ACTA ARITHMETICA
138.3 (2009)

Indivisibility of class numbers of global function fields

by

Allison M. Pacelli (Williamstown, MA) and
Michael Rosen (Providence, RI)

1. Introduction. It is well known that infinitely many quadratic number fields and function fields have class number divisible by a given integer n (see Nagell [21] for imaginary number fields, Yamamoto [29] or Weinberger [28] for real number fields, and Friesen [7] for function fields). In fact, given any integers m and n, there are infinitely many fields of fixed degree m with class number divisible by n (see for example Azuhata and Ichimura [3] or Nakano [22] for number fields and the first author [25, 26] for function fields). Less is known, however, about the indivisibility of class numbers of global fields. 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 pth 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 [9] showed that infinitely many imaginary quadratic number fields have class number not divisible by 3. The analogous result for function fields was proven in 1999 by Ichimura [14]. Horie and Onishi [11, 12, 13], Jochnowitz [15], and Ono and Skinner [24] 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 [6], Datskovsky and Wright [4], and Kimura [17] (for relative class numbers). Kohnen and Ono made further progress in [18]. 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

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

2000 *Mathematics Subject Classification*: 11R29, 11R58.
Key words and phrases: class group, class number, function field.

DOI: 10.4064/aa138-3-4

As usual, less is known about class numbers in real quadratic fields, but in 1999, Ono [23] 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 [14] constructed an explicit infinite family of quadratic function fields with class number not divisible by 3. Moreover, Achter [1, 2] has determined the probability that a particular type of quadratic function field has class number indivisible by a prime ℓ. In this paper, we give a generalization of Ichimura's work, constructing, for a large class of q, infinitely many function fields of any degree m, $3 \nmid m$, over $\mathbb{F}_q(T)$ with class number indivisible by 3.

As in [14], the fields above 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 $3 \nmid h_{M_1}$, N_{i+1}/N_i is cyclic, cubic, and ramified at exactly one prime, M_i/N_i is a degree m extension, 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 $3 \nmid h_{M_i}$ 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 3.

Let q be a power of an odd prime, and $\mathbb{F}_q$ the finite field with q elements.

The main result is as follows:

THEOREM 1. *Let $m > 1$ be any positive integer with $3 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 3.*

The density of the fields constructed is at least $1/m$ if $4 \nmid m$. We will say more about this later. Also note that if the divisor class number is not divisible by 3, then the ideal class number must also be indivisible by 3 since the ideal class group is a quotient of the class group of divisors of degree 0.

In Section 2, we will prove the main result, assuming the existence of a positive density of primes (and prime powers) q that satisfy certain necessary properties. We should note that the proof of Theorem 1 is fairly short; a good deal of the paper is concerned with proving the existence of such q. The following theorem, which is a fairly straightforward application of the Frobenius density theorem, will be very useful to us. We will give a proof in Section 3.

THEOREM 2. *Let $f_1, \ldots, f_t$ be irreducible polynomials in $\mathbb{Z}[x]$ with splitting fields $K_1, \ldots, K_t$. Let G_i denote the Galois group of K_i over $\mathbb{Q}$. Suppose that $G_1 \times \cdots \times G_t$ is the Galois group of the composite field $K_1 \cdots K_t$. For each i, let d_i be a possible decomposition type of f_i. Then there are infinitely many primes q such that each f_i decomposes modulo q with decomposition type d_i.*

In Section 4, we use Theorem 2 to show that for any given m, there are a positive density of primes q for which Theorem 1 holds. Furthermore, for each such q satisfying the hypotheses, q^r satisfies the hypotheses as well if r is odd and $(r, m) = 1$.

Finally, we note that it appears likely that the main result can be extended to construct, subject to certain conditions on q, infinitely many extensions of degree m of $\mathbb{F}_q(T)$, whose class number is indivisible by a given odd prime ℓ. This is current work [5] with Daub, Lang, Merling, and Pitiwan.

2. Proof of Theorem 1. Let ζ denote a root of the polynomial $X^2 + X + 1 \in \mathbb{F}_q[X]$. We prove the main result under the assumption that for any fixed positive integer $m > 1$ with $3 \nmid m$, there are a positive density of primes q such that

(i) $q \equiv 2 \pmod 3$, $q \nmid m$,
(ii) there exists $\gamma \in \mathbb{F}_q^\times$ such that $\gamma + 3\zeta$ is not a pth power in $\mathbb{F}_q(\zeta)$ for all primes p dividing m, and
(iii) if $4 \mid m$, then $\gamma + 3\zeta \notin -4\mathbb{F}_q(\zeta)^4$.

We will see that (ii) and (iii) together are equivalent to the assertion that $X^m - (\gamma + 3\zeta)$ is irreducible over $\mathbb{F}_q(\zeta)$. We will prove the following.

THEOREM 3. *Let $m > 1$ be any positive integer with $3 \nmid m$. If q is a prime satisfying conditions* (i)–(iii) *above, then there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number not divisible by $n = 3$.*

Let T be any transcendental element over $\mathbb{F}_q$, so that $\mathbb{F}_q(T)$ is the rational function field. As in [14], we define rational functions $X_n(T)$ recursively as follows:

$$X_0 = T, \quad X_j = \frac{X_{j-1}^3 - 3X_{j-1} - 1}{3(X_{j-1}^2 + X_{j-1})} \quad \text{for } j \geq 1. \tag{1}$$

Note that $X_j(T)$ has degree 3^j.

