Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 9

Relating Lehmer symbols

In this chapter we show that for certain well-chosen related pairs of potential starting values $s, t \in K$ (see Definition 8.1) the product of the corresponding Lehmer symbols $\epsilon(s,p)$ and $\epsilon(t,p)$ is "periodic in the variable p". Below we make this precise.

Woltman's conjecture

The following theorem, proved by S.Y. Gebre-Egziabher in 2000, was first stated in 1996 by G. Woltman as a conjecture (see [8, Chapter 2, §4]).

Theorem 9.1. *Let $p \in \mathbb{Z}_{>2}$ and suppose that $M = 2^p - 1$ is prime. Then*

$$\epsilon(4,p) \cdot \epsilon(10,p) = 1 \Leftrightarrow p \equiv 5 \text{ or } 7 \mod 8 \quad \text{and} \quad p \neq 5.$$

A proof of Theorem 9.1 can be found at the end of this section.

In this chapter we generalize Theorem 9.1. To state this generalization concisely we will use the definition of periodic functions (see Definition 7.4). Let $s, t \in K$. In Chapter 5 we defined the map $\epsilon_s : P(s) \to \{\pm 1\}$ by $p \mapsto \epsilon(s,p)$. This map yields a map $\epsilon_{s,t} : P(s) \cap P(t) \to \{\pm 1\}$ defined by $p \mapsto \epsilon(s,p) \cdot \epsilon(t,p)$. For well-chosen values of s and t the map $\epsilon_{s,t}$ is periodic. If we take $s = 4$ and $t = 10$, and apply Theorem 9.1, then we see that $\epsilon_{s,t}$ is periodic, since we can take $l = 5$ and $m = 8$ (see Definition 7.4).

Next we state a first version of the main theorem of this chapter. First we recall some notation of Chapters 4 and 8. Let $s, t \in K$ be a related pair of potential starting values. Define L_s as the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}(s)$. Let $K_{s,t} = (L_s L_t) \cap K$, let $E' = K_{s,t}(\sqrt{4 - s^2})$, let $F_s = E'(\alpha_s + \alpha_s^{-1})$ and let $E = F_s \cap F_t$. Note that Lemma 8.16 implies $[E : E'] = 2, 4$ or 8.

Proposition 9.2. *Let s, t be a related pair of potential starting values. Then $\epsilon_{s,t}$ is periodic if $[E : E']$ equals 4 or 8. Moreover if $[E : E']$ equals 8, then $\epsilon_{s,t}$ is a constant function.*

We prove Proposition 9.2 in the last section of this chapter.

Suppose $[E : E'] = 8$. Then Proposition 9.2 implies that we can set $l = 0$ and $m = 1$ in Definition 7.4. Next we state a theorem on the possible values for l and m in Definition 7.4 in the case $[E : E'] = 4$.

Let $s, t \in K$ be a related pair of potential starting values. Let T be as in Proposition 8.9. Proposition 8.9 implies $[T : K_{s,t}] \leq 2$. Let $n = [K_{s,t} : \mathbb{Q}]$, so that $K_{s,t}$ equals $\mathbb{Q}(\sqrt[n]{2})$. Denote a modulus for $T/K_{s,t}$ by $\mathfrak{t}$. Write $\mathfrak{t}_{\text{odd}}$ for the odd part of $\mathfrak{t}$, i.e. $\mathfrak{t} = \mathfrak{t}_{\text{odd}} \cdot (\sqrt[n]{2})^i$ for some $i \in \mathbb{Z}_{\geq 0}$ and $(\sqrt[n]{2}) \nmid \mathfrak{t}_{\text{odd}}$. Let $\mathcal{O}_{K_{s,t}}$ be the ring of integers of $K_{s,t}$. Write ω for the order of $(\sqrt[n]{2} \bmod \mathfrak{t}_{\text{odd}})$ in $(\mathcal{O}_{K_{s,t}}/\mathfrak{t}_{\text{odd}})^*$.

Theorem 9.3. *Let $s, t \in K$ be a related pair of potential starting values. Suppose $[E : E'] = 4$ or 8. Then $\epsilon_{s,t}$ is periodic and we can set $l = 2n + 1$ and $m = \omega$ in Definition 7.4. Moreover we have $n \mid 4 \cdot [\mathbb{Q}(s, t) : \mathbb{Q}]$.*

For a proof of Theorem 9.3 see the last section of this chapter.

To verify if the conditions of Theorem 9.3 hold, one has to do some computations. Moreover to find a suitable m one also has to do computations. Next we state a corollary of Theorem 9.3 that makes these computations easier.

