Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 12

Lehmer's question

In the second edition of Richard Guy's book "Unsolved Problems in Number Theory" one can read in section A3 a question of D.H. Lehmer, namely: what is $\epsilon_4(p)$? In this chapter we prove assuming the working hypothesis Mer $= W$ that $\epsilon_4(p)$ is non-periodic.

Converse of the main theorems

In the following table we see the Lehmer symbol $\epsilon_4(p)$ for the first 25 odd p such that $2^p - 1$ is a Mersenne prime.

p	$\epsilon_4(p)$	mod 3	mod 5	mod 7	mod 9	mod 11	mod 13
3	+	0	3	3	3	3	3
5	+	2	0	5	5	5	5
7	−	1	2	0	7	7	7
13	+	1	3	6	4	2	0
17	−	2	2	3	8	6	4
19	−	1	4	5	1	8	6
31	+	1	1	3	4	9	5
61	+	1	1	5	7	6	9
89	−	2	4	5	8	1	11
107	−	2	2	2	8	8	3
127	+	1	2	1	1	6	10
521	−	2	1	3	8	4	1
607	−	1	2	5	4	2	9
1279	−	1	4	5	1	3	5
2203	+	1	3	5	7	3	6
2281	−	1	1	6	4	4	6
3217	−	1	2	4	4	5	6
4253	+	2	3	4	5	7	2
4423	−	1	3	6	4	1	3
9689	−	2	4	1	5	9	4

p	$\epsilon_4(p)$	mod 3	mod 5	mod 7	mod 9	mod 11	mod 13
9941	+	2	1	1	5	8	9
11213	−	2	3	6	8	4	7
19937	+	2	2	1	2	5	8
21701	−	2	1	1	2	9	4
23209	+	1	4	4	7	10	4

If the working hypothesis is true then one cannot find patterns between the column with the signs and the modulo-columns. We state this more precisely in the following theorem.

Theorem 12.1. *If ϵ_4 is periodic, then* Mer *is not W.*

Theorem 12.1 implies that if one proves that ϵ_4 is periodic, then one has new knowledge about the Frobenius symbols of Mersenne primes.

We will prove the following generalization of Theorem 12.1 in the next section. This Theorem can been seen as the converse of Theorem 7.5.

Theorem 12.2. *Let $s \in K$ be a universal starting value. If ϵ_s is periodic and $4 - s^2 \notin K^{*2}$, then* Mer *is not W.*

We get the following similar result for a related pair of potential starting values. This result can been seen as the converse of Corollary 9.4.

Theorem 12.3. *Let $s, t \in K$ be a related pair of potential starting values and suppose both s and t are universal starting values. If $\epsilon_{s,t}$ is periodic and $(2 + \sqrt{2+s})(2+\sqrt{2+t})$ is not a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$, then* Mer *is not W.*

We prove Theorem 12.3 in the next section.

Lehmer's question and the working hypothesis

In this section we prove Theorem 12.1, Theorem 12.2 and Theorem 12.3.

Proof of Theorem 12.2. Let $s \in K$ be a universal starting value. Theorem 3.2 implies that s is a potential starting value. Assume that $4 - s^2 \notin K^{*2}$. Then Proposition 4.3 implies that the Galois group of the extension L'_s/K_s is isomorphic to the dihedral group D_8 of 16 elements. Let $E = K_s(\sqrt{4-s^2}, \sqrt{s+2}) \subset L'_s$. Since s is a potential starting value and $4 - s^2 \notin K^{*2}$, we have $[E : K_s] = 4$. The commutator subgroup of D_8 has 4 elements and $[E : K_s] = 4$, so E is the maximal abelian extension of K_s in L'_s. By assumption ϵ_s is periodic. Let $l \in \mathbb{Z}_{>0}$ and $m \in \mathbb{Z}_{>0}$ be as in Definition 7.4. Define $\zeta = \zeta_{2^m-1} \in \overline{\mathbb{Q}}$ to be a primitive $(2^m - 1)$-th root of unity. Let L be the Galois closure of $L'_s(\zeta)$ over $\mathbb{Q}$. Let $n = [L \cap K : \mathbb{Q}]$, so that $L \cap K = \mathbb{Q}(\sqrt[n]{2})$. By definition $K_s = L'_s \cap K$. Therefore $L'_s \cap \mathbb{Q}(\sqrt[n]{2})$ equals K_s. Hence the restriction map $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism. Therefore $E\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $L'_s\mathbb{Q}(\sqrt[n]{2})$.