Given $\gamma \in \mathbb{F}_q^\times$ satisfying (ii) above, let $L_n = \mathbb{F}_q(T)(\sqrt[m]{3X_n + \gamma})$. We will see that $X^m - (3X_n + \gamma)$ is irreducible over $\mathbb{F}_q$, so up to isomorphism, it does not matter which mth root we choose. We will show that for all positive integers n, the divisor class number of L_n is not divisible by 3, and that the L_n are pairwise nonisomorphic.

Fix $n \geq 1$. For $1 \leq i \leq n$, define

$$N_i = \mathbb{F}_q(X_{n-i}), \quad M_i = \mathbb{F}_q(X_{n-i}, \sqrt[m]{3X_n + \gamma}).$$

It follows from (1) that

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n = \mathbb{F}_q(T) \quad \text{and} \quad M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = L_n.$$

We will see that M_i has degree m over N_i for each i. Let

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

and let (P_i) denote the divisor of N_i corresponding to the zeros of P_i. Since $q \equiv 2 \pmod 3$, we see that P_i is irreducible over $\mathbb{F}_q$, so (P_i) is a prime divisor.

The following lemma is a function field analogue of a well-known result from class field theory. See [14] for a proof.

LEMMA 1. *Let l be a prime, K a finite l-Galois extension of k, and suppose that exactly one prime divisor $\mathfrak{P}$ of K is ramified over k and $l \nmid \deg(\mathfrak{P})$. If $l \mid h_K$, then $l \mid h_k$.*

The following lemma is also well-known (a proof can be found in [19]).

LEMMA 2. *Let k be a field, m an integer ≥ 2, and $a \in k$, $a \neq 0$. 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 $k[x]$.*

LEMMA 3. *For each i, N_{i+1} is a cyclic, cubic extension of N_i, totally ramified at (P_i), and unramified outside (P_i).*

Proof. Notice that $N_{i+1} = N_i(X_{n-i-1})$, and we claim that the minimal polynomial for X_{n-i-1} over N_i is

$$H(X) = X^3 - 3X_{n-i}X^2 - 3(X_{n-i} + 1)X - 1.$$

Note that the polynomial is irreducible because any root in $\mathbb{F}_q(X_{n-i})$ would have to divide -1 and thus be a nonzero constant. But if a constant $a \in \mathbb{F}_q^\times$ were a root, then

$$a^3 - 3X_{n-i}a^2 - 3(X_{n-i} + 1)a - 1 = 0.$$

This implies that

$$X_{n-i} = \frac{a^3 - 3a - 1}{3a^2 + 3a},$$

contradicting the fact that $X_{n-i} \notin \mathbb{F}_q$ unless $a = -1$. It is easy to check, however, that -1 is not a root. Thus the cubic $H(X)$ is, in fact, the minimal polynomial for N_{i+1} over N_i.

Shanks proved in [27] that the discriminant of the polynomial $X^3 - aX^2 - (a+3)X - 1$ is $(a^2 + 3a + 9)^2$. It follows that the discriminant of H above is $81(X_{n-i}^2 + X_{n-i} + 1)^2 = 81P_i^2$, so N_{i+1} is a cyclic extension of N_i. Hence the only possible ramification occurs at (P_i) and the prime at infinity. Note that the infinite prime has degree 1, so if (P_i) were unramified, then the Riemann–Hurwitz formula implies that

$$2g_{N_{i+1}} - 2 = 3(2g_{N_i} - 2) + e_\infty - 1.$$

Since N_i and N_{i+1} have genus 0, it follows that $e_\infty = 5$, which is impossible. So (P_i) must be ramified in N_{i+1}, and the ramification index is 3, since the extension is Galois. It follows that the infinite prime is unramified, because

$$-2 = -6 + 2\deg(P_i) + e_\infty - 1 = -3 + e_\infty. \ \blacksquare$$

LEMMA 4. *The prime (P_1) of N_1 is inert in the extension M_1.*

Proof. Since $M_1 = N_1(\sqrt[m]{3X_n + \gamma})$, it suffices to show that the minimal polynomial for $\sqrt[m]{3X_n + \gamma}$ over N_1 is irreducible modulo P_1. We will show that $X^m - (3X_n + \gamma)$ is irreducible modulo P_1, which implies that $X^m - (3X_n + \gamma)$ is irreducible over N_1 and thus must be the minimal polynomial for $\sqrt[m]{3X_n + \gamma}$ over N_1. The result follows.

Note that since P_1 is irreducible over $\mathbb{F}_q$, we have

$$\mathbb{F}_q[X]/(P_1(X)) \cong \mathbb{F}_q(\zeta),$$

so $X_{n-1} \equiv \zeta \pmod{P_1}$. By (1),

$$\begin{aligned} 3X_n + \gamma &\equiv \frac{X_{n-1}(X_{n-1}^2 - 3) - 1}{X_{n-1}^2 + X_{n-1}} + \gamma \pmod{P_1} \\ &\equiv \frac{X_{n-1}(-X_{n-1} - 4) - 1}{-1} + \gamma \pmod{P_1} \\ &\equiv -X_{n-1} - 1 + 4X_{n-1} + 1 + \gamma \pmod{P_1} \equiv 3X_{n-1} + \gamma \pmod{P_1}. \end{aligned}$$

Thus, $X^m - (3X_n + \gamma) \equiv X^m - (3X_{n-1} + \gamma) \equiv X^m - (3\zeta + \gamma) \pmod{P_1}$. By Lemma 2 and conditions (ii) and (iii) we see that the polynomial $X^m - (3\zeta + \gamma)$ is irreducible over $\mathbb{F}_q(\zeta)$. Thus $X^m - (3X_n + \gamma)$ is irreducible modulo P_1, as claimed. $\blacksquare$

LEMMA 5. *The class number of M_1 is not divisible by* 3.