Let s, t be a related pair of potential starting values. Set $d = [\mathbb{Q}(s, t) : \mathbb{Q}]$. Let $\mathfrak{d}_s = \{x \in \mathbb{Z}[\sqrt[d]{2}] : x \cdot s \in \mathbb{Z}[\sqrt[d]{2}]\}$ be the denominator ideal of s. Similarly we define $\mathfrak{d}_t$. Let $\mathfrak{d} = \mathfrak{d}_{s,t} = \mathfrak{d}_s\mathfrak{d}_t$, which is an ideal of $\mathbb{Z}[\sqrt[d]{2}]$. Let $\mathfrak{e}$ be the product of all prime ideals $\mathfrak{p}$ of $\mathbb{Z}[\sqrt[d]{2}]$ for which $\text{ord}_{\mathfrak{p}}(4 - s^2)$ is odd. Let $\mathfrak{r} = \mathfrak{r}_{s,t}$ be the product of all prime ideals $\mathfrak{p} \neq (\sqrt[d]{2})$ of $\mathbb{Z}[\sqrt[d]{2}]$ which divide $\mathfrak{d}\mathfrak{e}$. Define $w_{s,t} = \text{ord}(\sqrt[d]{2} \bmod \mathfrak{r})$ to be the multiplicative order of $(\sqrt[d]{2} \bmod \mathfrak{r})$ in $(\mathbb{Z}[\sqrt[d]{2}]/\mathfrak{r})^*$.

Corollary 9.4. *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 $\epsilon_{s,t}$ is periodic and we can take $l = 8 \cdot d + 1$ and $m = 4 \cdot w_{s,t}$ in Definition 7.4. If in addition to the assumptions above*

$$\left(2 + \sqrt{2 + \sqrt{2 + s}}\right)\left(2 + \sqrt{2 + \sqrt{2 + t}}\right)$$

is a square in $K(\sqrt{2 + s}, \sqrt{2 - s}, \sqrt{2 + \sqrt{2 + s}})^*$, then $\epsilon_{s,t}$ is constant.

We prove Corollary 9.4 in the last section of this chapter.

Now we state two more examples of a periodic $\epsilon_{s,t}$. The starting values in these examples are universal starting values. Only the starting value in the first corollary has a bad prime (see just below Definition 2.5), which is 11.

Corollary 9.5. *Let $s = \frac{1108}{529}$ and let $t = \frac{5476}{529}$. Then both s and t are universal starting values, each with the set of bad primes equal to $\{11\}$. Furthermore for all $p \in P(s) \cap P(t)$ we have*

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

Corollary 9.6. *Let $s = \frac{1492}{121}$ and let $t = \frac{1924}{121}$. Then both s and t are universal starting values with no bad primes. Furthermore for all $p \in P(s) \cap P(t)$ we have*

$$\epsilon(s, p) \cdot \epsilon(t, p) = -1.$$

In the last section of this chapter we prove these two corollaries.

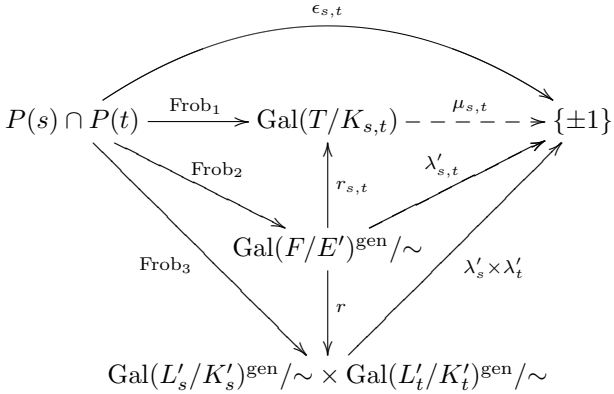
Proof of Woltman's Conjecture. Let $s = 4$ and $t = 10$. We recall from the first section of Chapter 8 that s, t is a related pair of potential starting values. Note the following idenity

$$(2 + \sqrt{2+4})(2 + \sqrt{2+10}) = (\sqrt[4]{2}(1 + \sqrt{2} + \sqrt{3}))^2 \in K(\sqrt{6}, \sqrt{-2})^{*^2}.$$

Now Corollary 9.4 implies that $\epsilon_{s,t}$ is periodic. Clearly we have $d = 1$, $\mathfrak{d} = (1)$ and $\mathfrak{e} = (3)$. Therefore we have $\mathfrak{r} = 3$. The multiplicative order $w_{s,t}$ of (2 mod $\mathfrak{r}$) is 2. Hence by Corollary 9.4 we can set $l = 8 \cdot d + 1 = 9$ and $m = 4 \cdot w_{s,t} = 8$ in Definition 7.4. After calculating $\epsilon_{s,t}(p)$ for $p = 3, 5, 7, 13, 17, 19$ and 31 Theorem 9.1 follows. □

Relating Lehmer symbols via Frobenius symbols

In this section we relate a product of Lehmer symbols with a Frobenius symbol. We start with recalling (from Chapter 8) and defining the maps in the diagram below.



