Function Fields with Class Number Indivisible by a Prime ℓ

Michael Daub, Jaclyn Lang, Mona Merling, Allison M. Pacelli, Natee Pitiwan, and Michael Rosen

July 18, 2010

Abstract

It is known that infinitely many number fields and function fields of any degree m have class number divisible by a given integer n. However, significantly less is known about the indivisibility of class numbers of such fields. While it's known that there exist infinitely many quadratic number fields with class number indivisible by a given prime, the fields are not constructed explicitly, and nothing appears to be known for higher degree extensions. In the function field case, in 1999 Ichimura [12] constructed an explicit infinite family of quadratic function fields over $\mathbb{F}_q(T)$ with class number not divisible by 3; he requires that $q \equiv 2 \pmod 3$. Pacelli and Rosen [32] extended this to non-quadratic fields of degree m over $\mathbb{F}_q(T)$, $3 \nmid m$, for an infinite number of prime powers q, $q \equiv 2 \pmod 3$. In this paper, we generalize Pacelli and Rosen's result, constructing, for a large class of q, infinitely many function fields of any degree m over $\mathbb{F}_q(T)$ with class number indivisible by an arbitrary prime ℓ. We give an explicit description of those primes (and prime powers) q for which the result holds. For the special case where $\ell = 3$ and $m = 2$, we recover Ichimura's result.

1 Introduction

The question of class number indivisibility has always been more difficult than the question of class number divisibility. For example, although Kummer was able to prove Fermat's Last Theorem for regular primes, that is, primes p not dividing the class number of the p-th cyclotomic field, it is still unknown today whether infinitely many regular primes exist (in 1915, Jensen did prove the existence of infinitely many irregular primes).

In 1976, Hartung [8] showed that infinitely many imaginary quadratic number fields have class number not divisible by 3. Horie and Onishi [9, 10, 11], Jochnowitz [14], and Ono and Skinner [29] proved that there are infinitely many imaginary quadratic number fields with class number not divisible by a given prime p. Quantitative results on the density of quadratic fields with class number indivisible by 3 have been obtained by Davenport and Heilbronn [3], Datskovsky and Wright [2], and Kimura [16] (for relative class numbers). Kohnen and Ono made further progress in [17]. They proved that for all $\epsilon > 0$ and sufficiently large x, the number of imaginary quadratic number fields $K = \mathbb{Q}(\sqrt{-D})$ with $p \nmid h_K$ and $D < x$ is

$$\geq \left(\frac{2(p-2)}{\sqrt{3}(p-1)} - \epsilon \right) \frac{\sqrt{x}}{\log x}.$$

Less is known about class numbers in real quadratic fields, but in 1999, Ono [28] obtained a similar lower bound for the number of real quadratic fields K with $p \nmid h_K$ and bounded discriminant; this bound is valid for primes p with $3 < p < 5000$. The results above do not give explicit families of fields with the desired class number properties. In 1999, Ichimura [12] constructed an explicit infinite family of quadratic function fields over $\mathbb{F}_q(T)$ with class number not divisible by 3; he requires that $q \equiv 2 \pmod 3$. Pacelli and Rosen [32] extended this to non-quadratic fields of degree m over $\mathbb{F}_q(T)$, $3 \nmid m$, for an infinite number of prime powers q, also with the condition that $q \equiv 2 \pmod 3$.

In this paper, we generalize Pacelli and Rosen's result, constructing, for a large class of q, infinitely many function fields of any degree m over $\mathbb{F}_q(T)$ with class number indivisible by an arbitrary prime ℓ. We give an explicit description of those primes (and prime powers) q for which the result holds. For the special case where $\ell = 3$ and $m = 2$, we recover Ichimura's result.

For related results on divisibility of class numbers, see Nagell [26] for imaginary number fields, Yamamoto [39] or Weinberger [38] for real number fields, and Friesen [6] for function fields. For quantitative results, see for example Murty [25, 4]. More generally, to see results on the minimum n-rank of the ideal class group of a global field, see Azuhata and Ichimura [1] or Nakano [27] for number fields and Lee and Pacelli [20, 21, 22, 30, 31] for function fields.

As in [12] and [32], the fields we construct are given explicitly. The idea of the proof is to construct two towers of fields $N_1 \subset \cdots \subset N_t = \mathbb{F}_q(T)$ and $M_1 \subset \cdots \subset M_t$. The fields are designed so that $\ell \nmid h_{M_1}$, N_{i+1}/N_i is cyclic of degree ℓ and ramified (totally) at exactly one prime $\mathfrak{p}_i$, M_i/N_i is a degree m extension in which $\mathfrak{p}_i$ is inert, and M_{i+1} is the composite field of M_i and N_{i+1}. Together with class field theory, this is enough to show that $\ell \nmid h_{M_i}$ for any $1 < i \leq t$. Thus M_t has degree m over N_t, the rational function field, and has class number not divisible by ℓ.

Let q be a power of an odd prime, and $\mathbb{F}_q$ the finite field with q elements. The main results are as follows:

Theorem 1.1. *Let m be any positive integer $m > 1$ and ℓ an odd prime. Write $m = \ell^t m_1$ for integers t and m_1 with $\ell \nmid m_1$. Let m_0 be the square-free part of m_1, and assume that q is sufficiently large with $q \equiv 1 \pmod{m_0}$ and $q \equiv -1 \pmod{\ell}$. Then there are infinitely many function fields K of degree m over $\mathbb{F}_q(T)$ with $\ell \nmid h_K$.*

Corollary 1.2. *Suppose m is indivisible by ℓ and that $q \equiv 1 \pmod m$. If, in addition, $q \equiv -1 \pmod{\ell}$, there are infinitely many geometric and cyclic extensions K of degree m over $\mathbb{F}_q(T)$ such that $\ell \nmid h_K$.*

Corollary 1.3. *Suppose $t \geq 1$ and $m = \ell^t m_1$ with m_1 not divisible by ℓ. If $q \equiv 1 \pmod{m_1}$ and $q \equiv -1 \pmod{\ell^t}$, then there are infinitely many geometric and cyclic extensions K of degree m over $\mathbb{F}_q(T)$ such that $\ell \nmid h_K$.*

For the remainder of this introduction, we will outline some important results and methods which will be used in the proof of the main theorem, Theorem 1.1. In the statement of Theorem 1.1 we use the phrase "all sufficiently large q." In the Appendix we give a quantitative version of this restriction. In Section 3, we prove a function field analogue of a class field theoretic result of Iwasawa; this result is stated but not proved by Ichimura in [12]. In Section 4, we prove the main theorem, and in Section 5, we prove the two corollaries stated above.

In [12] the cubic extensions needed were generated by using a variant of the "simplest cubic polynomials" discovered by Dan Shanks [36]; $X^3 - 3uX^2 - (3u+3)X - 1$. Any root of this polynomial generates a Galois extension of $k(u)$ with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Here k is any field with characteristic different from 3. Hashimoto and Miyake found generalizations of this polynomial for any odd degree ℓ. Their work was simplified and extended by Rikuna in [33] and further developed by Komatsu in [18]. We will restrict ourselves to the case ℓ is odd and present Rikuna's polynomials as exposited in Komatsu.

Let K be a field whose characteristic does not divide ℓ. Let ζ be a primitve ℓ-th root of unity in some field containing k and suppose $\omega = \zeta + \zeta^{-1}$ is in K. Define

$$\mathcal{P}(X) := (\zeta^{-1} - \zeta)^{-1} \left(\zeta^{-1}(X - \zeta)^{\ell} - \zeta(X - \zeta^{-1})^{\ell} \right) , \tag{1}$$

and

$$\mathcal{Q}(X) := (\zeta^{-1} - \zeta)^{-1} \left((X - \zeta)^{\ell} - (X - \zeta^{-1})^{\ell} \right) .$$

Note that $\mathcal{P}(X)$ has degree ℓ, $\mathcal{Q}(X)$ has degree $\ell - 1$, and both polynomials have coefficients in K. It will be convenient to define the rational function $r(X) = \mathcal{P}(X)/\mathcal{Q}(X)$. Finally, define

$$F(X, u) = \mathcal{P}(X) - u\mathcal{Q}(X) \in K[X, u] . \tag{2}$$

Here we assume u is transcendental over K. As can be seen from the following theorem, this is a higher degree analogue of the Shanks polynomial.