Proof. Recall that $M_1 = \mathbb{F}_q(X_{n-1})(\sqrt[m]{3X_n + \gamma})$. First, we claim that the genus of M_1 is $2m - 2$. For ease of notation, let $Z = \sqrt[m]{3X_n + \gamma}$, 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

$$\begin{aligned} X^m - (3X_n + \gamma) &= X^m - \left(\frac{X_{n-1}^3 - 3X_{n-1} - 1}{X_{n-1}^2 + X_{n-1}} + \gamma\right) \\ &= X^m - \frac{X_{n-1}^3 + \gamma X_{n-1}^2 - (3 - \gamma)X_{n-1} - 1}{X_{n-1}^2 + X_{n-1}}. \end{aligned} \tag{2}$$

It is not hard to see that X_{n-1}, $X_{n-1} + 1$, and infinity are totally ramified in $M_1\overline{\mathbb{F}}_q$. Notice that the numerator $X_{n-1}^3 + \gamma X_{n-1}^2 - (3 - \gamma)X_{n-1} - 1$ has three distinct roots since the discriminant of the polynomial

$$U^3 + \gamma U^2 - (3 - \gamma)U - 1$$

is $(\gamma^2 - 3\gamma + 9)^2$, which is nonzero. Also note that the numerator and denominator in (2) are relatively prime. It is not hard to see that each of these roots corresponds to a prime that is totally ramified prime in $M_1\overline{\mathbb{F}}_q$. Since $q \nmid m$, each of these is tamely ramified in $M_1\overline{\mathbb{F}}_q$. Since no other primes can be ramified, and each of the primes above has degree 1, the Riemann–Hurwitz formula implies that

$$\begin{aligned} 2g_{M_1\overline{\mathbb{F}}_q} - 2 &= m(2g_{\overline{\mathbb{F}}_q(X_{n-1})} - 2) + \sum_{\mathfrak{p}} [e(\mathfrak{p}) - 1] \deg(\mathfrak{p}) \\ &= -2m + 6(m-1)(1) = 4m - 6, \end{aligned}$$

which implies that $g_{M_1\overline{\mathbb{F}}_q} = 2m - 2$, as claimed.

Next, observe that $M_1 = \mathbb{F}_q(Z)(X_{n-1})$ is a cubic extension of $\mathbb{F}_q(Z)$, because X_{n-1} is a root of

$$X^3 - (Z^m - \gamma)X^2 - (Z^m - \gamma + 3)X - 1, \tag{3}$$

which we claim is irreducible. Otherwise, any root would have to divide -1 and therefore be a nonzero constant a. Note that $a \neq -1$, since if -1 were a root of (3), we would have $1 = 0$. If

$$a^3 - (Z^m - \gamma)a^2 - (Z^m - \gamma + 3)a - 1 = 0,$$

then

$$Z^m = \frac{a^3 - 3a - 1}{a^2 + a} + \gamma,$$

which implies that Z^m is constant, a contradiction. This proves that (3) is the minimal polynomial for M_1 over $\mathbb{F}_q(Z)$. The discriminant of (3) is $[(Z^m - \gamma)^2 + 3(Z^m - \gamma) + 9]^2$, so M_1 is a cyclic, cubic extension of $\mathbb{F}_q(Z)$.

Finally, let (Q) be the divisor corresponding to

$$Q = (Z^m - \gamma)^2 + 3(Z^m - \gamma) + 9 \in \mathbb{F}_q(Z).$$

We will show that M_1 is ramified only at the single prime (Q) of $\mathbb{F}_q(Z)$, where $3 \nmid 2m = \deg(Q)$. This completes the proof, by Lemma 1, since the prime 3 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 $\alpha^m - \gamma = 3\zeta$, so $(\alpha^m - \gamma)/3$ has degree 2 over $\mathbb{F}_q$. Then since $X^m - (3\zeta + \gamma)$ is irreducible over $\mathbb{F}_q(\zeta)$,

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q((\alpha^m - \gamma)/3)][\mathbb{F}_q((\alpha^m - \gamma)/3) : \mathbb{F}_q] = m \cdot 2 = 2m,$$

which proves that Q must be irreducible over $\mathbb{F}_q$. Thus the divisor (Q) is in fact prime, and it is ramified (totally ramified since the extension is Galois) in M_1 since it divides the discriminant of $M_1/\mathbb{F}_q(Z)$. To see that M_1 is ramified at no other prime of $\mathbb{F}_q(Z)$, we again use the Riemann–Hurwitz

formula:

$$2(2m-2)-2 = 3(-2) + 2\deg(Q) + \sum_{\mathfrak{p}} (e_{\mathfrak{p}} - 1)\deg(\mathfrak{p}). \tag{4}$$

Since (Q) has degree $2m$, equation (4) shows that no other primes can be ramified. ∎

