CONGRUENCE FUNCTION FIELDS WITH CLASS NUMBER ONE

MARTHA RZEDOWSKI–CALDERÓN AND GABRIEL VILLA–SALVADOR

To the memory of Prof. Manohar L. Madan

ABSTRACT. We prove that there exists, up to isomorphism, exactly one function field over the finite field of two elements of class number one and genus four. This result, together with the ones of MacRae, Madan, Leitzel, Queen and Stirpe, establishes that there exist eight non-isomorphic congruence function fields of genus larger than zero and class number one.

1. Introduction

Let $K$ be a congruence function field with exact field of constants $\mathbb{F}_q$, the finite field of $q$ elements. Consider the class group of divisors of degree zero of $K$: $\text{Cl}_0(K)$. It is a finite abelian group with $h_K$ elements, $h_K$ is called the class number of $K$. When $K$ is a function field of genus 0, we have $h_K = 1$. Thus, we consider $K$ of genus $g_K \geq 1$. When $q \geq 5$ and $g_K \geq 1$ we have $h_K > 1$. In [2] R. MacRae found all the congruence function fields with class number one in the particular case that $K$ is a quadratic extension of the rational function field $k = \mathbb{F}_q(T)$ and $K$ contains a prime divisor of degree one. He proved that there are four quadratic fields with class number one which have a prime of degree one. M. Madan and C. Queen continued the study of this problem in [3]. They showed that if $q = 2$ and $g_K > 4$, or $q = 3$ and $g_K > 2$ then $h_K \neq 1$. Finally, they proved that except for the case $q = 2$ and $g_K = 4$ there exist exactly seven congruence function fields with class number one and genus larger than zero. The case $q = 2$, $g_K = 4$ was not settled.

In [1] J. Leitzel, M. Madan and C. Queen considered the case $q = 2$ and $g_K = 4$ and claimed that there is no field of class number one over the finite field of two elements and genus four. However C. Stirpe [5] found a counterexample to this claim. The example runs as follows. Let $\mathfrak{m}$ be the place associated to the irreducible polynomial $T^4 + T + 1 \in \mathbb{F}_2[T]$ and let $S$ be the place associated to the irreducible polynomial $T^7 + T^4 + 1$. Let $K_S^\infty$ be the ray class field of conductor $\mathfrak{m}$ and such that $S$ splits in $K_S^\infty/\mathbb{F}_2(T)$. Stirpe established that the subfield of degree five over $\mathbb{F}_2(T)$ satisfies that $h_K = 1$ and $g_K = 4$. Furthermore, Stirpe claims that $T^7 + T^4 + 1$ is not unique. For instance, he remarks that we may take $S_1$ to be the place associated to $T^7 + T^3 + 1$ and the unique subfield $K_1$ of $K_{S_1}^\infty$ of degree five over $\mathbb{F}_2(T)$ also satisfies that $h_{K_1} = 1$ and $g_{K_1} = 4$.

In [6], P. Mercuri and C. Stirpe proved that the two fields found by Stirpe in [5] are in fact isomorphic. Furthermore, they show that, up to isomorphism, there
is only one field of genus 4 and class number one. This result together with the 
results of Madan, Leitzel, Queen and Stirpe, shows that, up to isomorphism, there 
are exactly eight congruence function fields $K$ of genus larger than zero and class 
number one.