We denote the maximal abelian extension of $L \cap K$ in L by L^{ab}. Since $E\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $L'_s\mathbb{Q}(\sqrt[n]{2})$, the field $E\mathbb{Q}(\sqrt[n]{2})$ is a subfield of L^{ab} and $L^{\mathrm{ab}} \cap L'_s\mathbb{Q}(\sqrt[n]{2})$ equals $E\mathbb{Q}(\sqrt[n]{2})$. Clearly $\mathbb{Q}(\zeta)$ is a subfield of L^{ab}. In the following diagram we see an overview of the fields, four Galois groups and three group elements used in this proof.

$$\begin{tikzcd}
 & & L \arrow[dl, dash] \arrow[d, dash] & L \arrow[d, dash, "\sigma_1 \neq \sigma_2, \sigma_2^{-1}"] \\
 & L'_s\mathbb{Q}(\sqrt[n]{2})) \arrow[dl, dash] \arrow[d, dash, "C_4"] & L^{\mathrm{ab}} \arrow[dl, dash] \arrow[d, dash] & L^{\mathrm{ab}} \arrow[dd, dash, "\sigma_1 = \sigma_2"] \\
L'_s \arrow[d, dash, "C_4"'] & E\mathbb{Q}(\sqrt[n]{2}) \arrow[dl, dash] \arrow[d, dash, "V_4"] & \mathbb{Q}(\sqrt[n]{2}, \zeta) \arrow[dl, dash] \arrow[d, dash] & \\
E \arrow[d, dash, "V_4"'] & \mathbb{Q}(\sqrt[n]{2}) \arrow[dl, dash] & \mathbb{Q}(\zeta) \arrow[ddll, dash] & \mathbb{Q}(\zeta) \arrow[ddd, dash] \\
K_s \arrow[d, dash] & & & \\
K_s \cap \mathbb{Q}(\zeta) \arrow[d, dash] & & & \\
\mathbb{Q} & & & \mathbb{Q}
\end{tikzcd}$$

Next we recall the definition of T_L. Denote the conductor of L^{ab} over $\mathbb{Q}(\sqrt[n]{2})$ by $\mathfrak{f}$. Write $\mathfrak{f} = (\sqrt[n]{2})^{\mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})} \cdot \mathfrak{f}_{\mathrm{odd}}$. Denote the multiplicative order of $\sqrt[n]{2}$ modulo $\mathfrak{f}_{\mathrm{odd}}$ in the group $(\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}/\mathfrak{f}_{\mathrm{odd}})^*$ by k. The map $\tau : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ is defined by $u \mapsto ((\sqrt[n]{2}^x - 1), L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$, where $x \in \mathbb{Z}$ is such that $x \equiv u \bmod k$ and $x \geq \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})$. Let $r : \mathrm{Gal}(L/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ be the restriction map. We recall $T_L = r^{-1}(\text{image of } \tau)$.

Suppose for a contradiction the working hypothesis $\mathrm{Mer} = W$. Since the restriction map $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism, Proposition 4.3 and Proposition 5.10(iv) imply that for any $\sigma \in T_L$ the element $\sigma|_{L'_s\mathbb{Q}(\sqrt[n]{2})}$ generates the cyclic group $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2}, \sqrt{4-s^2}))$ of order 8 . Since $L^{\mathrm{ab}} \cap L'_s\mathbb{Q}(\sqrt[n]{2})$ equals $E\mathbb{Q}(\sqrt[n]{2})$, there exist $\sigma_1, \sigma_2 \in T_L$ such that $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$ and $\sigma_1|_{L'_s\mathbb{Q}(\sqrt[n]{2})} \neq (\sigma_2|_{L'_s\mathbb{Q}(\sqrt[n]{2})})^{\pm 1}$. Since $\sigma_1|_{L'_s\mathbb{Q}(\sqrt[n]{2})} \neq (\sigma_2|_{L'_s\mathbb{Q}(\sqrt[n]{2})})^{\pm 1}$ and the restriction map $\mathrm{Gal}(L'_s\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism, we have $\sigma_1|_{L'_s} \neq (\sigma_2|_{L'_s})^{\pm 1}$. Hence Definition 4.6 and Definition 4.5 imply $\lambda'_s([\sigma_1|_{L'_s}]) \neq \lambda'_s([\sigma_2|_{L'_s}])$.