LEMMA 6. *If $3 \nmid h_{M_i}$ and the prime divisor (P_i) of N_i is inert in M_i, then $3 \nmid h_{M_{i+1}}$ and the prime divisor (P_{i+1}) is inert in M_{i+1}.*

Proof. Notice that $M_{i+1} = M_i N_{i+1}$, so by Lemma 3, M_{i+1} is a cubic, Galois extension of M_i. Also by Lemma 3, M_{i+1} is totally ramified at the prime in M_i lying over (P_i), and unramified everywhere else. Since $3 \nmid h_{M_i}$, Lemma 1 implies that $3 \nmid h_{M_{i+1}}$. It also follows immediately that the prime divisor (P_{i+1}) of N_{i+1} is inert in M_{i+1}. ∎

Proof of Theorem 1. From Lemmas 3, 4, and 5, we see that $3 \nmid h_{M_2}$ and (P_2) is inert in M_2. Repeated application of Lemma 6 proves that L_n has class number indivisible by 3.

To show that there are infinitely many such fields, we prove that each L_n has genus $(m-1)(3^n-1)$, so the fields are distinct. It was shown in Lemma 5 that the genus of M_1 is $2m-2$. Since N_{i+1} is a cyclic, cubic extension of N_i, ramified only at (P_i), we deduce that M_{i+1} is a cyclic, cubic extension of M_i. So M_{i+1}/M_i is also ramified (totally) at a single prime, and since (P_i) is inert in M_i, it has degree $2m$ in M_i. Note that L_n has degree 3^{n-1} over M_1, so by Riemann–Hurwitz,

$$\begin{aligned} 2g_{L_n} - 2 &= 3^{n-1}(2g_{M_1} - 2) + (3^{n-1} - 1)(\deg(P_1)) \\ &= 3^{n-1}(4m-6) + (3^{n-1}-1)(2m) = 3^{n-1}(6m-6) - 2m \\ &= 3^n(2m-2) - 2m. \end{aligned}$$

Thus

$$g_{L_n} = 3^n(m-1) - m + 1 = (3^n - 1)(m-1). \quad ∎$$

3. Proof of Theorem 2. The rest of the paper is devoted to the proof that there are a positive density of primes q satisfying conditions (i)–(iii) in Section 2. In the present section, we prove Theorem 2, a key ingredient.

Let $d = (d_1, \ldots, d_r)$ be a partition of an integer n. For a polynomial $f \in \mathbb{Z}[x]$ of degree n and a prime q not dividing the discriminant of f, we say that f decomposes modulo q with *decomposition type* d if the polynomial f factors modulo q as a product of r irreducible polynomials with degrees $d_1, \ldots, d_r$. Note that for a given f, not every partition gives rise to a possible decomposition type. For example, one can show that the polynomial $f(x) = x^4 + 1$ is irreducible over $\mathbb{Z}$, but reducible modulo q for every prime q, so the partition (4) does not correspond to a possible decomposition type for $f(x)$.

A theorem in Hecke's famous *Lectures on the Theory of Algebraic Numbers* is the following:

THEOREM 4 ([10]). *Let $a_1, \dots, a_t$ be nonzero integers such that $a_1^{m_1} \cdots a_t^{m_t}$ is a square if and only if m_i is even for all i. For any $\epsilon_1, \dots, \epsilon_t \in \{-1, 1\}$, there are a positive density of primes q such that*

$$\left(\frac{a_i}{q}\right) = \epsilon_i \quad \text{for all } i = 1, \dots, t.$$

Note that we can think of Theorem 4 in terms of the decomposition types of the polynomials $x^2 - a_i$ since a_i is a square modulo q if and only if the polynomial $x^2 - a_i$ reduces modulo q with decomposition type $(1, 1)$. So Theorem 4 says that for the polynomials $x^2 - a_i$, $1 \le i \le t$, and for any decomposition types d_i, there are infinitely many primes q such that $x^2 - a_i$ reduces modulo q with decomposition type d_i. The condition that $a_1^{m_1} \cdots a_t^{m_t}$ is a square if and only if m_i is even can be rephrased in terms of the splitting fields K_i of the polynomials $x^2 - a_i$: the splitting fields $K_1, \dots, K_t$ are maximally disjoint, that is, for all i, the intersection of $\mathbb{Q}(\sqrt{a_i})$ and the compositum of the fields $\mathbb{Q}(\sqrt{a_j})$, $j \neq i$, is $\mathbb{Q}$. Equivalently, the Galois group of $K_1 \cdots K_t$ is the product of the Galois groups of the K_i. We now recall Theorem 2, which is a much more general version of Theorem 4 that we will need in Section 4.

THEOREM 2. *Let $f_1, \dots, f_t$ be irreducible polynomials in $\mathbb{Z}[x]$ with splitting fields $K_1, \dots, K_t$. Let G_i denote the Galois group of K_i over $\mathbb{Q}$. Suppose that $G_1 \times \cdots \times G_t$ is the Galois group of the composite field $K_1 \cdots K_t$. For each i, let d_i be a possible decomposition type of f_i. Then there are a positive density of primes q such that each f_i decomposes modulo q with decomposition type d_i.*

To prove Theorem 2, we will use the following theorem of Frobenius.