Theorem 1.4. *The polynomial $F(X, u)$ is irreducible over $K(u)$. Let x be a root in some extension field of $K(u)$. Then, $K(x, u) = K(x)$ is a Galois extension of $K(u)$ with Galois group isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$.*

The discriminant of $F(X, u)$ is given by

$$\ell^{\ell}(4 - \omega^2)^{(\ell-1)(\ell-2)/2}(u^2 - \omega u + 1)^{\ell-1} . \tag{3}$$

Note that if x is a root of $F(X, u) = 0$, then $u = \mathcal{P}(x)/\mathcal{Q}(x) = r(x)$. This justifies the equality $K(x, u) = K(x)$. The formula for the discriminant is stated in Rikuna's paper, but not proven there. A proof can be found in Komatsu [18], Lemma 2.1.

Finally, we note that the polynomial $P(u) = u^2 - \omega u + 1 = (u - \zeta)(u - \zeta^{-1})$ plays a big role in our considerations. From now on we will assume that $\zeta \notin K$. This implies that $P(u)$ is irreducible over K. The formula for the discriminant then shows that the only primes of $K(u)$ which can ramify in $K(x)$ are the zero divisor of $P(u)$ and possibly the prime at infinity. A simple calculation, using the Riemann-Hurwitz formula, shows that the prime at infinity does not ramify. Thus, $K(x)/K(u)$ ramifies at exactly one prime, the zero divisor of $P(u)$ (for details see the proof of Lemma 4.1).

2 Preliminaries

The following lemma is well-known, and a proof can be found in [19].

Lemma 2.1. *Let k be a field, m an integer ≥ 2, and $a \in k^\times$. Assume that for any prime p with $p \mid m$, we have $a \notin k^p$, and if $4 \mid m$, then $a \notin -4k^4$. Then $x^m - a$ is irreducible in $k[x]$.*

We will also need the following lemma whose proof is elementary.

Lemma 2.2. *Let A be an abelian group, and a an element of A. Suppose that a is an n_1-power and an n_2-power with $(n_1, n_2) = 1$. Then, a is an $n_1 n_2$-power.*

The main goal of this section is to prove the following.

Lemma 2.3. *Let ℓ be an odd prime, $m > 1$ an integer not divisible by ℓ, and ζ a primitive l-th root of unity. For all sufficiently large prime powers q satisfying*

(i) $q \equiv -1 \pmod{\ell}$, and

(ii) $q \equiv 1 \pmod{m_0}$ where m_0 is the square-free part of m,

there is a $\gamma \in \mathbb{F}_q^\times$ such that $X^m - (\gamma + \ell\zeta)$ is irreducible over $\mathbb{F}_q(\zeta)$.

Proof. We begin by reducing the problem to one which takes place entirely in the field $\mathbb{F}_q$.

Since $q \equiv -1 \pmod{\ell}$ it follows that the quadratic extension of $\mathbb{F}_q$ has the form $\mathbb{F}_q(\zeta)$, where ζ is a primitive ℓ-th root of unity. Note that since $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^2}$, then -1 must be a square in $\mathbb{F}_q(\zeta)$; say $-1 = \alpha^2$ in $\mathbb{F}_q(\zeta)$. As a result, to prove that $X^m - (\gamma + \ell\zeta)$ is irreducible over $\mathbb{F}_q(\zeta)$, it is enough by Lemma 2.1 to show that $\gamma + \ell\zeta$ is not a p-th power for all primes p dividing m. This suffices because if $4|m$ and $\ell\zeta + \gamma = -4\beta^4$ for some $\beta \in \mathbb{F}_q(\zeta)$, then $\ell\zeta + \gamma = (2\alpha\beta^2)^2$ is a square in $\mathbb{F}_q(\zeta)$, a contradiction.

So let p be a prime dividing m and suppose that $\gamma + \ell\zeta$ is a p-th power in $\mathbb{F}_q(\zeta)$. Taking norms from $\mathbb{F}_q(\zeta)$ to $\mathbb{F}_q$, we find that $\gamma^2 + \ell(\zeta + \zeta^{-1})\gamma + \ell^2$ is a p-th power in $\mathbb{F}_q$. Completing the square, we find c and d in $\mathbb{F}_q$ such that

$$\gamma^2 + (\zeta + \zeta^{-1})\ell\gamma + \ell^2 = (\gamma - c)^2 + d\ .$$

A short computation shows that $d \neq 0$. It follows that if we can find a $\gamma \in \mathbb{F}_q$ such that $(\gamma - c)^2 + d$ is not a p-th power in $\mathbb{F}_q$ for every prime $p|m$, then $X^m - (\gamma + \ell\zeta)$ is irreducible over $\mathbb{F}_q(\zeta)$ as required. We will show that for q large enough, there exists $\lambda \in \mathbb{F}_q$ such that $\lambda^2 + d$ is not a p-th power for every prime p dividing m. Then, $\gamma = \lambda + c$ will be the element we are looking for.

For each k dividing $q-1$, consider the curve $C_k : y^2 + d = x^k$. This curve is absolutely irreducible and non-singular except for the unique point at infinity when $k > 3$. Its genus is $(k-1)/2$ when k is odd, and $\frac{k}{2}-1$ when k is even. Let N_k be the number of points $(\alpha, \beta) \in \mathbb{F}_q^{(2)}$ such that $\beta^2 + d = \alpha^k$, i.e. the number of rational points on C_k. Using either the Riemann hypothesis for curves, or a more elementary argument using Jacobi sums (see [13], Chapter 8), one can show that $|N_k - q| \leq (k-1)\sqrt{q}$. We will need this estimate, especially when k is square-free dividing m. Our hypothesis insures that in this case, k divides $q-1$.

Let R_k denote the set of k-th powers in $\mathbb{F}_q$ (including zero), and let

$$S_k = \{\eta \in R_2 \mid \eta + d \in R_k\}.$$

It is easy to see that R_2 has $\frac{q+1}{2}$ elements. What can be said about the size of S_k? Well, if (α, β) is a rational point on C_k, i.e. an element of $C_k(\mathbb{F}_q)$, then $\beta^2 \in S_k$. So, there is a map $(\alpha, \beta) \to \beta^2$ from $C_k(\mathbb{F}_q)$ to S_k. From the definition of S_k, it is clear that this map is onto. Since $\pm 1 \in \mathbb{F}_q$ and the k-th roots of unity are in $\mathbb{F}_q$, the map is $2k$-to-1 at all but at most two elements of S_k, namely 0 and $-d$ (0 if d is a k-th power, and $-d$ if $-d$ is a square). In all cases, one can show that $|\#(S_k) - N_k/2k| < 2$. It follows that the number of elements in S_k is approximately $q/2k$.

If S is a subset of R_2, let S' denote its complement in R_2. Consider the set

$$T = \bigcap_{p|m} {S_p}' \ .$$

The intersection is over all primes dividing m. If $\tau \in T$, then $\tau + d$ is not a p-th power for any prime p dividing m. Thus, if $\tau = \lambda^2$ then $\gamma = \lambda + c$ is the element we are looking for. We will show that T is non-empty for q large enough. In fact, we will show a lot more, namely

$$\#T = \frac{q}{2} \prod_{p|m} (1 - \frac{1}{p}) + O(\sqrt{q}) \ .$$

Let $p_1, p_2, \ldots, p_t$ be the primes dividing m. Then,

$$T' = \bigcup_{i=1}^{t} S_{p_i} \ ,$$

and therefore,

$$\#(T') = \sum_i \#(S_{p_i}) - \sum_{i<j} \#(S_{p_i} \cap S_{p_j}) + \sum_{i<j<k} \#(S_{p_i} \cap S_{p_j} \cap S_{p_k}) - \ldots$$

by the inclusion/exclusion principle.