Let $\sigma_1, \sigma_2 \in T_L$ be as above. Then Theorem 11.7(i), applied to the extension $L/\mathbb{Q}(\sqrt[n]{2})$, implies that there exist $p, q \in \mathbb{Z}_{>l}$ with $\gcd(pq, n) = 1$ such that $\sigma_1 = (\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))$ and $\sigma_2 = (\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))$, and both ideals $\mathfrak{M}_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$ and $\mathfrak{M}_q \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^q - 1)$ are prime ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}$. Since $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$, we have $(\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)} = (\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)}$. The extension $\mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})$ is abelian, so $((\sqrt[n]{2}^p - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})) = ((\sqrt[n]{2}^q - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2}))$. Since the prime ideals $(\sqrt[n]{2}^p - 1)$ and $(\sqrt[n]{2}^q - 1)$ are of degree 1 over $\mathbb{Q}$, we have $((2^p - 1), \mathbb{Q}(\zeta)/\mathbb{Q}) = ((2^q - 1), \mathbb{Q}(\zeta)/\mathbb{Q})$. This implies $2^p - 1 \equiv 2^q - 1 \bmod (2^m - 1)$, so $p \equiv q \bmod m$. By construction $p, q > l$ and by assumption ϵ_s is periodic, so $\epsilon_s(p) = \epsilon_s(q)$. The consistency property implies

$[\sigma_1|_{L'_s}] = (\mathfrak{M}_p \cap L'_s, L'_s/K_s)$ and $[\sigma_2|_{L'_s}] = (\mathfrak{M}_q \cap L'_s, L'_s/K_s)$. Recall the definition of Frob' above Corollary 5.7. Now we see that $\mathrm{Frob}'(p) = (\mathfrak{M}_p \cap L'_s, L'_s/K_s)$ and $\mathrm{Frob}'(q) = (\mathfrak{M}_q \cap L'_s, L'_s/K_s)$. Therefore we have $(\lambda'_s \circ \mathrm{Frob}')(p) \neq (\lambda'_s \circ \mathrm{Frob}')(q)$. Now Corollary 5.7 implies $\epsilon_s(p) \neq \epsilon_s(q)$. This is a contradiction. Hence $\mathrm{Mer} \neq W$. $\square$

Proof of Theorem 12.1. Note that $4 - 4^2 = -12$ is not a square in K^*. Now Theorem 12.2 implies Theorem 12.1. $\square$

The ideas of the proof of Theorem 12.2 can also be applied to pairs of universal starting values. To illustrate this we give the following proof. The following proof is similar to the proof of Theorem 12.2.

Proof of Theorem 12.3. Let $s, t \in K$ be a related pair of potential starting values. We will recall from Chapter 8 the definition of the fields $K_{s,t}$, E', E'', E and F. Recall $f_s = x^{16} - sx^8 + 1$, the element $\alpha = \alpha_s \in \overline{\mathbb{Q}}$ a zero of f_s and L_s the splitting field of f_s over $\mathbb{Q}(s)$. Recall $K_{s,t} = (L_s L_t) \cap K$ and $F_s = K_{s,t}(\sqrt{4 - s^2}, \alpha_s + \alpha_s^{-1})$. Finally we recall $F = F_s F_t$, the field $E = F_s \cap F_t$, the field $E' = K_{s,t}(\sqrt{4 - s^2})$ and $E'' = E'(\sqrt{s+2})$. By assumption $e'' = (2 + \sqrt{2+s})(2 + \sqrt{2+t})$ is not a square in E''^*, so Lemma 9.13 implies $[E : E'] \neq 4$ or 8. Therefore Lemma 8.16 implies $[E : E'] = 2$. Denote the maximal abelian extension of $K_{s,t}$ in F by D. Let T be as in Proposition 8.9. Then D equals TE''.