In this paper we present another proof that, up to isomorphism, there is only 
one field of genus four and class number one. We do not use the examples found by 
Stirpe in [5]. Our approach uses the theory of cyclotomic function fields of Carlitz– 
Hayes. First, we consider a field $K$ over $\mathbb{F}_2$ such that $h_K = 1$ and $g_K = 4$. We show 
that $K$ has a unique rational function subfield $k := \mathbb{F}_2(T)$ such that $[K : k] = 5$ and 
that the extension $K/k$ is cyclic. There is only one prime of $k$ ramified in $K$ and 
this place is of degree four. From the result of Madan and Queen [3] that states 
that a function field $K$ over $\mathbb{F}_2$ satisfies that $h_K = 1$ and $g_K = 4$ if and only if 
$N_1 = N_2 = N_3 = 0$ and $N_4 = 1$ where $N_i$ denotes the number of prime divisors 
in $K$ of degree $i$, we deduce that, up to isomorphism, necessarily $K \subseteq k(\Lambda_M)\mathbb{F}_2^s$ 
where $M = T^4 + T + 1$ and $k(\Lambda_M)$ is the cyclotomic function field corresponding 
to the Carlitz module $\Lambda_M$. Finally, we prove that there are precisely two fields $K$ 
over $k$ contained in $k(\Lambda_M)\mathbb{F}_2^s$ such that $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$. In one of 
them $T^7 + T^4 + 1$ splits and $T^7 + T^3 + 1$ is inert and in the other $T^7 + T^4 + 1$ is 
inert and $T^7 + T^3 + 1$ splits. Both fields are isomorphic.

One of the key facts in our proof is that if $[K : k] = 5$ and $p$ is the divisor of 
degree four in $K$, then the different of $K/k$ is $p^4$ and $p$ is totally ramified. This was 
proved by Mercuri and Stirpe in [3].

2. The field $K$

Let $K$ be a congruence function field with exact field of constants the finite field 
of $q$ elements $\mathbb{F}_q$. Let $N_i$ denote the number of prime divisors of degree $i$ in $K$, 
i $i \geq 1$. Let $A_i$ be the number of integral divisors in $K$ of degree $i$, $i \geq 0$. The 
genus of $K$ will be denoted by $g$ and the class number of $K$ by $h$. Let $k = \mathbb{F}_q(T)$ 
be a rational congruence function field and let $R_T = \mathbb{F}_q[T]$ be its ring of integers. 
p will denote the pole divisor of $T$ in $k$. For the standard results on congruence 
function fields and cyclotomic function fields we refer to [7].

For any divisor $q$ in $K$ we denote by $d_K(q)$ its degree. If $P_K(u) = a_0 + a_1u + 
\cdots + a_{2g}u^{2g}$ is the numerator of the zeta function of $K$, where $u = q^{-s}$, we have the following relations ([7 Theorems 6.3.5 and 6.4.1])

\[ a_0 = 1, \quad a_{2g} = q^{2g}, \quad a_{2g-i} = a_ia_{g-i}, \quad 0 \leq i \leq 2g, \]
\[ a_i = A_i - (q + 1)A_{i-1} + qa_{i-2}, \quad 0 \leq i \leq 2g, \quad \text{with} \quad A_{-1} = A_{-2} = 0, \]
\[ P_K(1) = h, \quad A_n = h\left(\frac{q^{n-g+1} - 1}{q - 1}\right) \quad \text{for} \quad n > 2g - 2. \]

From now on, $K$ will denote a field over $\mathbb{F}_2$ such that $g = 4$ and $h = 1$. This 
condition is equivalent to $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$ ([3 Theorem 2 (v)]).
From that paper we know that the numerator of the zeta function of $K$ is $P_K(u) = 
1 - 3u + 2u^2 + 5u^4 - 4u^6 - 16u^7$. Let $p$ denote the only prime divisor of degree 
four in $K$.

In this case, from (2.1) we obtain that $A_0 = 1, \ A_i = N_i = 0, \ 0 \leq i \leq 3, 
A_4 = N_4 = 1$ and $A_5 = N_5 = 3$. Let $\xi_i, \ 1 \leq i \leq 3$ be the three places of degree 
five in $K$. Therefore $\ell(\xi_i^{-1}) = 2, L(\xi_i^{-1}) = \{0, 1, T, T + 1\}$ where $(T)K = \frac{\xi_3}{\xi_1}$ and 
$(T+1)K = \frac{\xi_5}{\xi_1}$ where $(y)_K$ denotes the divisor in $K$ of $y \in K^*$. We have $[K : k] = 5.$
Since $L(p^{-1}) = \mathbb{F}_2$, it follows that the minimal $n$ such that there exists $y \in K$ with $[K : \mathbb{F}_2(y)] = n$ is $n = 5$ and that $k$ is unique satisfying this property.