THEOREM 5 (Frobenius [8]). *Let f be an irreducible polynomial over $\mathbb{Q}$ with Galois group G. The density of the set of primes q for which f has a given decomposition type $d = (d_1, \dots, d_r)$ exists, and is equal to $1/\#G$ times the number of $\sigma \in G$ with cycle pattern d.*

Proof of Theorem 2. Let $\mathrm{Frob}_{K/\mathbb{Q}}(q)$ denote the Frobenius class of q for the extension $K/\mathbb{Q}$. If $d_i = (d_{i1}, \dots, d_{ir})$ is a possible decomposition type for f_i, then by Frobenius's theorem, there is an element $\sigma_i \in G_i$ such that the disjoint cycle decomposition of σ_i considered as a permutation of the roots of f_i has lengths $d_{i1}, \dots, d_{ir}$. It can be shown [20, p. 33] that if $\mathrm{Frob}_{K_i/\mathbb{Q}}(q)$ is the conjugacy class of σ_i, then f_i decomposes modulo q with decomposition type d_i. Since $G_1 \times \cdots \times G_t$ is the Galois group of $H = K_1 \cdots K_t$, there is a unique element $g \in G_1 \times \cdots \times G_t$ such that $g|_{K_i} = \sigma_i$ for all i. Hence if

$\mathrm{Frob}_{H/\mathbb{Q}}(q)$ is the conjugacy class of g, then f_i decomposes modulo q with decomposition type d_i for all i. By the Chebotarev Density Theorem, there are a positive density of primes q such that $\mathrm{Frob}_{H/\mathbb{Q}}(q)$ is the conjugacy class of g; for each such q, each f_i decomposes modulo q with decomposition type d_i. ∎

We should note that the condition that the Galois group of $K_1 \cdots K_t$ is $G_1 \times \cdots \times G_t$ is sufficient, but not always necessary, to obtain the result of Theorem 2. For example, using similar methods one can prove the following generalization of Theorem 4.

THEOREM 6. *Let $a_1, \ldots, a_t$ be integers such that $a_1^{m_1} \cdots a_t^{m_t}$ is a pth power if and only if $p \mid m_i$ for all i. For any $\epsilon_1, \ldots, \epsilon_t \in \{-1, 1\}$, there are a positive density of primes q such that a_i is a pth power modulo q if $\epsilon_i = 1$ and a_i is not a pth power modulo q if $\epsilon_i = -1$.*

4. Finding q for which conditions (i)–(iii) hold. In this section, we will use Theorem 2 to show that for a positive density of q, there is a corresponding γ such that conditions (i)–(iii) in Section 2 are satisfied.

Let ζ be a root of $X^2 + X + 1 \in \mathbb{F}_q[X]$. Choose an integer γ such that

$$\gamma \equiv \begin{cases} p & \pmod{p^2} \text{ for all } p \mid m \text{ with } p \equiv 1 \pmod 3, \\ 3+p & \pmod{p^2} \text{ for } p = 5, 11, \text{ and all } p \mid m \text{ with } p \equiv 2 \pmod 3, \\ 1 & \pmod 4, \\ 1 & \pmod 3. \end{cases} \tag{5}$$

As mentioned before, the primary purpose of conditions (i)–(iii) is that $3\zeta+\gamma$ is not a pth power in $\mathbb{F}_q(\zeta)$ for any p dividing m. As the next lemma shows, this gives rise to the following polynomials:

Fix a prime p dividing m, and let

$$f_p(x) = 3 \sum_{\substack{i=0 \\ i \equiv 0\,(3)}}^{p} \binom{p}{i} x^{p-i} - \gamma \sum_{\substack{i=0 \\ i \equiv 1\,(3)}}^{p} \binom{p}{i} x^{p-i} + (\gamma - 3) \sum_{\substack{i=0 \\ i \equiv 2\,(3)}}^{p} \binom{p}{i} x^{p-i},$$

and let Σ_p be the splitting field for $f_p(x)$ over $\mathbb{Q}$. If $4 \mid m$, let

$$f_4(x) = x^4 - \frac{4}{3}\gamma x^3 + (2\gamma - 6)x^2 + 4x - \frac{\gamma}{3}.$$

The general idea of the rest of the paper is as follows. We show in the next two lemmas that $\gamma + 3\zeta$ is not a pth power in $\mathbb{F}_q(\zeta)$ (that is, conditions (i)–(iii) in Section 2 hold) if the polynomial f_p has no roots modulo q for all primes p dividing m. So we need to show that there are a positive density of q's for which none of the f_p's have roots modulo q. We show that each f_p is irreducible over $\mathbb{Q}$. The special case where m is a power of a prime follows from results of Frobenius and Jordan. Jordan's theorem (Theorem 8 below)

implies that the Galois group of f_p contains an element which acts on the roots of f_p without a fixed point. By Frobenius (Theorem 5), there are a positive density of primes q for which f_p has no roots modulo q. The general case is more involved as we must show the existence of a positive density of primes q for which none of the f_p's have roots modulo q. To do this, we show that the splitting fields Σ_p are maximally disjoint, so that the Galois group of the compositum of the Σ_p's is the product of the Galois groups of the individual fields. Then since each individual Galois group contains an element which acts on the roots of f_p without fixed points, there must be an element of the Galois group of the compositum which acts without fixed points. The result follows again from Frobenius.