Let $s, t \in K$ be a related pair of potential starting values. By Proposition 8.2 both s and t are potential starting values. Recall the definition $\epsilon_{s,t}$ from the first section of this chapter. Let T be as in Proposition 8.9. The maps $r_{s,t}$, $\lambda'_{s,t}$ and $r_s : \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim \to \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim$ are defined in the second section of Chapter 8. The map $\mu_{s,t}$ exists if and only if $[E : E'] = 4$ or 8 (see Theorem 8.10). We define the map r in the diagram above by $r : [\sigma] \mapsto (r_s([\sigma]), r_t([\sigma]))$. From Definition 4.6 of Chapter 4 we recall the map $\lambda'_s : \mathrm{Gal}(L'_s/K'_s)^{\mathrm{gen}}/\sim \to \{\pm 1\}$. Define the map $\lambda'_s \times \lambda'_t$ in the diagram above by $\lambda'_s \times \lambda'_t : ([\sigma], [\tau]) \mapsto \lambda'_s([\sigma]) \cdot \lambda'_t([\tau])$. The following proposition will be used to define the maps Frob_1, Frob_2 and Frob_3.

Proposition 9.7. *Let $s, t \in K$, take $p \in P(s) \cap P(t)$ and set $n = [K_{s,t} : \mathbb{Q}]$. Then $(\sqrt[n]{2}^p - 1)$ is a prime ideal of $\mathcal{O}_{K_{s,T}}$ of degree one over $\mathbb{Q}$ unramified in F.*

We prove this proposition at the end of this section.

Next we define the three remaining maps in the diagram above, namely the Frobenius maps Frob_1, Frob_2 and Frob_3. Let $n = [K_{s,t} : \mathbb{Q}]$. We define the map Frob_1 by $\text{Frob}_1 : p \mapsto ((\sqrt[n]{2}^p - 1), T/K_{s,t})$. Note that by Proposition 9.7 this map is well-defined.

Proposition 9.8. *Let $s, t \in K$ be a related pair of potential starting values and let $n = [K_{s,t} : \mathbb{Q}]$. Suppose $p \in P(s) \cap P(t)$. Then $((\sqrt[n]{2}^p - 1), F/K_{s,t})$ is an element of $\text{Gal}(F/E')^{\text{gen}}/\sim$.*

We prove Proposition 9.8 at the end of this section. Define the map Frob_2 by $\text{Frob}_2 : p \mapsto ((\sqrt[n]{2}^p - 1), F/K_{s,t})$. Let $n_s = [K_s : \mathbb{Q}]$ and let $n_t = [K_t : \mathbb{Q}]$. Define the map Frob_3 by

$$\text{Frob}_3 : p \mapsto (((\sqrt[n_s]{2}^p - 1), L'_s/K_s), ((\sqrt[n_t]{2}^p - 1), L'_t/K_t)).$$

Note that by Proposition 9.7 these two maps are well-defined.

Theorem 9.9. *Let $s, t \in K$ be a related pair of potential starting values. Then the diagram without $\mu_{s,t}$ above commutes. Moreover if $[E : E']$ equals 4 or 8, then the entire diagram exists and commutes.*

A proof of Theorem 9.9 can be found at the end of this section. The following corollary, which follows directly from Theorem 9.9, can be seen as an analog of Corollary 5.7.

Corollary 9.10. *Let $s, t \in K$ be a related pair of potential starting values. Then the diagram*

$$\begin{array}{ccc} P(s) \cap P(t) & \xrightarrow{\epsilon_{s,t}} & \{+1, -1\} \\ & \searrow^{\text{Frob}_2} & \uparrow \lambda'_{s,t} \\ & & \text{Gal}(F/E')^{\text{gen}}/\sim \end{array}$$

commutes.

To prove that ϵ_s is periodic if $[K'_s : K_s]$ equals 1, we used the fact that the Frobenius map in Corollary 5.7 becomes the Artin map if the Galois group $\text{Gal}(L'_s/K_s)$ is abelian. We cannot apply this method to $\epsilon_{s,t}$ with Corollary 9.10, since the Galois group $\text{Gal}(F/K_{s,t})$ is not abelian. However we can use the following corollary, which follows directly from Theorem 9.9, to prove that $\epsilon_{s,t}$ is periodic if $[E : E']$ equals 4 or 8.

Corollary 9.11. *Let $s, t \in K$ be a related pair of potential starting values. Suppose $[E : E']$ equals 4 or 8. Then the diagram*

$$\begin{array}{ccc} P(s) \cap P(t) & \xrightarrow{\epsilon_{s,t}} & \{+1, -1\} \\ & \searrow^{\text{Frob}_1} & \uparrow \mu_{s,t} \\ & & \text{Gal}(T/K_{s,t}) \end{array}$$

commutes.

Proof of Proposition 9.7. Let $p \in P(s) \cap P(t)$. Then Proposition 5.10(ii) implies $p \nmid [K_s : \mathbb{Q}]$ and $p \nmid [K_t : \mathbb{Q}]$. By Proposition 8.3 we have $[K_{s,t} : \mathbb{Q}(s,t)] \mid 4$. Since p is odd, the inclusions $\mathbb{Q}(s,t) \subset K_s K_t \subset K_{s,t}$ imply $p \nmid [K_{s,t} : \mathbb{Q}] = n$. Since $2 \mid n$, the absolute norm of $\sqrt[n]{2}^p - 1$ equals $-(2^p - 1)$. By definition of $P(s)$ the integer $2^p - 1$ is a prime number, so the ideal $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$ is a prime ideal of degree 1 over $\mathbb{Q}$.