The intersections simplify considerably. Namely, it can be shown via Lemma 2.2 that

$$S_{p_{i_1}} \cap S_{p_{i_2}} \cap \cdots \cap S_{p_{i_r}} = S_{p_{i_1} p_{i_2} \cdots p_{i_r}} \ .$$

Since, by hypothesis, the square-free part of m divides $q-1$, we can use our previous estimates, $|\#(S_k) - N_k/2k| < 2$ and $|N_k - q| \le k\sqrt{q}$. From this we see that

$$\#(S_k) = \frac{q}{2k} + O(\sqrt{q}) \ ,$$

for all square-free k dividing m. Using this in the above expression for $\#(T')$ yields

$$2\#(T')/q = \sum_i \frac{1}{p_i} - \sum_{i<j} \frac{1}{p_i p_j} + \sum_{i<j<k} \frac{1}{p_i p_j p_k} - \cdots + O(q^{-\frac{1}{2}}) \ .$$

which is equivalent to (using $\#(R_2) = \frac{q+1}{2}$)

$$\#(T) = \frac{q}{2} \prod_i (1 - \frac{1}{p_i}) + O(\sqrt{q}) \ .$$

□

By paying more attention to detail it is fairly easy to give an explicit lower bound for $\#(T)$ in terms of q and thus determine how large q has to be in order to insure the T is non-empty. See the appendix for details.

3 Ichimura's Lemma and Class Number Indivisibility

In [12], Ichimura states a version of the following lemmas, though his proof seems incomplete. Here we give a rigorous proof, using the same ideas which Iwasawa used in his original result for number fields.

Proposition 3.1. *(Ichimura's Lemma) Let K/k be a finite, geometric, ℓ-extension which is ramified at exactly one prime $\mathfrak{p}$ of k. Suppose that only one prime $\mathfrak{P}$ of K lies above $\mathfrak{p}$, and $\ell \nmid \deg \mathfrak{p}$. Then, $\ell \mid h_K$ implies $\ell \mid h_k$.*

First, we fix some notation. Let k be a function field in one variable with finite field of constants $\mathbb{F}_q$. Let $\mathfrak{p}$ be a prime of k and A the subring of k consisting of elements whose only poles are at $\mathfrak{p}$. It is well known that A is a Dedekind domain and that its group of units is precisely $\mathbb{F}_q^\times$.

The proof of the following lemma is given in [34].

Lemma 3.2. *Let J_k be the group of divisor classes of degree 0 of k, Cl_A the ideal class group of A, and $d = \deg \mathfrak{p}$. Then, the following sequence is exact.*

$$(0) \to J_k \to Cl_A \to \mathbb{Z}/d\mathbb{Z} \to (0).$$

Corollary 3.3. *Let $h_A = \#Cl_A$, the class number of A, and $h_k = \#J_k$, the class number of k. Then*

$$h_A = h_k d.$$

A proof of the following can be found in [34].

Proposition 3.4. *Let k_A be the maximal, abelian, unramified extension of k in which $\mathfrak{p}$ splits completely. Then k_A is a finite abelian extension of k and*

$$\mathrm{Gal}(k_A/k) \cong Cl_A.$$

Proof of Ichimura's Lemma. Let B be the integral closure of A in K. Applying Lemma 3.2 and its corollary to the pair $B, \mathfrak{P}$, we see that $\ell \mid h_K$ implies $\ell \mid h_B$. Let E be the maximal abelian, unramified, ℓ-extension of K in which $\mathfrak{P}$ splits completely. Since $E \subset K_B$, and $\ell \mid h_B = [K_B : K]$, we see that E properly contains K.

It is easily seen that E/k is a Galois ℓ-extension. Let G denote its Galois group. For a prime $\mathcal{P}$ of E lying over $\mathfrak{P}$, let $D(\mathcal{P}/\mathfrak{p})$ be its decomposition group over k. Note that

$$|D(\mathcal{P}/\mathfrak{p})| = e(\mathcal{P}/\mathfrak{p})f(\mathcal{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = [K : k] \ .$$

The last inequality is because of the assumption that $\mathfrak{P}$ is the only prime of K lying over $\mathfrak{p}$. We conclude that $D(\mathcal{P}/\mathfrak{p})$ is a proper subgroup of G. Since G is an ℓ-group, it follows from a well known result about ℓ-groups that $D(\mathcal{P}/\mathfrak{p})$ is contained in a normal subgroup $N \subset G$ of index ℓ. Any other prime $\mathcal{P}'$ of E over $\mathfrak{P}$ has a decomposition group over k which is conjugate to $D(\mathcal{P}/\mathfrak{p})$ and is thus also contained in N. It follows that the fixed field L of N is a cyclic, unramified extension of k in which $\mathfrak{p}$ splits completely. It follows that $L \subset k_A$. Thus, $l \mid h_A = h_k d$ by the corollary to Lemma 3.2. Since we are assuming that ℓ does not divide d, we must have $\ell \mid h_k$, as asserted. □

Before getting to the main result of this section we will need a lemma whose proof is a simple consequence of class field theory. It will be notationally convenient to use the language of valuations rather than primes. As is well known, these are completely equivalent concepts. Let M_k be the set of normalized valuations of k. For each $v \in M_k$, let k_v be the completion of k at v, O_v the ring of integers of k_v, P_v the maximal ideal of O_v, and U_v the unit group of the ring O_v. The norm of v, Nv, is the number of elements in the residue class field $\kappa_v = O_v/P_v$.

Working inside a fixed algebraic closure of k, let $\bar{k}$ be the maximal constant field extension of k, and k^{un} the maximal unramified extension of k. It is well known that $k^{un}/\bar{k}$ is a finite Galois extension with Galois group isomorphic to the divisor classes of degree zero of k. Thus, $[k^{un} : \bar{k}] = h_k$. Now choose a valuation w of k and let k_w be the maximal abelian extension of k which is at most tamely ramified at w and unramified everywhere else.

Lemma 3.5. *The Galois group of $k(w)/k^{nr}$ is cyclic of order $\frac{Nw-1}{q-1}$.*

Proof. We sketch the proof. The open subgroups of the idéles of k corresponding to k^{un} and $k(w)$ respectively are

$$k^* \prod_v U_v \quad \text{and} \quad k^* \big(\prod_{v \neq w} U_v \times U_w^{(1)} \big) \ ,$$

where $U_w^{(1)}$ is the subgroup of U_w consisting of units congruent to 1 modulo P_w. By class field theory the Galois group in question is isomorphic to the quotient of these two groups. The result now follows by a simple index calculation, which shows that this quotient is isomorphic to $\kappa_w^*/\mathbb{F}_q^*$. □

We are now in a position to prove the following theorem. We are indebted to the referee for a suggestion which allowed us to considerably simplify our original proof.

Theorem 3.6. *Let $k/\mathbb{F}_q$ be a function field in one variable over a finite constant field $\mathbb{F}_q$ with q elements. Let ℓ be a fixed rational prime, and suppose that ℓ does not divide $q(q-1)$. Suppose further that the class number h_k is not divisible by ℓ. Then for every positive integer t, there are infinitely many non-isomorphic geometric extensions L of k such that $[L:k]=\ell^t$ and for which h_L is not divisible by ℓ.*

Proof. It suffices to prove the result for $t=1$. If one has that case in hand, one can iterate the construction. Suppose L_{t-1} is a geometric extension of k of degree ℓ^{t-1} with class number prime to ℓ. Then all the hypotheses of the theorem apply to L_{t-1} as base field, and we can find a geometric extension L_t of degree ℓ over L_{t-1} whose class number is not divisible by ℓ.

The proof will also show that the construction provides infinitely many non-isomorphic examples of fields with the required properties.

Fix a valuation w of k, and let G_w to be the Galois group of k_w over k. Let ϕ be a topological generator of $\mathrm{Gal}(\bar{k}/k)$, for example, one can choose ϕ to be the Frobenius automorphism of $\bar{k}/k$. Next, choose an element $\sigma \in G_w$ which restricts to ϕ, and let D be the closure in G_w of the cyclic group generated by σ. The restriction map from D to $\bar{k}$ is an isomorphism of D onto $\mathrm{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$. In particular, D is torsion free. Let $N = \mathrm{Gal}(k_w/\bar{k})$. This is a finite group, so we have $D \cap N = \langle e \rangle$. We also deduce that $DN = G_w$.