**Remark 2.1.** Every proper subfield $\mathbb{F}_2 \subseteq E \subseteq K$ such that $K/E$ is separable, is of genus 0. Indeed, for any finite subextension $E$ of $K$, the differential exponent of every prime appearing in the different $\mathcal{D}_{K/E}$ of the extension is greater than or equal to 2 and since the minimum degree of a prime in $K$ is 4, the degree of $d$ of $\mathcal{D}_{K/E}$ is greater than or equal to 8 except in the case that $K/E$ is unramified. From the Riemann-Hurwitz formula, if $g_E \geq 1$ and $K/E$ ramified, we obtain

$$6 = 2g_K - 2 = [K : E](2g_E - 2) + d \geq d \geq 8.$$ 

Thus, if $g_E \geq 1$, $K/E$ is unramified, $[K : E] = 3$, and $g_E = 2$. If $K/E$ is normal, let $t = p \cap E$. Then since $[K : E] = 3$ is relatively prime to $\deg_K p = 4$, it follows that $t$ decomposes fully in $K/E$ and in particular $K$ would contain at least 3 primes of degree four. Therefore $K/E$ is non-normal. Let $\hat{K}$ be the Galois closure of $K/E$. Then $[\hat{K} : K] = 2$ and since $K/K$ is unramified, it follows that $\hat{K} = \mathbb{F}_4$. We have that $K/E\mathbb{F}_4$ is a normal extension of degree 3. Since $\deg_K p = 4$ and $\hat{K}/K$ is an extension of constants of degree 2, we obtain that $p$ decomposes into two primes of degree 2 in $\hat{K}$ (see [7 Theorem 6.2.1]). Thus $\hat{K}$ has exactly two primes of degree 2. Let $\bar{p}$ one of them and let $t = \bar{p} \cap E\mathbb{F}_4$. As above we obtain that $t$ decomposes fully in $\hat{K}/E\mathbb{F}_4$ and in particular we have at least three primes in $\hat{K}$ of degree 2. This contradiction shows that $g_E = 0$.

**Remark 2.2.** Let $\theta \in \mathcal{G} := \text{Aut}_{\mathbb{F}_2} K$. Since $\theta$ permutes the three divisors $\mathcal{C}_i$, $1 \leq i \leq 3$, we have that $\theta|_k \in \text{Aut}_{\mathbb{F}_2} k \cong \text{PSL}(2, \mathbb{F}_2) \cong S_3$ where $k = \mathbb{F}_2(T)$ and $S_3$ is the symmetric group in three elements. Therefore $K^\mathcal{G} \supseteq k^{S_3}$. Therefore $|\mathcal{G}| \text{ divides } 30$. If 5 divides $|\mathcal{G}|$, then the field fixed by an element of order 5 of $\mathcal{G}$ is necessarily $k$ and $K/k$ is normal. If $K/k$ is not normal then $\mathcal{G}$ is trivial since otherwise for each non–trivial subgroup of $\mathcal{G}$, the fixed field is of genus 0 but one of them is of degree less than five. This contradicts that five is the minimum degree of a proper subfield of $K$. Therefore, we have that $K/k$ is normal if and only if $\text{Aut}_{\mathbb{F}_2} K \neq \{\text{Id}\}$.

One of the key facts to prove the uniqueness of $K$ is the following theorem.

**Theorem 2.3.** The extension $K/k$ is normal.

**Proof.** Stirpe and Mercuri [6] proved that $p$ is fully ramified in $K/k$ and in particular $\mathcal{D}_{K/k} = p^4$, where $\mathcal{D}_{K/k}$ denotes the different of the extension $K/k$.