By Proposition 5.10(ii) the prime ideal $\mathfrak{m}_p \cap K_s$ of K_s is unramified in L_s. This implies that $\mathfrak{m}_p$ is unramified in $L_s K_{s,t}$ (see [7, Chapter II, §4]). Similarly we derive that $\mathfrak{m}_p$ is unramified in $L_t K_{s,t}$. We recall $K_{s,t} = (L_s L_t) \cap K$, so $K_{s,t} \subset L_s L_t$. Hence $\mathfrak{m}_p$ is unramified in $F \subset L_s L_t$ (see [7, Chapter II, §4]). □

Proof of Proposition 9.8. Let $p \in P(s) \cap P(t)$ and let $\mathfrak{m}_p = (\sqrt[n]{2}^p - 1)$. By Proposition 9.7 the ideal $\mathfrak{m}_p$ is a prime ideal of degree 1 over $\mathbb{Q}$. Let $\mathfrak{m}'_p = \mathfrak{m}_p \cap K_s$. The consistency property implies $(\mathfrak{m}_p, F_s/K_{s,t})|L_s = (\mathfrak{m}'_p, L_s/K_s)$. We recall the notation $K'_s = K_s(\sqrt{4 - s^2})$. Further we recall from Proposition 5.10(iv) that every element of the conjugacy class $(\mathfrak{m}'_p, L_s/'K_s)$ generates the group $\mathrm{Gal}(L'_s/K'_s)$. By Proposition 8.4 the restriction map $\mathrm{Gal}(F_s/K_{s,t}) \to \mathrm{Gal}(L'_s/K_s)$ is an isomorphism. Since K'_s is a subfield of $E' = K_{s,t}(\sqrt{4 - s^2})$, the restriction map $\mathrm{Gal}(F_s/E') \to \mathrm{Gal}(L'_s/K'_s)$ is an isomorphism. Hence every element of the conjugacy class $(\mathfrak{m}_p, F_s/K_{s,t})$ generates the group $\mathrm{Gal}(F_s/E')$. Similarly for t we get: every element of the conjugacy class $(\mathfrak{m}_p, F_t/K_{s,t})$ generates the group $\mathrm{Gal}(F_t/E')$. Hence by Proposition 8.6 we have $(\mathfrak{m}_p, F/K_{s,t}) \in \mathrm{Gal}(F/E')^{\mathrm{gen}}/\sim$. □

Proof of Theorem 9.9. Suppose $s, t \in K$ is a related pair of potential starting values. Then the maps Frob_1, Frob_2, $\mu_{s,t}$, $\lambda'_{s,t}$ and $r_{s,t}$ are defined. By Proposition 8.2 both s and t are potential starting values. Hence also the maps Frob_3, r and $\lambda'_s \times \lambda'_t$ are defined. The identity $\lambda'_{s,t} = (\lambda'_s \times \lambda'_t) \circ r$ follows directly from the definition of $\lambda'_{s,t}$ (see Definition 8.7). The identities $\mathrm{Frob}_3 = r \circ \mathrm{Frob}_2$ and $\mathrm{Frob}_1 = r_{s,t} \circ \mathrm{Frob}_2$ follow from the consistency property (see Proposition 5.4). The identity $\epsilon_{s,t} = (\lambda'_s \times \lambda'_t) \circ \mathrm{Frob}_3$ follows from Corollary 5.7 and the definitions of the maps $\epsilon_{s,t}$ and $\lambda'_s \times \lambda'_t$. From the identities that we just proved we get

$$\epsilon_{s,t} = (\lambda'_s \times \lambda'_t) \circ \mathrm{Frob}_3 = (\lambda'_s \times \lambda'_t) \circ (r \circ \mathrm{Frob}_2) = ((\lambda'_s \times \lambda'_t) \circ r) \circ \mathrm{Frob}_2 = \lambda'_{s,t} \circ \mathrm{Frob}_2.$$

Hence $\epsilon_{s,t}$ equals $\lambda'_{s,t} \circ \mathrm{Frob}_2$. This proves the first part of Theorem 9.9. Now assume $[E : E'] = 4$ or 8. From Theorem 8.10 we get $\lambda'_{s,t} = \mu_{s,t} \circ r_{s,t}$. From the identities that we proved so far we get

$$\epsilon_{s,t} = \lambda'_{s,t} \circ \mathrm{Frob}_2 = (\mu_{s,t} \circ r_{s,t}) \circ \mathrm{Frob}_2 = \mu_{s,t} \circ (r_{s,t} \circ \mathrm{Frob}_2) = \mu_{s,t} \circ \mathrm{Frob}_1.$$

Hence $\epsilon_{s,t}$ equals $\mu_{s,t} \circ \mathrm{Frob}_1$. □

Proofs

In this section we prove Proposition 9.2, Theorem 9.3, Corollary 9.4, Corollary 9.5 and Corollary 9.6.