By assumption $\epsilon_{s,t}$ is periodic. Let $l \in \mathbb{Z}_{>0}$ and $m \in \mathbb{Z}_{>0}$ be as in Definition 7.4. Define $\zeta = \zeta_{2^m - 1} \in \overline{\mathbb{Q}}$ to be a primitive $(2^m - 1)$-th root of unity. Let L be the Galois closure of $F(\zeta)$ over $\mathbb{Q}$. Let $n = [L \cap K : \mathbb{Q}]$, so that $L \cap K = \mathbb{Q}(\sqrt[n]{2})$. By definition $K_{s,t} = F \cap K$. Therefore $F \cap \mathbb{Q}(\sqrt[n]{2})$ equals $K_{s,t}$. Hence the restriction map $\mathrm{Gal}(F\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(F/K_{s,t})$ is an isomorphism. Therefore $D\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $F\mathbb{Q}(\sqrt[n]{2})$.

We denote the maximal abelian extension of $L \cap K$ in L by L^{ab}. Since $D\mathbb{Q}(\sqrt[n]{2})$ is the maximal abelian extension of $\mathbb{Q}(\sqrt[n]{2})$ in $F\mathbb{Q}(\sqrt[n]{2})$, the field $D\mathbb{Q}(\sqrt[n]{2})$ is a subfield of L^{ab} and $L^{\mathrm{ab}} \cap F\mathbb{Q}(\sqrt[n]{2})$ equals $D\mathbb{Q}(\sqrt[n]{2})$. Clearly $\mathbb{Q}(\zeta)$ is a subfield of L^{ab}. In the following diagram we see an overview of the fields used in this proof.

$$\begin{tikzcd}
 & & L \arrow[d, dash] \\
 & F\mathbb{Q}(\sqrt[n]{2})) \arrow[ur, dash] & L^{\mathrm{ab}} \\
F \arrow[ur, dash] & D\mathbb{Q}(\sqrt[n]{2}) \arrow[u, dash] \arrow[ur, dash] & \mathbb{Q}(\sqrt[n]{2}, \zeta) \arrow[u, dash] \\
D = TE'' \arrow[u, dash] \arrow[ur, dash] & \mathbb{Q}(\sqrt[n]{2}) \arrow[u, dash] \arrow[ur, dash] & \mathbb{Q}(\zeta) \arrow[u, dash] \\
K_{s,t} \arrow[u, dash] \arrow[ur, dash] & & \\
K_{s,t} \cap \mathbb{Q}(\zeta) \arrow[u, dash] \arrow[uurr, dash] & & \\
\mathbb{Q} \arrow[u, dash] & &
\end{tikzcd}$$

Next we recall the definition of T_L. Denote the conductor of L^{ab} over $\mathbb{Q}(\sqrt[n]{2})$ by $\mathfrak{f}$. Write $\mathfrak{f} = (\sqrt[n]{2})^{\mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})} \cdot \mathfrak{f}_{\mathrm{odd}}$. Denote the multiplicative order of $\sqrt[n]{2}$ modulo $\mathfrak{f}_{\mathrm{odd}}$ in the group $(\mathcal{O}_{\mathbb{Q}(\sqrt[n]{2})}/\mathfrak{f}_{\mathrm{odd}})^*$ by k. The map $\tau : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ is defined by $u \mapsto ((\sqrt[n]{2}^x - 1), L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$, where $x \in \mathbb{Z}$ is such that $x \equiv u \bmod k$ and $x \geq \mathrm{ord}_{\sqrt[n]{2}}(\mathfrak{f})$. Let $r : \mathrm{Gal}(L/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(L^{\mathrm{ab}}/\mathbb{Q}(\sqrt[n]{2}))$ be the restriction map. We recall $T_L = r^{-1}(\text{image of } \tau)$.

