ is even, so for odd $q \in \mathbb{Z}_{>1}$ we have $s-2, -s-2 \in (\mathbb{Z}/M_q\mathbb{Z})^*$. Hence for each odd $q \in \mathbb{Z}_{>1}$ the Jacobi symbols $\left(\frac{s-2}{M_q}\right)$ and $\left(\frac{-s-2}{M_q}\right)$ equal $\left(\frac{-3}{M_q}\right) = 1$. Therefore s is a universal starting value with bad prime 2. The element $4 - s^2 = 2^5 \cdot 5^2 \cdot 13^2 \cdot 3^{-2} \cdot 11^{-4}$ is a square in the multiplicative group $\mathbb{Q}(\sqrt{2})^*$. The denominator d_s equals $363 = 3 \cdot 11^2$, so $r_s = 33$. The order w_s of $(2 \bmod 33)$ in $(\mathbb{Z}/r_s\mathbb{Z})^*$ is 10. Hence by Theorem 7.2 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 13$ and $p \equiv q \bmod 20$. After we calculate $\epsilon(\frac{626}{363}, p)$ for $p = 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 2203$ the above corollary follows. □

Main theorem

To state the main theorem concisely we first define periodicity for Lehmer symbols. Let $s \in K$. In Chapter 5 we defined the map

$$\epsilon_s : P(s) \to \{\pm 1\}$$

by $p \mapsto \epsilon(s,p)$.

Definition 7.4. *We call a function ϵ defined on a set P of prime numbers periodic if there exist positive integers l, m such that for all $p, q \in P$ we have*

$$\epsilon(p) = \epsilon(q) \text{ if } p, q \geq l \text{ and } p \equiv q \bmod m.$$

For example if we take $s = \frac{2}{3}$ and apply Theorem 7.1 then we see that ϵ_s is periodic, since we can set $l = 6$ and $m = 4$.

Let $K_s = K \cap \mathbb{Q}(s, \sqrt{2}, \sqrt{s-2}, \sqrt{-s-2})$ (by Proposition 4.4 this definition agrees with the definition of K_s in Chapter 4). Let $\mathcal{O}_s = \mathcal{O}_{K_s}$ be the ring of integers of K_s, let $\mathfrak{d}_s = \{x \in \mathcal{O}_s : \ x \cdot s \in \mathcal{O}_s\}$ and let $n = [K_s : \mathbb{Q}]$, so that $K_s = \mathbb{Q}(\sqrt[n]{2})$. Let $\mathfrak{r}_s$ be the ideal $\prod_{\mathfrak{p} \mid \mathfrak{d}_s} \mathfrak{p}$ of $\mathcal{O}_s$ where the product is taken over all prime ideals $\mathfrak{p} \neq (\sqrt[n]{2})$ of $\mathcal{O}_s$ that divide $\mathfrak{d}_s$. Define $\omega_s = \mathrm{ord}(\sqrt[n]{2} \bmod \mathfrak{r}_s)$ to be the multiplicative order of the element $(\sqrt[n]{2} \bmod \mathfrak{r}_s)$ in $(\mathcal{O}_s/\mathfrak{r}_s)^*$.

Theorem 7.5. *Let $s \in K$ be such that $4 - s^2$ is a square in K^*. Then ϵ_s is periodic. Furthermore we can take $l = 4 \cdot n + 1$ and $m = \omega_s$ in Definition 7.4.*

For a proof of Theorem 7.5 see the next section of this chapter.

In the remainder of this section we give some corollaries of the main theorem. Recall the definition of bad prime of Chapter 2.

Corollary 7.6. *Let $s = -\frac{14}{75} + \frac{32}{25}\sqrt{2}$. Then s is a universal starting value with the set of bad primes equal to $\{2\}$. Furthermore we have*

$$\epsilon(s,p) = -1 \text{ if and only if } p \neq 3,5.$$

Proof. Note that $-3 \cdot (s-2) = (\frac{6}{5} - \frac{8}{5}\sqrt{2})^2$ and $-3 \cdot (-s-2) = (\frac{8}{5} + \frac{6}{5}\sqrt{2})^2$. Hence s is a universal starting value with bad prime 2 and in the group K^*/K^{*2} the identity $4 - s^2 = -3 \cdot (s-2) \cdot -3 \cdot (-s-2) = 1$ holds. By Theorem 7.5 we conclude that ϵ_s is periodic. Next we calculate l and m. From the identities for $-3 \cdot (s-2)$ and $-3 \cdot (-s-2)$ it follows that $K_s = \mathbb{Q}(\sqrt{2})$. This yields $n = [K_s : \mathbb{Q}] = 2$, the ideal $\mathfrak{d}_s$ equals (75) and the ideal $\mathfrak{r}_s$ equals (15). The order of $(\sqrt{2} \bmod (15))$ in $(\mathbb{Z}[\sqrt{2}]/(15))^*$ equals 8. We conclude that we can set $l = 4 \cdot n + 1 = 9$ and $m = \omega_s = 8$. Hence by Theorem 7.5 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 9$ and $p \equiv q \bmod 8$. After we calculate $\epsilon(s,p)$ for $p = 3,5,7,13,17,19,31$ the above corollary follows. □