Note that condition (iii) on q is actually unnecessary to prove that $X^m - (\gamma + 3\zeta)$ is irreducible over $\mathbb{F}_q(\zeta)$. From (ii) we have $3\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$ for all primes p dividing m. If $4 \mid m$, then $2 \mid m$, so $3\zeta + \gamma$ is not a square in $\mathbb{F}_q(\zeta)$. But we claim that -1 must be a square in $\mathbb{F}_q(\zeta)$. Otherwise, let α be a square root of -1. Then

$$\mathbb{F}_q(\alpha) \cong \mathbb{F}_q[X]/\langle X^2 + 1\rangle \cong \mathbb{F}_{q^2} \cong \mathbb{F}_q(\zeta).$$

If $3\zeta + \gamma = -4w^4$ for some $w \in \mathbb{F}_q(\zeta)$, then $3\zeta + \gamma = (2w^2\alpha)^2$ is a square in $\mathbb{F}_q(\zeta)$, a contradiction. Hence, $3\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$. Thus condition (ii) is sufficient to show that $X^m - (3\zeta + \gamma)$ is irreducible over $\mathbb{F}_q(\zeta)$.

LEMMA 7. *Suppose $q \equiv 2 \pmod 3$, so $\zeta \notin \mathbb{F}_q$. If $f_p(x)$ has no roots modulo q for a prime q, then $\gamma + 3\zeta$ is not a pth power in $\mathbb{F}_q(\zeta)$ for all p dividing m.*

Proof. Suppose, for contradiction, that $\gamma + 3\zeta = (u + v\zeta)^p$ for some $u, v \in \mathbb{F}_q$. So

$$\gamma = \sum_{\substack{i=0 \\ i\equiv 0\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i - \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i,$$

$$3 = \sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i - \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i.$$

Then

$$0 = 3\cdot\gamma - \gamma\cdot 3 = 3\sum_{\substack{i=0 \\ i\equiv 0\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i - 3\sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i$$
$$- \gamma\sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i + \gamma\sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i$$

$$= 3 \sum_{\substack{i=0 \\ i\equiv 0\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i - \gamma \sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i + (\gamma - 3) \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} u^{p-i}v^i$$
$$= v^p f_p(u/v).$$

Since $v \neq 0$ (otherwise $\zeta \in \mathbb{F}_q$), this proves the lemma. ∎

So to guarantee that $3\zeta + \gamma$ is not a pth power in $\mathbb{F}_q(\zeta)$, we need to show that the polynomials f_p have no roots modulo the prime q. We will need more information about the polynomials and their splitting fields.

Let ζ_3 be a primitive cube root of unity in $\mathbb{C}$.

LEMMA 8. *For all p, the polynomial f_p is irreducible over $\mathbb{Q}$.*

Proof. If p is a prime dividing m, then $f_p(x)$ is Eisenstein with respect to p (recall that $3 \nmid m$ so $p \neq 3$). Clearly, p does not divide the leading coefficient of f_p, and p does divide all other coefficients by (5). Notice that since $\gamma \equiv p \pmod{p^2}$ for $p \equiv 1 \pmod 3$ and $\gamma - 3 \equiv p \pmod{p^2}$ for $p \equiv 2 \pmod 3$, the constant term is not divisible by p^2. Thus f_p is Eisenstein with respect to p and irreducible over $\mathbb{Q}$. ∎

LEMMA 9. *If Σ_p is the splitting field for f_p over $\mathbb{Q}$, then $\Sigma_p \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$ for all p dividing m.*

Proof. First we will show that $\Sigma_p \subset \mathbb{R}$. Let α be any complex root of $f_p(x)$, so $f_p(\alpha) = 0$. Then

$$3 \sum_{\substack{i=0 \\ i\equiv 0\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} = \gamma \sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} + (3 - \gamma) \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} \alpha^{p-i},$$

and it follows that

$$(6) \quad (\alpha + \zeta_3)^p = \sum_{i=0}^{p} \binom{p}{i} \alpha^{p-i}\zeta_3^i$$
$$= \sum_{\substack{i=0 \\ i\equiv 0\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} + \sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} \alpha^{p-i}\zeta_3 + \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} \alpha^{p-i}\zeta_3^2$$
$$= \left(\frac{\gamma}{3} + \zeta_3\right)\left[\sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} - \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} \right].$$

Similarly,

$$(\alpha + \zeta_3^2)^p = \left(\frac{\gamma}{3} + \zeta_3^2\right)\left[\sum_{\substack{i=0 \\ i\equiv 1\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} - \sum_{\substack{i=0 \\ i\equiv 2\,(3)}}^{p} \binom{p}{i} \alpha^{p-i} \right].$$

Thus

$$\left(\frac{\alpha+\zeta_3^2}{\alpha+\zeta_3}\right)^p = \frac{3\zeta_3^2+\gamma}{3\zeta_3+\gamma}, \tag{7}$$

so

$$\left(\frac{\overline{\alpha}+\zeta_3}{\overline{\alpha}+\zeta_3^2}\right)^p = \overline{\left(\frac{\alpha+\zeta_3^2}{\alpha+\zeta_3}\right)^p} = \frac{\overline{3\zeta_3^2+\gamma}}{3\zeta_3+\gamma} = \frac{3\zeta_3+\gamma}{3\zeta_3^2+\gamma} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^p,$$

where $\overline{\alpha}$ denotes the complex conjugate of α. For some pth root of unity $\zeta_p \in \mathbb{C}$, we then have

$$\frac{\overline{\alpha}+\zeta_3}{\overline{\alpha}+\zeta_3^2} = \zeta_p\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right).$$