Now, let K be the fixed field of D. From Galois theory we deduce $\mathrm{Gal}(K/k) \cong N$, and $K \cap \bar{k} = k$. Thus, K is a finite geometric extension of k. Let E be the maximal unramified extension of k in K. Using the isomorphism of N with $\mathrm{Gal}(K/k)$ together with Lemma 3.5, we see that $[K:E] = (Nw-1)/q-1$ and $[E:k]=h_k$.

Let e be the order of q modulo ℓ. By hypothesis, $e>1$. Also, $e \mid (\ell-1)$ so $\ell \nmid e$. For sufficiently large positive integers n there exist valuations of degree ne (see Theorem 5.12 in [35]). So, let n be a sufficiently large integer prime to ℓ and choose w to be a valuation of degree ne.

$$\frac{Nw-1}{q-1} = \frac{q^{ne}-1}{q-1} = \frac{q^{ne}-1}{q^e-1}\frac{q^e-1}{q-1}\ .$$

Both factors are in $\mathbb{Z}$ and the last factor is divisible by ℓ since ℓ does not divide $q-1$. By Lemma 3.5, we see that ℓ divides [K:E] which in turn divides $[K:k]$. Since K/k is an abelian extension, there is an intermediate extension L with $[L:k]=\ell$. We claim that L has all the properties required.

First of all, L/k is a geometric extension, since K/k is geometric. Secondly, L is totally ramified at w and nowhere else. Again, since $L \subseteq K$ we know that L is unramified away from w. If it were also unramified at w, then it would follow that $L \subseteq E$. However, $[E:k]=h_k$

which is prime to ℓ by hypothesis. This would contradict $[L : k] = \ell$. In order to apply Ichimura's Lemma, Proposition 3.1, it remains to show that $\deg w$ is prime to ℓ. We have chosen w such that $\deg w = ne$ where n is prime to ℓ and since $e < \ell$ it too is prime to ℓ. Finally, we apply Proposition 3.1 to conclude that the class number of L is not divisible by ℓ. □

The fields L constructed in Theorem 3.6 need not be Galois over k. It is of interest to examine under what conditions we can construct such extensions which are cyclic over k. By restricting the prime power q somewhat, we can assure the existence of such fields.

Corollary 3.7. *Suppose the conditions of the theorem are satisfied and in addition that* $q \equiv -1 \pmod{\ell^t}$. *Then there are infinitely many geometric and cyclic extensions* L *of degree* ℓ^t *over* $k = \mathbb{F}_q(T)$ *such that* h_L *is not divisible by* ℓ.

Proof. First of all, note that the congruence $q \equiv -1 \pmod{\ell}$ implies that the order of q modulo ℓ is $e = 2$. Let n be a large integer prime to ℓ and w a valuation of k of degree $2n$.

Using Corollary 3.5, and the notation in the proof of the theorem, we see that $\mathrm{Gal}(K/E)$ is a cyclic group of order

$$\frac{Nw - 1}{q - 1} = \frac{q^{2n} - 1}{q^2 - 1}\frac{q^2 - 1}{q - 1} .$$

Thus, the order of $\mathrm{Gal}(K/E)$ is divisible by $q+1$, and so by ℓ^t. It follows that, $\mathrm{Gal}(K/k)$ has a cyclic subgroup of order ℓ^t, and consequently a cyclic quotient group of order ℓ^t. Let $k \subset L \subseteq K$ be an intermediate field such that $\mathrm{Gal}(L/k)$ is cyclic of order ℓ^t. We claim that L has all the desired properties.

The only property that is not immediate is that L/k is totally ramified at w and nowhere else. It is certainly unramified at every valuation $v \neq w$. Let $T \subseteq \mathrm{Gal}(L/k)$ be the ramification of any valuation above w in L and L_1 the fixed field of T. Then L_1 is unramified everywhere and so is a subfield of E. If $L_1 \neq k$ it would follow that ℓ divides $[E : k] = h_k$. This is contrary to assumption. Thus, $L_1 = k$ which proves L/k is totally ramified at w. Since $\deg w = 2n$ is prime to ℓ we can once agan invoke Ichimura's lemma to conclude that h_L is indivisible by ℓ. □

Theorem 3.6 and its corollary will be used in the proof of Corollary 1.3 to be given in Section 5.

4 Proofs of Main Results

We are now ready to prove Theorem 1.1. Let m be any positive integer $m > 1$ and ℓ an odd prime. Write $m = \ell^t m_1$ for integers t and m_1 with $\ell \nmid m_1$. Let m_0 be the square-free part of m_1, and fix a prime power q, sufficiently large, with $q \equiv 1 \pmod{m_0}$ and $q \equiv -1 \pmod{\ell}$. First, we prove the theorem for the case when $\ell \nmid m$.

Define rational functions $X_j(T)$ recursively as follows, $X_0(T) = T$ and

$$X_j = \frac{\mathcal{P}(X_{j-1})}{\mathcal{Q}(X_{j-1})} = r(X_{j-1}) \quad \text{for} \quad j \geq 1 \ , \tag{4}$$

where $\mathcal{P}$ and $\mathcal{Q}$ are defined as in Eq. 1. Note that $X_j = r^{(j)}(T)$, where the superscript (j) means to compose $r(T)$ with itself j times.

Recalling the Rikuna polynomial $F(X,u) = \mathcal{P}(X) - u\mathcal{Q}(X)$ we see that $F(X_{j-1}, X_j) = 0$. It follows from Theorem 1.4, and the remarks following, that $\mathbb{F}_q(X_{j-1})/\mathbb{F}_q(X_j)$ is a cyclic extension of degree ℓ, ramified only at the zero divisor of $X_j^2 - \omega X_j + 1$.

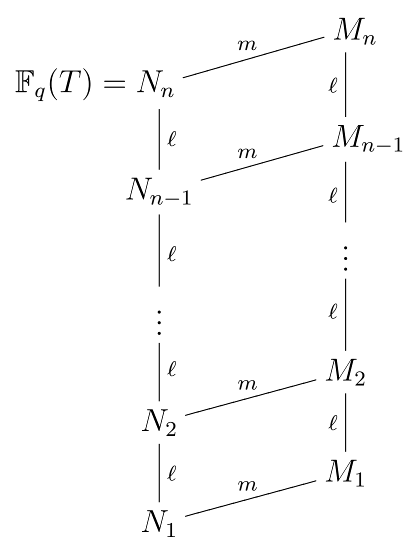
Now fix a positive integer $n \geq 1$, and for $1 \leq i \leq n$ define

$$N_i = \mathbb{F}_q(X_{n-i}) \quad \text{and} \quad M_i = N_i(\sqrt[m]{\ell X_n + \gamma}) \ .$$

Here $\gamma \in \mathbb{F}_q$ is chosen so that $X^m - (\ell\zeta + \gamma)$ is irreducible over $\mathbb{F}_q(\zeta)$ (see Lemma 2.3).

Note that $N_n = \mathbb{F}_q(T)$ and $M_n = \mathbb{F}_q(T)(\sqrt[m]{\ell X_n + \gamma})$. We will show that M_n is an extension of $\mathbb{F}_q(T)$ of degree m and that its class number is not divisible by ℓ. Further, the genus of M_n is a monotone increasing function of n. Thus, all the fields M_n are pairwise non-isomorphic. This will prove our theorem in the case that m is not divisible by ℓ.

We will see that for all i such that $1 \leq i \leq n-1$, $[N_{i+1} : N_i] = \ell$, $[M_{i+1} : M_i] = \ell$, and for all i, $[M_i : N_i] = m$. The field diagram is shown below.



Let

$$P_i = X_{n-i}^2 - \omega X_{n-i} + 1,$$

and let (P_i) denote the divisor of N_i corresponding to the zeros of P_i. Recall that $q \equiv -1 \pmod{\ell}$ which implies that $X^2 - \omega X + 1$ is irreducible over $\mathbb{F}_q$. Therefore, P_i is irreducible in $\mathbb{F}_q[X_{n-i}]$, and hence (P_i) is a prime divisor.