Corollary 7.7. *Let $s = \frac{238}{507} + \frac{160}{169}\sqrt{2}$. Then s is a universal starting value with the set of bad primes equal to $\{2\}$. Furthermore we have*

$$\epsilon(s,p) = 1 \text{ if and only if } p \equiv 5 \bmod 6 \text{ and } p \neq 5.$$

Proof. Note that $-3 \cdot (s-2) = (-\frac{24}{13} + \frac{10}{13}\sqrt{2})^2$ and $-3 \cdot (-s-2) = (\frac{10}{13} + \frac{24}{13}\sqrt{2})^2$. Hence s is a universal starting value with bad prime 2 and in the group K^*/K^{*2} the identity $4 - s^2 = -3 \cdot (s-2) \cdot -3 \cdot (-s-2) = 1$ holds. By Theorem 7.5 we conclude that ϵ_s is periodic. Next we calculate l and m. From the identities for $-3 \cdot (s-2)$ and $-3 \cdot (-s-2)$ it follows that $K_s = \mathbb{Q}(\sqrt{2})$. This yields $n = [K_s : \mathbb{Q}] = 2$, the ideal $\mathfrak{d}_s$ equals (507) and the ideal $\mathfrak{r}_s$ equals (39). The order of $(\sqrt{2} \bmod (39))$ in $(\mathbb{Z}[\sqrt{2}]/(39))^*$ equals 24. We conclude that we can set $l = 4 \cdot n + 1 = 9$ and $m = \omega_s = 24$. Hence by Theorem 7.5 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 9$ and $p \equiv q \bmod 24$. After we calculate $\epsilon(s,p)$ for $p = 3,5,7,13,17,19,31,107,2281,4253,756839$ the above corollary follows. □

Corollary 7.8. *Let $s = \frac{118}{49} - \frac{800}{147}\sqrt[4]{2} - \frac{96}{49}\sqrt[4]{2}^2 + \frac{704}{147}\sqrt[4]{2}^3$. Then s is a universal starting value with the set of bad primes equal to $\{2,3\}$. Furthermore we have*

$$\epsilon(s,p) = 1 \text{ if and only if } p \equiv 5,7 \bmod 12.$$

Proof. Note that $-3 \cdot (s-2) = (\frac{18}{7} + \frac{8}{7}\sqrt[4]{2} - \frac{8}{7}\sqrt[4]{2}^2 - \frac{16}{7}\sqrt[4]{2}^3)^2$ and $-3 \cdot (-s-2) = (-\frac{16}{7} + \frac{16}{7}\sqrt[4]{2} + \frac{18}{7}\sqrt[4]{2}^2 - \frac{4}{7}\sqrt[4]{2}^3)^2$. Hence s is a universal starting value with bad primes 2 and 3, and in the group K^*/K^{*2} the identity $4 - s^2 = -3 \cdot (s-2) \cdot -3 \cdot (-s-2) = 1$ holds. By Theorem 7.5 we conclude that ϵ_s is periodic. Next we calculate l and m. From the identities for $-3 \cdot (s-2)$ and $-3 \cdot (-s-2)$ it follows that $K_s = \mathbb{Q}(\sqrt[4]{2})$. This yields $n = [K_s : \mathbb{Q}] = 4$, the ideal $\mathfrak{d}_s$ divides (147) and the ideal $\mathfrak{r}_s$ divides (21). The order of $(\sqrt[4]{2} \bmod (21))$ in $(\mathbb{Z}[\sqrt[4]{2}]/(21))^*$ equals 24. We conclude that we can set $l = 4 \cdot n + 1 = 17$ and $m = \omega_s = 24$. Hence by Theorem 7.5 the equality $\epsilon(s,p) = \epsilon(s,q)$ holds if $p, q \geq 17$ and $p \equiv q \bmod 24$. After we calculate $\epsilon(s,p)$ for $p = 5,7,13,17,19,31,61,107,2281,4253,756839$ the above corollary follows. □

Proof of the main theorem

We recall the notation of Chapters 4 and 5. Let $s \in K$ be a potential starting value, let $\alpha \in \overline{\mathbb{Q}}$ be a zero of $f_s = x^{16} - sx^8 + 1$, let L_s be the splitting field of f_s over $\mathbb{Q}(s)$ and let $n \in \mathbb{Z}_{>0}$ be such that $K_s = L_s \cap K = \mathbb{Q}(\sqrt[n]{2})$. Let $L'_s = K_s(\sqrt{4-s^2}, \alpha + \alpha^{-1})$ (by Proposition 4.1 the field L'_s is well-defined and Galois over K_s) and let G'_s be the Galois group of L'_s over K_s.