We recall some notation from the first section of Chapter 9. Let $s, t \in K$ be a related pair of potential starting values. Let T be as in Proposition 8.9. Let $n = [K_{s,t} : \mathbb{Q}]$. Denote a modulus for $T/K_{s,t}$ by $\mathfrak{t}$. Write $\mathfrak{t} = \mathfrak{t}_{\text{odd}} \cdot (\sqrt[n]{2})^i$ for some $i \in \mathbb{Z}_{\geq 0}$ and $(\sqrt[n]{2}) \nmid \mathfrak{t}_{\text{odd}}$. Let $\mathcal{O}_{K_{s,t}}$ be the ring of integers of $K_{s,t}$. Write ω for the order of $(\sqrt[n]{2} \bmod \mathfrak{t}_{\text{odd}})$ in $(\mathcal{O}_{K_{s,t}}/\mathfrak{t}_{\text{odd}})^*$.

Proof of Theorem 9.3. Let $\mathfrak{f}$ be the conductor of $T/K_{s,t}$. Write $\mathfrak{f}$ as the product $(\sqrt[n]{2})^j \cdot \mathfrak{f}_{\text{odd}}$ where $j \in \mathbb{Z}_{\geq 0}$ and $\mathfrak{f}_{\text{odd}}$ is not divisible by the prime $(\sqrt[n]{2})$. By Theorem 6.3 we have $(\sqrt[n]{2})^j \mid 2 \cdot 2 \cdot \sqrt[n]{2}$. Hence $\mathfrak{m} = (\sqrt[n]{2})^{2n+1} \cdot \mathfrak{f}_{\text{odd}}$ is a modulus for $T/K_{s,t}$.

Suppose $p, q \in P(s) \cap P(t)$ satisfy $p \equiv q \bmod \omega$ and $p, q \geq 2n+1$. Let $m_p = \sqrt[n]{2}^p - 1$ and let $m_q = \sqrt[n]{2}^q - 1$. By definition ω is the order of $\sqrt[n]{2}$ in $(\mathcal{O}_{K_{s,t}}/\mathfrak{t}_{\text{odd}})^*$, so $p \equiv q \bmod \omega$ implies $m_p \equiv m_q \bmod \mathfrak{t}_{\text{odd}}$. Note that $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{t}_{\text{odd}}$, so $p \equiv q \bmod \omega$ implies $m_p \equiv m_q \bmod \mathfrak{f}_{\text{odd}}$. The assumption $p, q \geq 2n+1$ implies $m_p \equiv m_q \bmod (\sqrt[n]{2})^{2n+1}$. 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 T/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 $K_{s,t}$ 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. the element x is totally positive in $T/K_{s,t}$. 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 $((x), T/K_{s,t})$ is the trivial element of $\text{Gal}(T/K_{s,t})$, so $((m_p), T/K_{s,t})$ equals $((m_q), T/K_{s,t})$. Therefore the definition of Frob_1 implies $\text{Frob}_1(p) = \text{Frob}_1(q)$. Note that the assumptions of Theorem 9.3 are the same as the assumptions of Corollary 9.11. By Corollary 9.11 it follows that $\epsilon_{s,t}(p)$ equals $\epsilon_{s,t}(q)$. By Proposition 8.3 we have $n \leq 4 \cdot [\mathbb{Q}(s,t) : \mathbb{Q}]$. □

Proof of Proposition 9.2. The first part of Proposition 9.2 follows directly from Theorem 9.3. Since $[E : E'] = 8$, Proposition 8.8 implies that $\lambda'_{s,t}$ is not surjective. Hence from Corollary 9.10 the map $\epsilon_{s,t}$ is constant. □

Let $s, t \in K$ be a related pair of potential starting values. Recall $E' = K_{s,t}(\sqrt{4-s^2})$ and $E'' = E'(\sqrt{2+s})$. Define $e'' = (2+\sqrt{2+s})(2+\sqrt{2+t})$, $E''' = E''(\sqrt{2+\sqrt{2+s}})$ and

$$e = \left(2+\sqrt{2+\sqrt{2+s}}\right)\left(2+\sqrt{2+\sqrt{2+t}}\right).$$

Lemma 9.12. *Assume e'' is a square in $(E''K)^*$. Then e'' is a square in E''^*. Moreover if e'' and e are squares in $(E''K)^*$ and $(E'''K)^*$ respectively, then e is a square in E'''^*.*

Proof. By assumption e'' is a square in $(E''K)^*$. Proposition 4.11 implies that e'' is a square in $(L_sL_t)^*$. Hence e'' is a square in $(E''K)^* \cap (L_sL_t)^* = E''^*$. By assumption e is a square in $(E'''K)^*$. Proposition 4.11 implies that e is a square in $(L_sL_t)^*$. Hence e is a square in $(E'''K)^* \cap (L_sL_t)^* = E'''^*$. □