The idea of the proof of the main result is as follows. We will show that $\ell \nmid h_{M_1}$, and use Proposition 3.1 to conclude that $\ell \nmid h_{M_n}$. The next few lemmas show that Proposition 3.1

applies. Finally, we show that the M_n's are distinct, so there are infinitely many degree m extensions of $\mathbb{F}_q$ with class number indivisible by ℓ.

Lemma 4.1. *For each i, N_{i+1} is a $\mathbb{Z}/\ell\mathbb{Z}$-extension of N_i, totally ramified at (P_i), and unramified outside (P_i).*

Proof. By the remarks on the previous page, we see that N_{i+1} is a $\mathbb{Z}/\ell\mathbb{Z}$-extension of N_i. By Eq.(3), the discriminant is

$$\ell^\ell(4-\omega^2)^{(\ell-1)(\ell-2)/2}(X_{n-i}^2-\omega X_{n-i}+1)^{\ell-1} = \ell^\ell(4-\omega^2)^{(\ell-1)(\ell-2)/2}P_i^{\ell-1},$$

where $\ell^\ell(4-\omega^2)^{(\ell-1)(\ell-2)/2} \in \mathbb{F}_q^\times$. It is easy to see $\ell^\ell(4-\omega^2)^{(\ell-1)(\ell-2)/2} \neq 0$ since $\operatorname{char} \mathbb{F}_q \neq \ell$ and if $4-\omega^2=0$, then $\omega = \pm 2$. This implies that $\zeta+\zeta^{-1} = \pm 2$, so $\zeta = \pm 1$, a contradiction since $\ell \geq 3$.

Since any finite ramified prime would divide the discriminant, it follows that the only possible ramification is at P_i and at the prime at infinity. Note that the infinite prime has degree 1, so if (P_i) were unramified, then Riemann-Hurwitz implies that

$$2g_{N_{i+1}} - 2 = \ell(2g_{N_i}-2) + e_\infty - 1.$$

Since N_i and N_{i+1} are rational function fields, they both have genus 0. It follows that $e_\infty = 2\ell - 1$, which is impossible since the ramification index is at most the degree of the extension, which is ℓ in this case. So (P_i) must be ramified in N_{i+1}, and the ramification index is ℓ since the extension is Galois of prime degree ℓ. It follows that the infinite prime is unramified, because

$$-2 = -2\ell + (\ell-1)\deg(P_i) + e_\infty - 1 = -2\ell + 2\ell - 2 + e_\infty - 1 = e_\infty - 3.$$

So $e_\infty = 1$, as claimed. □

Lemma 4.2. *The extension M_i/N_i has degree m, and the prime (P_i) of N_i is inert in the extension M_i.*

Proof. Since $M_i = N_i(\sqrt[m]{\ell X_n + \gamma})$, it suffices to show that the minimal polynomial for $\sqrt[m]{\ell X_n + \gamma}$ over N_i is irreducible mod P_i. We will show that $X^m - (\ell X_n + \gamma)$ is irreducible mod P_i, which implies that $X^m - (\ell X_n + \gamma)$ is irreducible over N_i and thus must be the minimal polynomial for $\sqrt[m]{\ell X_n + \gamma}$ over N_i.

Let λ be the unique $\mathbb{F}_q$ - homomorphism from $\mathbb{F}_q[X_{n-i}]$ to $\mathbb{F}_q(\zeta)$ which takes X_{n-i} to ζ. It is clear that λ is onto and has as kernel the principal ideal generated by P_i. In the usual way, λ extends to a homomorphism from the localization R_i of $\mathbb{F}_q[X_{n-i}]$ at the prime ideal (P_i).

By definition, we know that $r^i(X_{n-i}) = X_n$. One easily checks that $r(\zeta) = \zeta$. Using these two facts and $\lambda(X_{n-i}) = \zeta$, one deduces that $\lambda(X_n) = \zeta$. The homomorphism λ extends in the obvious way to a homomorphism from $R_i[X]$ to $\mathbb{F}_q(\zeta)[X]$. This homomorphism takes $X^m - (\ell X_n + \gamma)$ to $X^m - (\ell\zeta + \gamma)$. Since the latter polynomial is irreducible by our choice of γ, the former one must be irreducible as well. This completes the proof. □

Lemma 4.3. *The polynomial $\mathcal{Q}(X) \in \mathbb{F}_q(X)$ is separable.*

Proof. It suffices to show that $\mathcal{Q}(X)$ and $\mathcal{Q}'(X)$ have no common roots, where $\mathcal{Q}'(X)$ is the formal derivative of $\mathcal{Q}(X)$. The derivative of $\mathcal{Q}(X)$ is given as follows:

$$\mathcal{Q}'(X) = \frac{\ell((X-\zeta)^{\ell-1} - (X-\zeta^{-1})^{\ell-1})}{\zeta^{-1}-\zeta}.$$

Let $\alpha \in \overline{\mathbb{F}_q}$ be a root of $\mathcal{Q}(X)$. Then, by definition of $\mathcal{Q}(X)$, we have $(\alpha-\zeta)^\ell = (\alpha-\zeta^{-1})^\ell$. Clearly, we cannot have $\alpha = \zeta$ or $\alpha = \zeta^{-1}$, because $\zeta - \zeta^{-1} \neq 0$. If α were also a root of $\mathcal{Q}'(X)$, then we would have $(\alpha-\zeta)^{\ell-1} = (\alpha-\zeta^{-1})^{\ell-1}$. So

$$(\alpha-\zeta)^\ell = (\alpha-\zeta^{-1})^\ell = (\alpha-\zeta)^{\ell-1}(\alpha-\zeta^{-1}).$$

Since $\alpha \neq \zeta$, then $\alpha - \zeta = \alpha - \zeta^{-1}$, implying that $\zeta = \zeta^{-1}$, a contradiction. □

Lemma 4.4. *The class number of M_1 is not divisible by ℓ.*

Proof. Recall that $M_1 = \mathbb{F}_q(X_{n-1})(\sqrt[m]{\ell X_n + \gamma})$. First, we claim that the genus of M_1 is $(\ell-1)(m-1)$. For ease of notation, let $Z = \sqrt[m]{\ell X_n + \gamma}$, so $M_1 = \mathbb{F}_q(X_{n-1})(Z)$. Notice that $M_1\overline{\mathbb{F}_q}$ is a degree m extension of $\overline{\mathbb{F}_q}(X_{n-1})$ with minimal polynomial

$$\begin{aligned} X^m - (\ell X_n + \gamma) &= X^m - \left(\frac{\ell\mathcal{P}(X_{n-1})}{\mathcal{Q}(X_{n-1})} + \gamma\right) \\ &= X^m - \frac{\ell\mathcal{P}(X_{n-1}) + \gamma\mathcal{Q}(X_{n-1})}{\mathcal{Q}(X_{n-1})} \\ &= X^m - \frac{F(X_{n-1}, -\gamma/\ell)}{\mathcal{Q}(X_{n-1})/\ell}. \end{aligned} \tag{5}$$

(Notice that the polynomial $X^m - (\ell X_n + \gamma)$ remains irreducible over $\overline{\mathbb{F}_q}$: if α is a zero, then it has multiplicity one; then, in the local ring at $X_{n-1} - \alpha$ the polynomial in question is Eisenstein and so, irreducible.) The discriminant of $F(X, -\gamma/\ell)$ is $\ell^{-(\ell-2)}(4-\omega^2)^{(\ell-1)(\ell-2)/2}(\gamma^2 + \ell\omega\gamma + \ell^2)$ by Eq.(3). This must be non-zero, otherwise $P_1(-\gamma/\ell) = (\gamma^2 + \omega\gamma\ell + \ell^2)/\ell^2 = 0$. But $-\gamma/\ell \in \mathbb{F}_q$, and P_1 is irreducible over $\mathbb{F}_q$, a contradiction. So $F(X_{n-1}, -\gamma/\ell)$ has non-zero discriminant, and hence no multiple roots. By Lemma 4.3, $\mathcal{Q}(X)$ has no multiple roots.