Lemma 7.9. *Let $s \in K$. Suppose $4 - s^2$ is a square in K^*. Then $4 - s^2$ is a square in K_s^*.*

Proof. Clearly $\sqrt{4-s^2} \in K^*$ and by Proposition 4.1 we have $\sqrt{4-s^2} \in L_s$, so $\sqrt{4-s^2} \in K^* \cap L_s = K_s^*$. Hence $4 - s^2$ is a square in K_s^*. □

Proof of Theorem 7.5. If $P(s) \subset \{2\}$ then the theorem follows immediately. Suppose $P(s) \not\subset \{2\}$. Then $P(s)$ contains an odd prime. By Theorem 3.2 the value s is a potential starting value. Lemma 7.9 yields $4 - s^2 \in (K_s^*)^2$. Hence K'_s, defined by $K'_s = K_s(\sqrt{4-s^2})$, equals the field K_s, so by Proposition 4.3 the group G'_s is cyclic of order 8.

Next we describe a modulus for L'_s/K_s. Let $\mathfrak{f}$ be the conductor of L'_s/K_s. Write $\mathfrak{f}$ as the product $(\sqrt[n]{2})^i \cdot \mathfrak{f}_{\text{odd}}$ where $i \in \mathbb{Z}_{\geq 0}$ and $\mathfrak{f}_{\text{odd}}$ is not divisible by the prime $(\sqrt[n]{2})$. By Proposition 5.9 we know that all primes $\neq (\sqrt[n]{2})$ that ramify in L'_s/K_s divide $\mathfrak{d}_s$ and hence $\mathfrak{r}_s$. By Theorem 6.3 and $[L'_s : K_s] = 8$, the ideal $\mathfrak{f}_{\text{odd}}$ equals the product of the primes $\neq (\sqrt[n]{2})$ that ramify in L'_s/K_s. Hence $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{r}_s$. By Corollary 6.4 we have $i \leq 4n + 1$. Hence $\mathfrak{m} = (\sqrt[n]{2})^{4n+1} \cdot \mathfrak{r}_s$ is a modulus for L'_s/K_s.

Suppose $p, q \in P(s)$ satisfy $p \equiv q \bmod \omega_s$ and $p, q \geq 4n+1$. Let $m_p = \sqrt[n]{2}^p - 1$ and let $m_q = \sqrt[n]{2}^q - 1$. By definition ω_s is the order of $\sqrt[n]{2}$ in $(\mathcal{O}_s/\mathfrak{r}_s)^*$, so $p \equiv q \bmod \omega_s$ implies $m_p \equiv m_q \bmod \mathfrak{r}_s$. The assumption $p, q \geq 4n + 1$ implies $m_p \equiv m_q \bmod (\sqrt[n]{2})^{4n+1}$. Hence we have $m_p \equiv m_q \bmod \mathfrak{m}$. Let $x = m_p \cdot m_q^{-1}$. The ideal $\mathfrak{m}$ is a modulus for L'_s/K_s, so $\text{ord}_{\mathfrak{p}}(x-1) \geq \text{ord}_{\mathfrak{p}}(\mathfrak{f})$ for all prime ideals $\mathfrak{p} \mid \mathfrak{f}$. The field K_s has two real embeddings, namely σ defined by $\sigma(\sqrt[n]{2}) = \sqrt[n]{2}$ and τ defined by $\tau(\sqrt[n]{2}) = -\sqrt[n]{2}$. Since both p and q are odd, we see that $\sigma(x) > 0$ and $\tau(x) > 0$, i.e. x is totally positive in L'_s/K_s. Now conditions (i) and (ii) of Theorem 6.1 are satisfied, therefore we conclude that the ideal (x) is in the kernel of the Artin map. Hence $((x), L'_s/K_s)$ is the trivial element of G'_s, so $((m_p), L'_s/K_s) = ((m_q), L'_s/K_s)$. By Corollary 5.7 it follows that $\epsilon_s(p) = \epsilon_s(q)$. □

Proof of Theorem 7.2. Let $s \in \mathbb{Q}$ be such that $4 - s^2$ is a square in $\mathbb{Q}(\sqrt{2})^*$. By Proposition 4.4 we have $n = [K_s : \mathbb{Q}(s)] = 2$. From Theorem 7.5 it follows that ϵ_s is periodic. Since $s \in \mathbb{Q}$, we have $\mathfrak{d}_s = (d_s)$, the ideal $\mathfrak{r}_s$ equals (r_s) and hence ω_s divides $2 \cdot w_s$. Hence we can take $l \geq 4 \cdot 2 + 1 = 9$ and $m = \omega_s = 2 \cdot w_s$. Since $p, q \in P(s)$ and $p, q \geq 9$ imply $p, q \geq 13$, we set $l = 13$. □