Lemma 9.13. *The element e'' is a square in E''^* if and only if $[E : E']$ equals 4 or 8. Moreover if e'' and e are squares in E''^* and E'''^* respectively, then $[E : E']$ equals 8.*

Proof. Lemma 8.16 implies $[E : E'] = 2, 4$ or 8. Suppose e'' is a square in E''^*. Then Proposition 4.11 implies $[E : E'] = 4$ or 8. If e is also a square in E'''^*, then Proposition 4.11 yields $[E : E'] = 8$. Suppose e'' is not a square in E''^*. Then Proposition 4.11 and Kummer theory imply $[E : E'] = 2$. □

Recall the definition of $\mathfrak{f}_{\text{odd}}$ (see proof of Theorem 9.3) and $\mathfrak{r}$ (see just above Corollary 9.4).

Proposition 9.14. *Let s, t be a pair of potential starting values. Then $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{r}$.*

Proof. Recall the definition of $\mathfrak{d}_s$, $\mathfrak{d}_t$ and $\mathfrak{e}$. Proposition 5.9 implies that if a prime ideal $\mathfrak{p} \neq (\sqrt[n]{2})$ of the ring of integers of $K_{s,t}$ ramifies in $K_{s,t}L_s$, then $\mathfrak{p}$ divides $\mathfrak{d}_s\mathfrak{e}$ (see [7, Chapter II, §5]). We get a similar result for $K_{s,t}L_t/K_{s,t}$. Hence if a prime ideal $\mathfrak{p} \neq (\sqrt[n]{2})$ of the ring of integers of $K_{s,t}$ ramifies in L_sL_t, then $\mathfrak{p}$ divides $\mathfrak{d}_s\mathfrak{d}_t\mathfrak{e} = \mathfrak{d}_{s,t}\mathfrak{e}$. From the definition of F we get $F \subset L_sL_t$. By Proposition 8.6 we have $[F : K_{s,t}] \mid 64$. Hence only the prime $(\sqrt[n]{2})$ is wildly ramified in $F/K_{s,t}$. Therefore Theorem 6.8 implies $\mathfrak{f}_{\text{odd}} \mid \mathfrak{r}$. □

Proof of Corollary 9.4. Let $s, t \in K$ be a related pair of potential starting values. Assume that $(2+\sqrt{2+s})(2+\sqrt{2+t})$ is a square in $K(\sqrt{2+s}, \sqrt{2-s})^*$. Then Lemma 9.12 and Lemma 9.13 imply $[E : E'] = 4$ or 8. Hence Theorem 9.3 implies that $\epsilon_{s,t}$ is periodic. From Theorem 9.3 it follows that $l = 2n+1 \leq 2 \cdot 4 \cdot [\mathbb{Q}(s,t) : \mathbb{Q}] + 1 = 8 \cdot d + 1$. By Proposition 9.14 the ideal $\mathfrak{f}_{\text{odd}}$ divides $\mathfrak{r}$. By Proposition 8.3 we have $n/d = 1, 2$ or 4. Therefore the multiplicative order of $(\sqrt[n]{2} \bmod \mathfrak{f}_{\text{odd}})$ divides four times the multiplicative order of $(\sqrt[d]{2} \bmod \mathfrak{r})$. Hence by Theorem 9.3 we can set $m = 4 \cdot w_{s,t}$. Suppose the extra assumption of Corollary 9.4 holds. Then Lemma 9.12 and Lemma 9.13 imply $[E : E'] = 8$. Hence by Proposition 9.2 the function $\epsilon_{s,t}$ is constant. □

Proof of Corollary 9.6. Taking the variable of Example 2.7 equal to $-\frac{2}{3}\sqrt{2}$ and $-\frac{1}{6}\sqrt{2}$ yields $s = \frac{1492}{121}$ and $t = \frac{1924}{121}$ respectively. Let α_s be a zero of $f_s = x^{16} - sx^8 + 1$. We recall $L_s = \mathbb{Q}(\zeta_8, \alpha_s)$ is the splitting field of $f_s = x^{16} - sx^8 + 1$ over $\mathbb{Q}$. By equations 4.2 and 4.3 of the proof of Proposition 4.8 we can write $\alpha_s^4 = \frac{\sqrt{s-2}+\sqrt{s+2}}{2}$. From the two equalities below Example 2.7 it follows that $s-2, t-2 \in \mathbb{Q}(\sqrt{2})^{*2}$ and $s+2, t+2 \in 3 \cdot \mathbb{Q}(\sqrt{2})^{*2}$. Hence we have $\mathbb{Q}(\zeta_8, \alpha_s^4) = \mathbb{Q}(\zeta_8, \alpha_t^4)$. Note that in the field $\mathbb{Q}(\zeta_8, \alpha_s^4)$ we have

$$\alpha_s^4 \cdot \alpha_t^4 = \frac{1}{4}\Big(\frac{25}{11}\sqrt{2} + \frac{17}{11}\sqrt{6}\Big)\Big(\frac{29}{11}\sqrt{2} + \frac{19}{11}\sqrt{6}\Big) = 7 + 4\sqrt{3} = \Big(\frac{1}{\sqrt{2}}(1+\sqrt{3})\Big)^4.$$

Hence by Kummer theory the fields L_s and L_t are the same. By Theorem 5.6 it follows that $\epsilon_{s,t}$ is constant.