Finally, $F(X, -\gamma/\ell)$ and $\mathcal{Q}(X)$ must be relatively prime. Otherwise, for some $\alpha \in \overline{\mathbb{F}_q}$, we would have

$$\mathcal{Q}(\alpha) = 0 = F(\alpha, -\gamma/\ell) = \mathcal{P}(\alpha) + (\gamma/\ell)\mathcal{Q}(\alpha).$$

It easily follows from the last equality that $\mathcal{P}(\alpha) = 0$. Thus $X - \alpha$ is a common factor of $\mathcal{P}(X)$ and $\mathcal{Q}(X)$ which contradicts the irreducibility of $F(X, u)$.

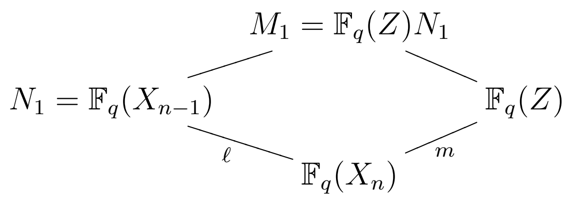
Hence, the numerator of the constant term in Eq.(5) has ℓ distinct roots, each corresponding to a prime that is totally ramified in $M_1\overline{\mathbb{F}_q}$. Similarly, the denominator of the constant term in Eq.(5) has $\ell - 1$ distinct roots, each corresponding to a prime that is totally ramified in $M_1\overline{\mathbb{F}_q}$. Finally, it is clear that the infinite prime is totally ramified in $M_1\overline{\mathbb{F}_q}$. Since $F(X, -\gamma/\ell)$ and $\mathcal{Q}(X)$ are relatively prime, then these 2ℓ primes are all distinct. Now

$\operatorname{char} \mathbb{F}_q \nmid m$, and so each of these primes is tamely ramified in $M_1\overline{\mathbb{F}_q}$. No other primes can be ramified since no other primes can divide the discriminant of $X^m - (\ell X_n + \gamma)$. Each of the ramified primes has degree 1, so Riemann-Hurwitz implies that

$$\begin{aligned} 2g_{M_1\overline{\mathbb{F}_q}} - 2 &= m(2g_{\overline{\mathbb{F}_q}(X_{n-1})} - 2) + \sum_{\mathfrak{p}} (e(\mathfrak{p}) - 1)\deg(\mathfrak{p}) \\ &= -2m + 2\ell(m-1) = 2(\ell-1)(m-1) - 2, \end{aligned}$$

and thus $g_{M_1\overline{\mathbb{F}_q}} = (\ell-1)(m-1)$, as claimed.

Next, we claim that $M_1 = \mathbb{F}_q(Z)(X_{n-1})$ is a $\mathbb{Z}/\ell\mathbb{Z}$-extension of $\mathbb{F}_q(Z)$. We know that N_1 is a $\mathbb{Z}/\ell\mathbb{Z}$-extension of $\mathbb{F}_q(X_n)$ and $\mathbb{F}_q(Z)$ is a degree m extension of $\mathbb{F}_q(X_n)$. (See figure below.)



Since $(\ell, m) = 1$, then $M_1 = \mathbb{F}_q(Z)N_1$ is a $\mathbb{Z}/\ell\mathbb{Z}$-extension of $\mathbb{F}_q(Z)$. Thus, the minimal polynomial for X_{n-1} over $\mathbb{F}_q(Z)$ must be $F(X, X_n) = F(X, (Z^m - \gamma)/\ell)$. The discriminant of this polynomial is, by Eq.(3),

$$(4-\omega^2)^{(\ell-1)(\ell-2)/2}\ell^\ell(X_n^2 - \omega X_n + 1)^{\ell-1} = (4-\omega^2)^{(\ell-1)(\ell-2)/2}\ell^{\ell-2(\ell-1)}((Z^m-\gamma)^2 - \ell\omega(Z^m-\gamma) + \ell^2)^{\ell-1}.$$

Let (Q) be the divisor corresponding to

$$Q = (Z^m - \gamma)^2 - \ell\omega(Z^m - \gamma) + \ell^2 \in \mathbb{F}_q(Z).$$

We will show that M_1 is ramified only at the single prime (Q) of $\mathbb{F}_q(Z)$, where $\ell \nmid 2m = \deg(Q)$. This completes the proof, by Proposition 3.1, since ℓ does not divide the class number of the rational function field $\mathbb{F}_q(Z)$. Notice that Q is irreducible over $\mathbb{F}_q$; if α is a root of Q in some extension of $\mathbb{F}_q$, then $(\alpha^m - \gamma)/\ell$ is a root of $X^2 - \omega X + 1$, the minimal polynomial of $\zeta^{\pm 1}$ over $\mathbb{F}_q$. So $(\alpha^m - \gamma)/\ell = \zeta^{\pm 1}$. Since $X^m - (\ell\zeta^{\pm 1} + \gamma)$ is irreducible over $\mathbb{F}_q(\zeta^{\pm 1})$, we have $[\mathbb{F}_q(\alpha) : \mathbb{F}_q(\zeta^{\pm 1})] = m$, and so

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q(\zeta^{\pm 1})][\mathbb{F}_q(\zeta^{\pm 1}) : \mathbb{F}_q] = m \cdot 2 = 2m,$$

which proves that Q must be irreducible over $\mathbb{F}_q$. Thus the divisor (Q) is indeed prime. Since (Q) is the only prime of $\mathbb{F}_q(Z)$ that divides the discriminant of the minimal polynomial of X_{n-1} over $\mathbb{F}_q(Z)$, only (Q) and the prime at infinity could be ramified. Assume (Q) is not ramified. By Riemann-Hurwitz, we get

$$2(\ell-1)(m-1) - 2 = (e_\infty - 1) - 2\ell,$$

so $e_\infty = 2\ell m - 2m + 1 > \ell$, a contradiction. So (Q) is ramified (totally ramified since the extension is Galois and has prime degree ℓ) in M_1. To see that M_1 is ramified at no other primes of $\mathbb{F}_q(Z)$, we again use the Riemann-Hurwitz formula (each sum is over all primes $\mathfrak{p} \neq (Q)$):

$$\begin{aligned} 2(\ell-1)(m-1)-2 &= \ell(-2)+(\ell-1)\deg(Q)+\sum_{\mathfrak{p}}(e_{\mathfrak{p}}-1)\deg(\mathfrak{p}) \\ &= (\ell-1)(2m)-2(\ell-1)-2+\sum_{\mathfrak{p}}(e_{\mathfrak{p}}-1)\deg(\mathfrak{p}) \\ &= 2(\ell-1)(m-1)-2+\sum_{\mathfrak{p}}(e_{\mathfrak{p}}-1)\deg(\mathfrak{p}). \end{aligned}$$

Thus, all other primes must be unramified. □

Proof of Theorem 1.1. Assume that $\ell \nmid m$. Notice that $M_{i+1} = M_i N_{i+1}$, so by Lemma 4.1, M_{i+1} is a $\mathbb{Z}/\ell\mathbb{Z}$-extension of M_i. Also by Lemma 4.1, M_{i+1} is totally ramified at the prime in M_i lying over (P_i) and unramified everywhere else. By Lemma 3.1, $\ell \nmid h_{M_i}$ implies that $\ell \nmid h_{M_{i+1}}$. From Lemma 4.4, we see that $\ell \nmid h_{M_1}$. Therefore, ℓ does not divide $h_{M_2}, h_{M_3}, ..., h_{M_n}$. Hence, M_n has class number indivisible by ℓ.

To show that there are infinitely many such fields, we prove that each M_n has genus $(\ell^n-1)(m-1)$, so the fields are pairwise non-isomorphic. It was shown in Lemma 4.4 that the genus of M_1 is $(\ell-1)(m-1)$. Since M_{i+1}/M_i is totally ramified at a single prime in M_i, denoted here by $\mathfrak{P}_i$, lying over (P_i) in N_i. Since (P_i) is inert in M_i, $\mathfrak{P}_i$ has degree $2m$ in M_i. Note that M_n has degree ℓ^{n-1} over M_1, so by Riemann-Hurwitz,

$$\begin{aligned} 2g_{M_n}-2 &= \ell^{n-1}(2g_{M_1}-2)+(\ell^{n-1}-1)(\deg(\mathfrak{P}_1)) \\ &= \ell^{n-1}(2\ell m-2\ell-2m+2-2)+2\ell^{n-1}m-2m \\ &= \ell^{n-1}(2\ell m-2\ell)-2m \\ &= 2\ell^n(m-1)-2(m-1)-2 \\ &= 2(\ell^n-1)(m-1)-2. \end{aligned}$$

Therefore, it follows that $g_{M_n} = (\ell^n-1)(m-1)$.