Therefore

$$\alpha\overline{\alpha}+\zeta_3^2\overline{\alpha}+\zeta_3\alpha+1 = \zeta_p(\zeta_3^2\alpha+1+\zeta_3\overline{\alpha}+\alpha\overline{\alpha}). \tag{8}$$

Notice that the left hand side is real since $\zeta_3^2\overline{\alpha}$ and $\zeta_3\alpha$ are conjugates. In fact, the left hand side can be rewritten as $(\alpha+\zeta_3^2)(\overline{\alpha}+\zeta_3) = |\alpha+\zeta_3^2|^2$, so the left hand side is positive. Similarly, $\zeta_3^2\alpha+1+\zeta_3\overline{\alpha}+\alpha\overline{\alpha} = |\alpha+\zeta_3|^2$ is real and positive as well, which implies that ζ_p is a real, positive pth root of unity. Thus $\zeta_p = 1$, so (8) implies that

$$\zeta_3(\overline{\alpha}-\alpha) = \overline{\alpha}-\alpha,$$

and so $\alpha = \overline{\alpha}$. Thus $\Sigma_p \subset \mathbb{R}$, so $\Sigma_p \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$, as claimed. ∎

LEMMA 10. *For any primes p_1 and p_2 dividing m, $\Sigma_{p_1} \cap \Sigma_{p_2} = \mathbb{Q}$.*

Proof. Suppose first that $p_1, p_2 \neq 2, 3$. Let α be any root of $f_p(x)$. Let

$$C_\alpha = \frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}, \quad \text{so} \quad C_\alpha^p = \frac{(\alpha+\zeta_3)^p}{(\alpha+\zeta_3^2)^p} = \frac{3\zeta_3+\gamma}{3\zeta_3^2+\gamma}$$

by (7). Thus $C_\alpha^p \in \mathbb{Q}(\zeta_3)$, and so

$$\alpha = \frac{\zeta_3(1-C_\alpha\zeta_3)}{C_\alpha-1} \in \mathbb{Q}(\zeta_3, C_\alpha).$$

Note that if α_1 and α_2 are both roots of f_p, then $C_{\alpha_1}/C_{\alpha_2}$ is a primitive pth root of unity, and $\alpha_1 = \alpha_2$ if and only if $C_{\alpha_1} = C_{\alpha_2}$. It follows that $\Sigma_p \subset \mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$, where ζ_p is a primitive pth root of unity in $\mathbb{C}$.

First we show that Σ_p is the maximal real subfield of $\mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$. We know from the above that $\Sigma_p \subset \mathbb{R}$. It suffices to show that the composite field $\Sigma_p\mathbb{Q}(\zeta_3)$ equals $\mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$. It is clear that $\Sigma_p\mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$. For the reverse containment, notice that $C_\alpha \in \mathbb{Q}(\alpha, \zeta_3) \subset \Sigma_p\mathbb{Q}(\zeta_3)$. Since all roots α of f_p are in Σ_p, the corresponding C_α satisfies

$$C_\alpha = \frac{\alpha+\zeta_3}{\alpha+\zeta_3^2} \in \Sigma_p\mathbb{Q}(\zeta_3).$$

If α_1 and α_2 are distinct roots of f_p, then $C_{\alpha_1}/C_{\alpha_2}$ is a primitive pth root of unity, so $\zeta_p \in \Sigma_p\mathbb{Q}(\zeta_3)$ as well. Thus $\Sigma_p\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$.

Now $\mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$ is a Galois extension of $\mathbb{Q}(\zeta_3)$ with Galois group G, the metacyclic group of order $p(p-1)$. Let σ and γ be generators of G of order p and $p-1$, respectively, where $\gamma\sigma = \sigma^r\gamma$ for a primitive root r modulo p. If $\tau \in G$, and τ restricted to Σ_p is the identity on Σ_p, then τ must also be the identity on $\mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)$ since τ fixes ζ_3. Thus the Galois group of $\Sigma_p/\mathbb{Q}$ is isomorphic to the Galois group of $\mathbb{Q}(\zeta_3, \zeta_p, C_\alpha)/\mathbb{Q}(\zeta_3)$, that is, G.

Let R_p denote the maximal real subfield of $\mathbb{Q}(\zeta_p)$, i.e., $R_p = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Recall that R_p has degree $(p-1)/2$ over $\mathbb{Q}$ and is ramified (totally) only at p. We also know that if $p \equiv 1 \pmod 4$, then $\mathbb{Q}(\sqrt{p})$ is the unique quadratic subfield of R_p (and Σ_p), and if $p \equiv 3 \pmod 4$, then $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$. In the second case, $\mathbb{Q}(\sqrt{3p})$ is the unique quadratic subfield of Σ_p. Let A_p be the maximal abelian subfield of Σ_p. Then A_p is the fixed field of the commutator subgroup of G. The commutator subgroup of G is the cyclic group generated by $\gamma\sigma\gamma^{-1}\sigma^{-1} = \sigma^{r-1}$. Since $r-1$ is relatively prime to p, this is the same as the subgroup generated by σ. So A_p is the fixed field of $\langle\sigma\rangle$, which implies that A_p has degree $p-1$ over $\mathbb{Q}$.