Next we show $\epsilon_{s,t}(p) = \epsilon(s,p) \cdot \epsilon(t,p) = -1$. Note that we have $s_{3-2} = s_1 = \frac{1492}{121} \equiv \frac{1}{2} \equiv -3 \equiv 2^{(3+1)/2} \bmod 7$, so $\epsilon_s(3)$ equals 1. Note that we have $t_{3-2} = t_1 = \frac{1924}{121} \equiv \frac{-1}{2} \equiv 3 \equiv -2^{(3+1)/2} \bmod 7$, so $\epsilon_t(3)$ equals -1. Hence $\epsilon_{s,t}(3)$ equals -1. Since $\epsilon_{s,t}$ is constant, we have $\epsilon_{s,t}(p) = \epsilon(s,p) \cdot \epsilon(t,p) = -1$. □

Let $s = \frac{1108}{529}$ and $t = \frac{5476}{529}$. The next table will be used in the proof of Corollary 9.5.

p	$\epsilon_s(p)$	$\epsilon_t(p)$	$\epsilon_{s,t}(p)$	$p \bmod 11$
3	+	+	+	3
5	+	−	−	5
7	−	+	−	7
13	−	+	−	2
17	−	−	+	6
19	−	+	−	8
31	−	−	+	9
61	−	−	+	6
89	+	−	−	1
107	+	−	−	8
127	−	−	+	6
521	+	+	+	4
607	−	+	−	2
1279	+	+	+	3
2203	−	−	+	3
2281	−	−	+	4
3217	−	+	−	5
4253	−	+	−	7
4423	−	+	−	1
9689	−	−	+	9
9941	+	−	−	8
11213	−	−	+	4
19937	−	+	−	5
21701	+	+	+	9
23209	−	−	+	10

Proof of Corollary 9.5. Taking the variable of Example 2.7 equal to $\frac{2}{7}\sqrt{2}$ and $-\frac{1}{8}\sqrt{2}$ yields $s = \frac{1108}{529}$ and $t = \frac{5476}{529}$ respectively. From the first equality below Example 2.7 it follows that both $s-2$ and $t-2$ are squares in $\mathbb{Q}(\sqrt{2})^*$. From the second equality below Example 2.7 it follows that both $-s-2$ and $-t-2$ can be written as -3 times a square of $\mathbb{Q}(\sqrt{2})^*$. Hence $K(\sqrt{2+s}, \sqrt{2-s})$ equals $K(\sqrt{3}, \sqrt{-1})$. Moreover neither $4-s^2$ nor $4-t^2$ is a square in K^*, and $(4-s^2)(4-t^2)$ and $(s+2)(t+2)$ are squares in K^* and $K(\sqrt{4-s^2})^*$ respectively. Definition 8.1 implies that s, t is a related pair of potential starting values.

Note the relation $(2+\sqrt{2+s})\cdot(2+\sqrt{2+t}) = \frac{1}{23^2}(46+19\sqrt{6})\cdot(46+33\sqrt{6}) = \frac{1}{23^2}\left((2+\sqrt{6})(2\sqrt{2}+\sqrt{3})^2\right)\cdot\left((2+\sqrt{6})(5\sqrt{2}-\sqrt{3})^2\right) \in K(\sqrt{3},\sqrt{-1})^{*2}$. By Corollary 9.4 it follows that $\epsilon_{s,t}$ is periodic.

Next we calculate possible l and m as in Definition 7.4. In this and the next three paragraphs we show that $K_{s,t} = \mathbb{Q}(\sqrt{2})$. Recall that $L_s = \mathbb{Q}(\zeta_8, \alpha_s)$, $K_s = L_s \cap K$ and $K_s'' = K_s(\sqrt{s-2}, \sqrt{-s-2})$. We want to apply Proposition 3.7 to the extensions $K_s \subset K_s'' \subset L_s$. First we show that the assumptions of Proposition 3.7 hold. By Proposition 8.2 we get s is a potential starting value. Proposition 4.4 implies $K_s'' = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and $K_s = \mathbb{Q}(\sqrt{2})$. From Proposition 4.2 we get $\mathrm{Gal}(L_s/K_s'')$ is cyclic of order 8. Clearly K_s''/K_s is Galois and $\mathrm{i} \in L_s$. Now Proposition 3.7 implies $L_s \cap K = K_s'' \cap K = \mathbb{Q}(\sqrt{2})$. Hence we have $\sqrt[4]{2} \notin L_s$. Similarly we get $\sqrt[4]{2} \notin L_t$.