Now we consider the general case. Write $m = \ell^t m_1$, where $\ell \nmid m_1$, and let m_0 be the square-free part of m_1. Since $\ell \nmid m_1$, the results above show that we have infinitely many extensions K_1 of degree m_1 over $\mathbb{F}_q(T)$ with $\ell \nmid h_{K_1}$. Note that the constant field of K_1 is $\mathbb{F}_q$, as K_1 is one of the fields M_n. This field is at the top of a tower of totally ramified extensions. At the bottom, M_1/N_1 is totally ramified at $X_{n-1}-\alpha$. Also, we know M_{i+1}/M_i is totally ramified at the prime of M_i above (P_i). At a totally ramified prime, the relative degree must be 1. So, in a tower of totally ramified extensions, the constant field at the top must be the same as the constant field at the bottom.

Since $q \equiv -1 \pmod{\ell}$, Theorem 3.6 implies that there are infinitely many non-isomorphic geometric extensions K of degree ℓ^t over K_1 with $\ell \nmid h_K$. Thus we have infinitely many extensions K of degree m over $\mathbb{F}_q(T)$ with $\ell \nmid h_K$, as claimed. □

5 Corollaries

We are now in a position to prove Corollaries 1.2 and 1.3 which are stated in the introduction. We reproduce them here for the convenience of the reader.

Corollary 1.2. *Suppose m is indivisible by ℓ and that $q \equiv 1 \pmod{m}$. If, in addition, $q \equiv -1 \pmod{\ell}$, there are infinitely many geometric and cyclic extensions K of $\mathbb{F}_q(T)$ such that $\ell \nmid h_K$.*

Proof. In the course of proving Theorem 1.1, we have shown that the following field extensions, $M_n = k(\sqrt[m]{\ell X_n + \gamma})$ have degree m and class number indivisible by ℓ. If $q \equiv 1 \pmod{m}$, then the base field contains a primitive m-th root of unity. This implies M_n is a Kummer, and thus cyclic, extension of k of degree m. □

Corollary 1.3. *Suppose $t \geq 1$ and $m = \ell^t m_1$ with m_1 not divisible by ℓ. If $q \equiv 1 \pmod{m_1}$ and $q \equiv -1 \pmod{\ell^t}$, then there are infinitely many geometric and cyclic extensions K of degree m over $\mathbb{F}_q(T)$ such that $\ell \nmid h_K$.*

Proof. By Corollary 1.2 above, there are infinitely many cyclic extensions K_1 of degree m_1 over k with class number indivisible by ℓ. By the corollary to Proposition 3.6 and its proof, we can find a valuation w of k of large even degree and a geometric and cyclic extension L/k of degree ℓ^t which is totally ramified at w and unramified elsewhere. We still have a lot of flexibility in the choice of w. Let's choose it so that $\deg w$ is prime to ℓ, w is unramified in K_1, and $\mathrm{Frob}(w)$ is a cyclic generator of $\mathrm{Gal}(K_1/k)$. This is possible by the Tchebotarev density theorem (see [35], Proposition 9.13B). To apply this result we need to know K_1/k is a geometric extension. In fact, K_1 is geometric over k because it is generated by the m-th root of a non-constant rational function (this is an exercise). With this choice, w is inert in K_1. Let W be the unique valuation of K_1 lying above w. Since $f(W/w) = m_1$, we have $\deg W = m_1 \deg w$ which is prime to ℓ.

We claim that $K = LK_1$ is a field with all the properties required. First of all, it is clear that $K_1 \cap L = k$. It follows that K is a cyclic extension of degree $l^t m_1 = m$. Next, notice that w is totally ramified in L and unramified in K_1. It follows that W is totally ramified in K. Also, no other valuation of K_1 is ramified in K. If we knew that K/K_1 was a geometric extension, we could invoke Ichimura's lemma one more time to deduce that h_L is indivisible by ℓ. We conclude the proof by showing that, indeed, K/K_1 is a geometric extension.

Let $\mathbb{E}$ be the constant field of K. The field $\mathbb{E}$ injects into the residue class field of the valuation above W in K. This is equal to the residue class field of W since K/K_1 is totally ramified. We have shown $\deg W = m_1 \deg w$ which is prime to ℓ. Thus $[E : F]$ is prime to ℓ. On the other hand, $\mathbb{E} \cap K_1 = \mathbb{F}$ since K_1/k is geometric. It follows that $[\mathbb{E} : \mathbb{F}]$ divides $[K : K_1]$ which is a power of ℓ. One concludes that $[\mathbb{E} : \mathbb{F}] = 1$. The corollary is proved. □

6 Appendix

The theorem on indivisibility by a prime ℓ of the class number of extensions of $\mathbb{F}_q(T)$ of degree m is dependent on the assumption that q is a sufficiently big prime power satisfying $q \equiv -1 \pmod{\ell}$ and $q \equiv 1 \pmod{m_o}$, where m_o is the squarefree part of m. This is equivalent to a single congruence $q \equiv -1 + 2\ell\ell' \pmod{\ell m_o}$, where ℓ' is a multiplicative inverse of ℓ modulo m_o. We look into the the question of how big q has to be in order for the theorem to be valid. If q lies in this arithmetic progression and is big enough to make the main theorem valid, we say that q is admissible.

The number of rational points on the curve $y^2 = x^k - d$ over $\mathbb{F}_q$ satisfies $|N_k - q| \leq (k-1)\sqrt{q}$ if k is odd, and $\leq 1 + (k-1)\sqrt{q}$ if k is even (see Theorem 5 of Chapter 8 in [13]). The theorem there is stated over the prime field, but the proof work over any finite field. We will work with the slightly weaker, but uniform, inequality $|N_k - q| < k\sqrt{q}$. Also, for the set S_k we have shown $|\#(S_k) - N_k/2k| < 2$. Let's write $N_k = q + \delta_1(k)k\sqrt{q}$ and $\#(S_k) = N_k/2k + 2\delta_2(k)$ where $|\delta_1(k)|$ and $|\delta_2(k)|$ are both less than 1. Putting these two inequalities together, we find

$$\#(S_k) = \frac{q}{2k} + \frac{\delta_1(k)}{2}\sqrt{q} + 2\delta_2(k) \ . \tag{6}$$

Earlier in this paper, we showed that

$$\#(T') = -\sum_{1<k|m} \mu(k)\#(S_k) \ .$$

Thus, since $\#(T') + \#(T) = (q+1)/2$, we have

$$\#(T) = \frac{q+1}{2} + \sum_{1<k|m} \mu(k)\#(S_k) \ . \tag{7}$$

Using Eq. (6) and substituting into Eq. (7), yields

$$\#(T) = \frac{q}{2} + \frac{1}{2} + \frac{q}{2}\sum_{1<k|m} \frac{\mu(k)}{k} + \sum_{1<k|m} \frac{\mu(k)\delta_1(k)}{2}\sqrt{q} + 2\sum_{1<k|m} \mu(k)\delta_2(k) \ . \tag{8}$$

Combining the first and third terms, simplifies to the following main term

$$\frac{q}{2}\prod_{p|m}(1 - \frac{1}{p}) = \frac{q}{2}\frac{\phi(m_o)}{m_o} \ .$$

To go further, we need the simple observation that $\sum_{k|m} |\mu(k)| = \sum_{r=0}^{t} \binom{t}{r} = 2^t$, where t is the number of primes dividing m. Since both $\delta_1(k)$ and $\delta_2(k)$ have absolute value less than 1, the sum of the second, fourth, and fifth terms of Eq. (8) are bounded above by $2^{t-1}\sqrt{q} + 2^{t+1}$.