Assume that $K/k$ is not normal. Let $\hat{K}$ be the Galois closure of $K/k$, $G := \text{Gal}(\hat{K}/k)$ and $H := \text{Gal}(\hat{K}/K)$. Then $G$ is a transitive subgroup of $S_5$, the symmetric group in five elements and $H$ is a subgroup of $S_4$. The field of constants of $\hat{K}$ is $\mathbb{F}_2$ because otherwise, since the primes of degree one are inert in $K/k$, we would have an element in $G$ of order $5r$ with $r \geq 2$ contrary to the fact that the elements in $S_5$ are of order less than or equal to six.

From Abhyankar Lemma we obtain that $\hat{K}/K$ is unramified. Let $H_1$ be a proper normal subgroup of $H$ such that $H/H_1$ is abelian. Then we obtain a non–trivial unramified abelian extension of $K$ and since the class number of $K$ is one, this extension would be a constant extension. This contradiction proves that $K/k$ is normal. \qed
We have $\mathfrak{D}_{K/k} = p^4$. Since $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$, we obtain that all prime divisors of $k$ of degree less than or equal to four, except for one of degree four, are inert in $K/k$ and one prime divisor of degree four is ramified.

In $K$ we have three prime divisors of degree four, namely the ones corresponding to $T^4 + T + 1$, $T^4 + T^3 + 1$ and $T^4 + T^3 + T^2 + T + 1$.

**Remark 2.4.** We may assume without loss of generality that the ramified prime of degree four $m$ is the place corresponding to $M = T^4 + T + 1$ for if $m_1$ is the place corresponding to $T^4 + T^3 + 1$ (resp. $T^4 + T^3 + T^2 + T + 1$), then $\sigma: k \to k$ given by $\sigma(T) = \frac{1}{p}$ (resp. $\sigma(T) = \frac{1}{p+1}$) satisfies $\sigma(T^4 + T + 1) = \frac{T^4 + T^3 + 1}{p}$ (resp. $\sigma(T^4 + T + 1) = \frac{T^4 + T^3 + T^2 + T + 1}{p}$). So that $\sigma(m) = m_1$, and extending $\sigma$ to $\tilde{\sigma}: K \to \tilde{K}$ we obtain $\tilde{\sigma}(K) \cong K$ and $\tilde{\sigma}(k) = k$. In $\tilde{\sigma}(K)/k$, the prime $m_1$ is the ramified one.

The extension $K/k$ is a cyclic extension such that all the primes of degree one, two and three in $k$ $\{p_\infty, T, T + 1, T^2 + T + 1, T^3 + T + 1, T^4 + T^3 + T^2 + 1\}$ and the primes of degree four associated to $T^4 + T^3 + 1$ and $T^4 + T^3 + T^2 + T + 1$ are inert. The prime $m$ associated to $T^4 + T + 1$ is ramified.

Since $p_\infty$ is unramified in $K/k$, in fact $\text{con}_{k/K} p_\infty = C_1$, and $m$ is the only ramified prime in $K$ and it is tamely ramified we have that $K \subseteq k(\Lambda_M)F_{2^5}$ (see [4, Proposition 3.4]) and $[K : k] = 5$.

The key step for the main result of this paper is the following theorem.

**Theorem 2.5.** Up to isomorphism, there exists only one field $K$ with $k \subseteq K \subseteq k(\Lambda_M)F_{2^5}$ such that $g = 4$ and $h = 1$.