We recall $K_s' = K_s(\sqrt{4-s^2})$ and $L_s' = K_s'(\alpha_s + \alpha_s^{-1})$. Since $s-2 \in K_s^{*2}$, we have $K_s' = K_s''$. Proposition 4.2 implies $L_s = L_s'$. Similarly we have $L_t = L_t'$. Hence $K_{s,t}$ equals $(L_s'L_t') \cap K$, so we have $F = L_s'L_t'$.

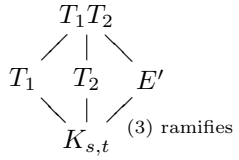
Suppose for a contradiction $L_s' = L_t'$. Then the fields $F_s = L_s'K_{s,t}$ and $F_t = L_t'K_{s,t}$ are equal. Now Proposition 9.2 implies that $\epsilon_{s,t}$ is constant. This contradicts the table above, so we conclude that $L_s' \neq L_t'$.

Proposition 4.11 and the relation $(2+\sqrt{2+s})\cdot(2+\sqrt{2+t}) \in K_s'(\sqrt{2+s})^{*2} = K_t'(\sqrt{2+t})^{*2}$ imply $[F : L_s' \cap L_t'] = 1$ or 4. From $L_s' \neq L_t'$ we get $[F : L_s' \cap L_t'] = 4$. Suppose for a contradiction that $\sqrt[4]{2} \in F$. Then the three intermediate fields of the extension $F/(L_s' \cap L_t')$ are L_s', L_t' and $(L_s' \cap L_t')(\sqrt[4]{2})$. Therefore we have $L_s'(\sqrt[4]{2}) = F = L_t'(\sqrt[4]{2})$. The assumption $\sqrt[4]{2} \in F$ implies $\sqrt[4]{2} \in K_{s,t} = F \cap K$. By definition of F_s and F_t we have $\sqrt[4]{2} \in K_{s,t} \subset F_s$ and $\sqrt[4]{2} \in K_{s,t} \subset F_t$. Therefore we have $F_s = L_s'(\sqrt[4]{2})$ and $F_t = L_t'(\sqrt[4]{2})$, so $F_s = F = F_t$. Now Proposition 9.2 implies that $\epsilon_{s,t}$ is constant. This contradicts the table above, so we conclude that $\sqrt[4]{2} \notin F$. Hence we have $K_{s,t} = F \cap K = \mathbb{Q}(\sqrt{2})$.

By Theorem 9.3 we can set $l = 2 \cdot [K_{s,t} : \mathbb{Q}] + 1 = 5$. In the next three paragraphs we will calculate a possible m.

Recall the notation just above Corollary 9.4. Clearly we have $\mathfrak{d} = (529)^2 = (23)^4$ and $529^2 \cdot (4 - s^2) = 4 \cdot 529^2 - 1108^2 = -(2^2 \cdot 3 \cdot 5^2 \cdot 19^2)$. Therefore $\mathfrak{e}$ equals (3), so that $\mathfrak{r}$ equals $(3)\cdot(23)$.

Note that Lemma 9.13 implies $[E : E'] = 4$ or 8. The table above shows that $\epsilon_{s,t}$ is surjective. Hence by Proposition 9.2 the degree $[E : E']$ equals 4. By Proposition 8.9 and Proposition 8.18 there are 4 different extensions T such that $[T : K_{s,t}] = 2$, the intersection $T \cap E'' = K_{s,t}$ and $T \subset F$. We can choose two, T_1 and T_2, such that T_1T_2 contains the field $E' = K_{s,t}(\sqrt{4-s^2}) = K_{s,t}(\sqrt{-3})$.



Note that (3) is inert in the extension $K_{s,t}/\mathbb{Q}$. Since 3 does not divide

$[L_sL_t : \mathbb{Q}]$, Proposition 5.8(vi) implies that $V_{(3),1}$ is the trivial group. Hence by Proposition 5.8(v) the group $V_{(3),0}$ is cyclic. Note that the prime ideal (3) ramifies in $E'/K_{s,t}$. Since $V_{(3),0}$ is cyclic, the prime ideal (3) cannot ramify in both extensions $T_i/K_{s,t}$ with $i \in \{1, 2\}$. Hence we can choose a field T_i such that (3) does not divide the conductor of $T_i/K_{s,t}$. By Proposition 9.14 we have $\mathfrak{f}_{\text{odd}} \mid \mathfrak{r}$. Since $\mathfrak{r}$ equals $3 \cdot 23$, we can conclude that $\mathfrak{f}_{\text{odd}}$ divides 23. Therefore $\mathfrak{t} = (23)$ is a modulus for $T_i/K_{s,t}$. Note that $\sqrt{2}^{22} \equiv 1 \bmod 23$, so the order ω of $(\sqrt{2} \bmod 23)$ is 22. Now Theorem 9.3 (and the definition of m) implies $m \mid 22$. Since p is odd, we see that we can set $m = 11$.

The table above shows the signs for s and t. This proves Corollary 9.5. □