Putting all this together, we have

$$|\#(T) - \frac{q}{2}\frac{\phi(m_o)}{m_o}| \leq 2^{t-1}\sqrt{q} + 2^{t+1} \ .$$

Thus, to insure that T is not empty, it suffices to insure that

$$q > \frac{2^t m_o}{\phi(m_o)}\sqrt{q} + 4\frac{2^t m_o}{\phi(m_o)} \ .$$

Set $C = 2^t m_o/\phi(m_o)$. The condition can now be written as

$$q > C\sqrt{q} + 4C \ . \tag{4}$$

Let $f(x) = x^2 - Cx - 4C$. The largest zero, x_o, of $f(x)$ is given by $2x_o = C + \sqrt{C^2 + 16C}$. Thus, x_o is less than $C + 4$. Equation (4) is satisfied if $f(\sqrt{q}) > 0$, and this is certainly the case if $\sqrt{q} > C + 4$ since $f(x)$ is easily seen to be increasing at x_o and beyond. We have proved

Proposition 6.1. *Let $C = 2^t m_o/\phi(m_o)$. A prime power q is admissible if $q > (C + 4)^2$.*

It is important to point out that this condition is sufficient but not necessary. We have made a number of somewhat coarse estimates during the derivation. For example, in the case where $\ell = 3$ and $m = m_o = 2$ (the case considered by Ichimura), every q such that $q \equiv -1 \pmod 3$ is admissible, whereas the Proposition requires $q > 16$. Nevertheless, the estimate is strong enough to give some surprising consequences, taking into account the fact that we are looking at q lying in the arithmetic progression $A(\ell, m_o)$ defined by $q \equiv -1 + ll' \pmod{\ell m_o}$. Every q in this progression, except possibly the smallest positive element, is greater than ℓm_o. Thus, if $\ell m_o \geq (C + 4)^2$, every possible q in this progression with perhaps one exception is admissible. We investigate two special cases.

Corollary 6.2. *Let's suppose $m_o = p$, a prime. If $p \geq 13$ then every prime power q in $A(\ell, m_o)$ is admissible with at most one exception.*

Proof. If $p \geq 13$, we claim that $\ell p \geq (C + 4)^2$ for any odd prime ℓ. First, let's write out this condition explicitly:

$$\ell p \geq (\frac{2p}{p-1} + 4)^2 = 4(\frac{p^2}{(p-1)^2} + \frac{4p}{p-1} + 4) \ .$$

Dividing both sides by $4p$, yields

$$\frac{\ell}{4} \geq \frac{p}{(p-1)^2} + \frac{4}{p-1} + \frac{4}{p} \ .$$

For $p \geq 13$, the right hand side is less than .74, so the inequality is satisfied if ℓ is greater than 2.96. Since ℓ is an odd prime, this condition is always satisfied. □

Corollary 6.3. *Suppose m_o is divisible by two or more primes and that the smallest prime dividing m_o is greater than or equal to 7. Then every prime power q in $A(\ell, m_o)$ is admissible with at most one exception.*

Proof. The condition we need is

$$\ell m_o \geq 16(\frac{2^{t-2}m_o}{\phi(m_o)} + 1)^2 \ .$$

Dividing both sides by $16m_o$ and simplifying yields

$$\frac{\ell}{16} \geq \frac{2^{2t-4}m_o}{\phi(m_o)^2} + \frac{2^{t-1}}{\phi(m_o)} + \frac{1}{m_o} \ .$$

If the right hand side of this inequality were less than or equal to 3/16 this would hold for all odd primes, and the corollary would follow.

An elementary argument shows if $t \geq 2$ the largest value of the right hand side occurs for $m_0 = 77 = 7 \cdot 11$. In this case the right hand side is

$$\frac{77}{60^2} + \frac{2}{60} + \frac{1}{77} \approx .0677 \ ,$$

which is comfortably less than 3/16. □

References

[1] T. Azuhata and H. Ichimura, *On the divisibility problem of the class numbers of algebraic number fields*, *J. Fac. Sci. Univ. Tokyo*, **30** (1984) 579-585.

[2] B. Datskovsky and D. Wright, *Density of discriminants of cubic extensions*, J. reine angew. Math. **386** (1988), 116-138.

[3] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Royal Soc. A, **322** (1971), 405-420.

[4] D. Cardon and R. Murty, *Exponents of class groups of quadratic function fields over finite fields*, Canad. Math. Bulletin, Vol. 44 (4) (2001) pp. 398-407.

[5] J. Esmonde and M. Murty, *Problems in algebraic number theory*, Springer-Verlag, New York, 2005.

[6] C. Friesen, *Class number divisibility in real quadratic function fields*, Canad. Math. Bull. **35** (1992), 361-370.

[7] A. Fröhlich and M. Taylor, *Algebraic number theory*, Cambridge University Press, Cambridge, 1991.

[8] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class numbers are not divisible by three*, J. Number Theory **6** (1976), 276-278.

[9] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields,* Invent. Math. **88** (1987), 31-38.

[10] K. Horie, *Trace formulae and imaginary quadratic fields,* Math. Ann. **288** (1990), 605 - 612.

[11] K. Horie and Y. Onishi, *The existence of certain infinite families of imaginary quadratic fields*, J. Reine und ange. Math. **390** (1988), 97 - 133.

[12] H. Ichimura, *Quadratic function fields whose class numbers are not divisible by three*, Acta Arith. **91** (1999), 181-190.

[13] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd edition, Springer, 1998.

[14] N. Jochnowitz, *Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves*, unpublished.

[15] C. Jordan, *Recherches sur les substitutions*, J. Liouville **17** (1872), 351-367.

[16] I. Kimura, *On class numbers of quadratic extensions over function fields*, Manuscripta Math. **97** (1998), 81-91.

[17] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387 - 398.

[18] Komatsu, Toru. *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), no. 3, 265-279.

[19] S. Lang, *Algebra*, 2nd edition, Addison-Wesley, Reading, MA, 1984.

[20] Y. Lee, *The structure of the class groups of global function fields with any unit rank*, J. Ramanujan Math. Soc. **20** (2005), 1 - 21.

[21] Y. Lee and A. Pacelli, *Subgroups of the class groups of global function fields: the inert case*, Proc. Amer. Math. Soc., **133** (2005), 2883-2889.

[22] Y. Lee and A. Pacelli, *Higher rank subgroups in the class groups of imaginary function fields*, Journal of Pure and Applied Algebra, 207 (2006), 51 - 62.

[23] H.W. Lenstra and P. Stevenhagen, *Chebotarëv and his density theorem*, Math Intelligencer **18** (1996), 26-37.

[24] D. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[25] R. Murty, *Exponents of class groups of quadratic fields*, Topics in Number Theory (University Park, PA, 1997), Math. Appl., **467**, *Kluwer Acad. Publ., Dordrecht*, (1999), 229-239.

[26] T. Nagell, *Uber die Klassenzahl imaginar quadratischer Zahlkorper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140-150.

[27] S. Nakano, *On ideal class groups of algebraic number fields*, J. Reine Angew. Math., **358** (1985), 61-75.

[28] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compos. Math. **119** (1999), 1 - 11.

[29] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo l*, Ann. Math. **147**, No. 2 (1998), 451-468.

[30] A. M. Pacelli, *Abelian subgroups of any order in class groups of global function fields*, J. Number Theory, **106**, (2004), 29 - 49.

[31] A. M. Pacelli, *The prime at infinity and the rank of the class group of global function fields*, J. Number Theory, **116** (2006), 311 - 323.

[32] A. M. Pacelli and M. Rosen, *Indivisibility of class numbers of global function fields*, Acta Arith. 138 (2009), 269-287.

[33] Y. Rikuna, *On simple families of cyclic polynomials*, Proceedings of the American Mathematical Society **130** (2002), no. 8, 2215-2218.

[34] M. Rosen, *The Hilbert class field in function fields*, Expo. Math. **5** (1987), 365-378.

[35] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, 2002.

[36] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137 - 1157.

[37] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48**, No. 177 (1987), 371-384.

[38] P. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory, **5** (1973), 237-241.

[39] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57-76.

Allison M. Pacelli, Williams College, Williamstown, MA 01267 apacelli@williams.edu

Michael Rosen, Brown University, Providence, RI 02906 mrosen@math.brown.edu