**Proof.** To start, let $t$ be any prime divisor of $k$ such that $t \neq p_\infty, m$, and let $P \in R_T := \mathbb{F}_2[T]$ be the monic irreducible polynomial associated to $t$. Then the Frobenius map $\varphi_P$ of $P$ in the extension $k(\Lambda_M)/k$ is given by $\varphi_P(\lambda) = \lambda^p$ where $\lambda$ is a generator of $\Lambda_M$ (see [7, Theorem 12.5.1]). In particular for $t \neq p_\infty, m$ we have that the decomposition group of $t$ is $D_P = \langle \varphi_P \rangle$ and $|D_P| = o(P \text{ mod } M)$. We have that $G_M := \text{Gal}(k(\Lambda_M)/k) \cong C_{15}$, the cyclic group of $15$ elements, and let $L$ be the subfield of $k(\Lambda_M)$ such that $[L : k] = 5$.

$$
\begin{array}{cc}
\mathbb{F}_{2^5} & \mathbb{F}_{2^5} \\
\tau^5 & \tau^5 \\
L & L \\
k & k
\end{array}
$$

From the isomorphism $G_M \cong (R_T/(M))^*$ we have that $\tau$, given by $\tau(\lambda) = \lambda^p$, is a generator of $G_M$. Therefore $\text{Gal}(L/k) \cong \langle \tau \text{ mod } (\tau^5) \rangle \cong \langle \tau^3 \rangle$.

Note that $P$ is inert in $L/k$ if and only if $o(\varphi_P) \in \{5, 15\}$. Direct computations give
$T^1 \equiv T \mod M$, $T^2 \equiv T^2 \mod M$, $T^3 \equiv T^3 \mod M$, $T^4 \equiv T + 1 \mod M$, $T^5 \equiv T^2 + T \mod M$, $T^6 \equiv T^3 + T^2 \mod M$, $T^7 \equiv T^3 + T + 1 \mod M$, $T^8 \equiv T^2 + 1 \mod M$, $T^9 \equiv T^3 + T \mod M$, $T^{10} \equiv T^2 + T + 1 \mod M$,

\begin{equation}
T^{11} \equiv T^3 + T^2 + T \mod M, \quad T^{12} \equiv T^3 + T^2 + T + 1 \mod M,
\end{equation}

$T^{13} \equiv T^3 + T^2 + 1 \mod M$, and $T^{14} \equiv T^3 + 1 \mod M$.

From (2.2) we may compute the order of $\varphi_P$:

\begin{equation}
o(\varphi_T) = 15, \quad o(\varphi_{T+1}) = 15, \quad o(\varphi_{T^2+T+1}) = 3, \quad o(\varphi_{T^3+T^2+1}) = 15, \quad o(\varphi_{T^3+T+1}) = 15, \quad o(\varphi_{T^4+T^3+1}) = 5, \quad o(\varphi_{T^4+T^3+T^2+1}) = 5,
\end{equation}

and we also have that $p_\infty$ is fully decomposed in $k(\Lambda_M)/k$ (see [7, Theorem 12.4.6]), that is $o(\varphi_{p_\infty}) = 1$ where $\varphi_{p_\infty}$ denotes the Frobenius of $p_\infty$ in $k(\Lambda_M)/k$. Therefore, the decomposition groups of $P$ in $k(\Lambda_M)/k$ are given by

\begin{align}
D_T &= D_{T+1} = D_{T^3+T^2+1} = D_{T^3+T+1} = G_M = \langle \tau \rangle,
D_{p_\infty} &= \{\text{Id}\}, \quad D_{T^2+T+1} = \langle \tau^5 \rangle,
D_{T^4+T^3+1} &= D_{T^4+T^3+T^2+T+1} = \langle \tau^3 \rangle.
\end{align}

In particular $p_\infty$ and $T^2 + T + 1$ are decomposed in $L/k$ and $T, T+1, T^3 + T^2 + 1, T^3 + T + 1, T^4 + T^3 + 1$ and $T^4 + T^3 + T^2 + T + 1$ are inert in $L/k$.