Suppose for a contradiction the working hypothesis Mer $= W$. Since the restriction map $\mathrm{Gal}(F\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}(\sqrt[n]{2})) \to \mathrm{Gal}(F/K_{s,t})$ is an isomorphism, Proposition 9.8 and the consistency property imply that for any $\sigma \in T_L$ the conjugacy class $[\sigma|_F]$ is an element of $\mathrm{Gal}(F/E')^{\mathrm{gen}}/{\sim}$. Since $[E : E'] = 2$, Theorem 8.10 implies that the map $\lambda'_{s,t} : \mathrm{Gal}(F/E')^{\mathrm{gen}}/{\sim} \to \{\pm 1\}$ does not factor via the restriction map $\mathrm{Gal}(F/E')^{\mathrm{gen}}/{\sim} \to \mathrm{Gal}(T/K_{s,t})$. Hence $L^{\mathrm{ab}} \cap F\mathbb{Q}(\sqrt[n]{2}) = D\mathbb{Q}(\sqrt[n]{2}) = (TE'')\mathbb{Q}(\sqrt[n]{2})$ implies that there exist $\sigma_1, \sigma_2 \in T_L$ such that $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$ and $\lambda'_{s,t}([\sigma_1|_F]) \neq \lambda'_{s,t}([\sigma_2|_F])$.

Let $\sigma_1, \sigma_2 \in T_L$ be as above. Then by Theorem 11.7(i) (applied to the extension $L/\mathbb{Q}(\sqrt[n]{2})$) there exist $p, q \in \mathbb{Z}_{>l}$ with $\gcd(pq, n) = 1$ such that $\sigma_1 = (\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))$ and $\sigma_2 = (\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))$, and $\mathfrak{M}_p \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^p - 1)$ and $\mathfrak{M}_q \cap \mathbb{Q}(\sqrt[n]{2}) = (\sqrt[n]{2}^q - 1)$ both prime ideals of $\mathbb{Q}(\sqrt[n]{2})$. Since $\sigma_1|_{L^{\mathrm{ab}}} = \sigma_2|_{L^{\mathrm{ab}}}$, the Frobenius symbol $(\mathfrak{M}_p, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)}$ equals $(\mathfrak{M}_q, L/\mathbb{Q}(\sqrt[n]{2}))|_{\mathbb{Q}(\sqrt[n]{2},\zeta)}$. The extension $\mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})$ is abelian, so $((\sqrt[n]{2}^p - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2})) = ((\sqrt[n]{2}^q - 1), \mathbb{Q}(\sqrt[n]{2}, \zeta)/\mathbb{Q}(\sqrt[n]{2}))$. Since the prime ideals $(\sqrt[n]{2}^p - 1)$ and $(\sqrt[n]{2}^q - 1)$ are of degree 1 over $\mathbb{Q}$, we have $((2^p - 1), \mathbb{Q}(\zeta)/\mathbb{Q}) = ((2^q - 1), \mathbb{Q}(\zeta)/\mathbb{Q})$. This implies $2^p - 1 \equiv 2^q - 1 \bmod (2^m - 1)$, so $p \equiv q \bmod m$. By construction we have $\lambda'_{s,t}([\sigma_1|_F]) \neq \lambda'_{s,t}([\sigma_2|_F])$. The consistency property implies $[\sigma_1|_F] = (\mathfrak{M}_p \cap F, F/K_{s,t})$ and $[\sigma_2|_F] = (\mathfrak{M}_q \cap F, F/K_{s,t})$. Recall the definition of Frob_2 above Corollary 9.10. Now we see that $\mathrm{Frob}_2(p) = (\mathfrak{M}_p \cap F, F/K_{s,t})$ and $\mathrm{Frob}_2(q) = (\mathfrak{M}_q \cap F, F/K_{s,t})$. Therefore we have $(\lambda'_{s,t} \circ \mathrm{Frob}_2)(p) \neq (\lambda'_{s,t} \circ \mathrm{Frob}_2)(q)$. Now Corollary 9.10 implies $\epsilon_{s,t}(p) \neq \epsilon_{s,t}(q)$. This is a contradiction. Hence Mer $\neq W$. $\square$