Now, in the extension of constants $k_5 := kF_{2^5}$ over $k$, all the primes of degree $i$, $1 \leq i \leq 4$, are inert ([7, Theorem 6.2.1]). We have that $\text{Gal}(k_5/k) = \langle \chi \rangle$ where $\chi$ is induced by the Frobenius map of the extension $F_{2^5}/F_2$. More precisely, if $Q(T) = \sum_{i=0}^{d} a_i T^i \in F_{2^5}[T]$, then $\chi(Q(T)) = \sum_{i=0}^{d} a_i^2 T^i$.

Let $P(T) \in R_T$ be a prime of degree $i$, $0 \leq i \leq 4$. Then the residue fields in $k_5/k$ are isomorphic to $F_{2^5}/F_2$, and the Frobenius map $\delta$ of $F_{2^5}/F_2$ is given by $\delta(\alpha) = \alpha^2$ for $\alpha \in F_{2^5}$. Therefore the Frobenius map of $P(T)$ in $k_5/k$ corresponds to $(\chi') \in \text{Gal}(k_5/k)$.

To find the Frobenius map of an arbitrary $P \in R_T$ in the extensions $Lk_5$ and $k(\Lambda_M)k_5$ we consider the following general situation. Let $E/F, J/F$ be Galois extensions of global or local fields such that $E \cap J = F$. Let $S := EJ$.

\begin{equation}
E \quad EJ = S
\end{equation}

\begin{equation}
F \quad J
\end{equation}

We have the isomorphism

\begin{equation}
\Phi : \text{Gal}(S/F) \rightarrow \text{Gal}(E/F) \times \text{Gal}(J/F)
\end{equation}

\begin{equation}
\Phi(\theta) = (\theta|_E, \theta|_J),
\end{equation}

and the inverse of $\Phi$ is given by

\begin{equation}
\Psi : \text{Gal}(E/F) \times \text{Gal}(J/F) \rightarrow \text{Gal}(S/F)
\end{equation}

\begin{equation}
\Psi(\alpha, \beta) = \tilde{\alpha} \tilde{\beta},
\end{equation}
where \( \tilde{\alpha}: S \rightarrow S \) and \( \tilde{\beta}: S \rightarrow S \) are defined, for \( z = \sum_{i=1}^{t} x_i y_i \in S \) with \( x_i \in E \) and \( y_i \in J \), by

\[
\tilde{\alpha}\left( \sum_{i=1}^{t} x_i y_i \right) = \sum_{i=1}^{t} \alpha(x_i) y_i
\]

and

\[
\tilde{\beta}\left( \sum_{i=1}^{t} x_i y_i \right) = \sum_{i=1}^{t} x_i \beta(y_i).
\]

Let \( P \) be a prime in \( F \), \( \mathfrak{P} \) be a prime in \( S \) above \( P \) and let \( q := \mathfrak{P} \cap J \) and \( t := \mathfrak{P} \cap E \). Assume that \( P \) is unramified in \( S/F \). Let \( \left[ \frac{S/F}{\mathfrak{P}} \right] \in \text{Gal}(S/F) \) be the Frobenius map of \( \mathfrak{P}/P \). Then

\[
\left[ \frac{S/F}{\mathfrak{P}} \right] \bigg|_E = \left[ \frac{E/F}{t} \right] \quad \text{and} \quad \left[ \frac{S/F}{\mathfrak{P}} \right] \bigg|_J = \left[ \frac{J/F}{q} \right].
\]

Therefore

\[
\left(2.4\right)
\]

We will apply formula (2.4) to our case \((F =) k = F_2(T), (E =) L, (J =) k_5 \) and \((S =) Lk_5 \)."There exist exactly four extensions \( R_j, 1 \leq j \leq 4 \) of degree five over \( k \) contained in \( L_5 := Lk_5 \) other than \( L \) and \( k_5 \). The fields \( K \) we are looking are, if any, among the fields \( R_j \) such that all the primes \( P(T) \) in \( k \) of degree less than or equal to four other than \( M \) are inert in \( K/k \). Note that since \( k_5/k \) is unramified and the only ramified prime in \( L/k \) is \( m \), the only ramified prime in each \( R_j \) is \( m \).

We have \( \text{Gal}(L_5/k) \cong C_5 \times C_5 \) and the decomposition group of any unramified prime is cyclic since the characteristic is \( 2 \neq 5 \). Thus, any prime of degree \( i \) with \( i \leq 4 \) other than \( m \) is decomposed in exactly one field among \( L, R_j, 1 \leq j \leq 4 \), namely, in the fixed field \( L_5^H \) where \( H \) denotes the decomposition group of the prime in \( L_5/k \). Now, \( p_\infty \) and \( T^2 + T + 1 \) are decomposed in \( L/k \) so they are inert in every \( R_j \), \( 1 \leq j \leq 4 \).
Next we compute the decomposition group \( D_P \) in \( k(\Lambda_M)k_5/k \) for \( P \in \{ T, T + 1, T^3 + T^2 + 1, T^3 + T + 1, T^4 + T^3 + 1, T^4 + T^2 + T + 1 \} \) using formula (2.4). We denote by \( \xi_P \) the Frobenius of \( P \) in \( k_5/k \) and by \( \varphi_P \) the Frobenius of \( P \) in \( k(\Lambda_M)/k \) (see (2.3)). Therefore, the Frobenius \( \theta_P \) of \( P \) in \( k(\Lambda_M)k_5/k \) is given by \( \theta_P = \varphi_P \xi_P \).

From (2.2) and from the fact that the Frobenius \( \xi_P \) of any \( P \) of degree \( i \) in \( k_5/k \) corresponds to \( \langle \chi^i \rangle \), we obtain \( \theta_P \) and the decomposition group \( D_P = \langle \theta_P \rangle \) for each \( P \) in \( k(\Lambda_M)k_5 \) as follows

\[
\begin{align*}
\theta_T &= \tilde{\tau} \tilde{\chi}, \\
\theta_{T+1} &= \tilde{\tau}^4 \tilde{\chi}, \\
\theta_{T^3+T^2+1} &= \tilde{\tau}^{13} \tilde{\chi}, \\
\theta_{T^3+T+1} &= \tilde{\rho}^{7} \tilde{\chi}, \\
\theta_{T^4+T^3+1} &= \tilde{\rho}^{9} \tilde{\chi}, \\
\theta_{T^4+T^3+T^2+T+1} &= \tilde{\rho}^{6} \tilde{\chi}.
\end{align*}
\]

Now let \( H_P \) be the subgroup of \( D_P \) of order 5. We obtain

(2.5) \[ H_T = H_{T^3+T^2+1} = H_{T^4+T^3+1} = \langle \tilde{\rho}^{6} \tilde{\chi} \rangle, \]

\[ H_{T+1} = H_{T^3+T+1} = H_{T^4+T^3+T^2+T+1} = \langle \tilde{\rho}^{9} \tilde{\chi} \rangle, \]

and note that \( \langle \tilde{\rho}^{6} \tilde{\chi} \rangle \neq \langle \tilde{\rho}^{9} \tilde{\chi} \rangle \).

Let \( R_3 = L_5^{(\tilde{\rho}^{6} \tilde{\chi})} \) and \( R_4 = L_5^{(\tilde{\rho}^{9} \tilde{\chi})} \). From (2.5) we have that in \( R_3/k, T, T^3+T^2+1 \) and \( T^4+T^3+1 \) split and in \( R_4/k, T+1, T^3+T+1 \) and \( T^4+T^3+T^2+T+1 \) split. Therefore all the primes of degree \( i \) with \( 1 \leq i \leq 4 \) other than \( m \) are inert in \( R_1/k \) and in \( R_2/k \), where \( R_1 = L_5^{(\tilde{\rho}^{6} \tilde{\chi})} \) and \( R_2 = L_5^{(\tilde{\rho}^{12} \tilde{\chi})} \) and we have \( \langle \tilde{\rho}^{3} \tilde{\chi} \rangle \neq \langle \tilde{\rho}^{12} \tilde{\chi} \rangle \). The fields \( R_1 \) and \( R_2 \) are of genus four and class number one.

Finally, we will prove that \( R_1 \cong R_2 \). Let \( \sigma: k \to k \) be given by \( \sigma(T) = \frac{T}{T} \) and extend \( \sigma \) to \( \tilde{\sigma}: R_1 \to \tilde{k} \). Since \( R_1 \) and \( R_2 \) are the only subfields of \( L_5 \) of genus four and class number one, necessarily we have \( \sigma(R_1) = R_1 \) or \( R_2 \). Now consider the primes \( T^7 + T^4 + 1 \) and \( T^7 + T^3 + 1 \). Since \( T^7 + T^4 + 1 \equiv T^3 + 1 \mod M \) we have that \( H_{T^7+T^4+1} = \langle \tilde{\rho}^{12} \tilde{\chi} \rangle \). Therefore \( T^7 + T^4 + 1 \) splits in \( R_2 \) and is inert in \( R_1 \).

Now consider the prime \( T^7 + T^3 + 1 \). Since \( T^7 + T^3 + 1 \equiv T \mod M \), it follows that \( H_{T^7+T^3+1} = \langle \tilde{\rho}^{3} \tilde{\chi} \rangle \) so that \( T^7 + T^3 + 1 \) splits in \( R_1 \) and is inert in \( R_2 \). Since \( \sigma(T^7 + T^4 + 1) = \frac{T^7 + T^3 + 1}{T^7} \) it follows that \( \sigma(R_1) = R_2 \) and \( R_1 \cong R_2 \). This proves Theorem 2.5.

Remark 2.6. The fields \( R_1 \) and \( R_2 \) are the fields described by C. Stirpe in [5].

The main result of this paper is a consequence of Theorem 2.3, Remark 2.4 and Theorem 2.5.

Theorem 2.7. Up to isomorphism, there exists exactly one function field over the finite field of two elements of class number one and genus four.

Remark 2.8. The field \( K \) (equal to either \( R_1 \) or \( R_2 \)) satisfies that \( \mathcal{G} = \text{Aut}_{F_2} K = \text{Aut}_K K = \text{Gal}(K/k) \cong C_5 \). Indeed, if \( |\mathcal{G}| > 5 \), there would exist an element of order 2 or 3 in \( \mathcal{G} \) and if \( S \) were the group generated by this element, we would have \( 1 < [K : K^S] = |S| < 5 \), thus \( K^S \) would be of genus 0 (see Remark 2.1). This contradicts that five is the minimum degree of a proper subfield of \( K \).
References

[1] Leitzel, James R.C.; Madan, Manohar L.; Queen, Clifford S., Algebraic function fields with small class number, Journal of Number Theory 7, 11–27, (1975).
[2] MacRae, Robert E., On unique factorization in certain rings of algebraic functions, Journal of Algebra 17, 243–261, (1971).
[3] Madan, Manohar L.; Queen, Clifford S., Algebraic function fields of class number one, Acta Arithmetica 20, 423–432–375, (1972).
[4] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, Genus fields of abelian extensions of rational congruence function fields, Finite Fields Appl. 20, 40–54, (2013).
[5] Stirpe, Claudio, A counterexample to ‘Algebraic function fields with small class number’, Journal of Number Theory 143, 402–404, (2014).
[6] Mercuri, Pietro; Stirpe, Claudio, Classification of Algebraic Function Fields with Class Number One, arXiv:1406.5505v3, December 2 (2014).
[7] Villa–Salvador, Gabriel, Topics in the theory of algebraic function fields, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N.
E-mail address: mrzedowski@ctrl.cinvestav.mx

Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del I.P.N.
E-mail address: gvillasalvador@gmail.com, gvilla@ctrl.cinvestav.mx