Now since Σ_{p_1} and Σ_{p_2} are both Galois extensions of $\mathbb{Q}$, so is $\Sigma_{p_1} \cap \Sigma_{p_2}$. We next show that $\Sigma_{p_1} \cap \Sigma_{p_2}$ is an abelian extension of $\mathbb{Q}$. It will then follow that $\Sigma_{p_1} \cap \Sigma_{p_2} \subset A_{p_1} \cap A_{p_2}$. Let $d = [\Sigma_{p_1} \cap \Sigma_{p_2} : \mathbb{Q}]$. We claim first that $d \leq p_1 - 1$. Suppose, for contradiction, that $d > p_1 - 1$. Then $\Sigma_{p_1} \cap \Sigma_{p_2} \cap \mathbb{Q}(\alpha_1) \neq \mathbb{Q}$ since otherwise

$$[\Sigma_{p_1} : \mathbb{Q}] \geq [\Sigma_{p_1} \cap \Sigma_{p_2} : \mathbb{Q}][\mathbb{Q}(\alpha_1) : \mathbb{Q}] > (p_1 - 1)p_1,$$

a contradiction. Thus $\Sigma_{p_1} \cap \Sigma_{p_2} \cap \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_1)$, which implies that $\mathbb{Q}(\alpha_1) \subset \Sigma_{p_1} \cap \Sigma_{p_2}$. Then $p_1 \mid d \mid p_2(p_2-1)$, so $p_1 \mid (p_2-1)$. Now $\mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}$ since $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\alpha_2)$ have prime degrees $p_1 \neq p_2$. Notice that $\mathbb{Q}(\alpha_2) \cap R_{p_2} = \mathbb{Q}$; otherwise, $\mathbb{Q}(\alpha_2) \cap R_{p_2} = \mathbb{Q}(\alpha_2)$ since $\mathbb{Q}(\alpha_2)$ has prime degree p_2 over $\mathbb{Q}$. This is impossible since p_2 does not divide $(p_2-1)/2$. Since f_{p_1} is Eisenstein with respect to p_1, we see that p_1 is totally ramified in $\mathbb{Q}(\alpha_1)$. But p_1 is unramified in $R_{p_2} \subset \mathbb{Q}(\zeta_{p_2})$, so $\mathbb{Q}(\alpha_1) \cap R_{p_2} = \mathbb{Q}$. It follows that

$$[\Sigma_{p_2} : \mathbb{Q}] \geq [R_{p_2} : \mathbb{Q}][\mathbb{Q}(\alpha_2) : \mathbb{Q}][\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \frac{p_1 p_2(p_2 - 1)}{2} > p_2(p_2 - 1),$$

a contradiction. So $d \leq p_1 - 1$, and furthermore, $d \mid (p_1-1)$, since $d \mid p_1(p_1-1)$. Similarly, $d \mid (p_2 - 1)$. The Galois group of $\Sigma_{p_1} \cap \Sigma_{p_2}$ is therefore a quotient of $\langle\gamma\rangle$, and so, cyclic.

Thus $\Sigma_{p_1} \cap \Sigma_{p_2}$ is a cyclic subfield of $A_{p_1} \cap A_{p_2}$. Let r be the degree of $A_{p_1} \cap A_{p_2}$ over $\mathbb{Q}$. If r is even, then $A_{p_1} \cap A_{p_2}$ has a unique quadratic subfield K. It follows that K is also the unique quadratic subfield of both Σ_{p_1} and Σ_{p_2}. This is impossible, however, since the quadratic subfield of Σ_{p_i} is either $\mathbb{Q}(\sqrt{p_i})$ or $\mathbb{Q}(\sqrt{3p_i})$. Thus d is odd. It follows that $A_{p_1} \cap A_{p_2} \subseteq$

$R_{p_1} \cap R_{p_2}$. But p_1 is totally ramified in R_{p_1} (and thus in $R_{p_1} \cap R_{p_2}$), and unramified in R_{p_2} (and thus in $R_{p_1} \cap R_{p_2}$). So we must have $A_{p_1} \cap A_{p_2} = \mathbb{Q}$. Thus $\Sigma_{p_1} \cap \Sigma_{p_2} = \mathbb{Q}$, as claimed.

If $p = 2$, then

$$f_2(x) = 3x^2 - 2\gamma x + (\gamma - 3).$$

Since $\gamma \equiv 1 \pmod 4$, we see that f_2 is Eisenstein with respect to 2, and Σ_2 is a quadratic field, totally ramified at 2. In fact, $\Sigma_2 = \mathbb{Q}(\sqrt{\gamma^2 - 3\gamma + 9})$. If $p \equiv 1 \pmod 3$, then $\gamma \equiv 0 \pmod p$, so

$$\gamma^2 - 3\gamma + 9 \equiv 9 \not\equiv 0 \pmod p,$$

hence p is unramified in $\mathbb{Q}(\sqrt{\gamma^2 - 3\gamma + 9})$. If $p \equiv 2 \pmod 3$, then $\gamma \equiv 3 \pmod p$; consequently,

$$\gamma^2 - 3\gamma + 9 \equiv 9 \not\equiv 0 \pmod p,$$

so p is unramified in $\mathbb{Q}(\sqrt{\gamma^2 - 3\gamma + 9})$. Thus $\Sigma_2 = \mathbb{Q}(\sqrt{\gamma^2 - 3\gamma + 9}) \neq \mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{3p})$ since p is ramified in $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{3p})$. Thus $\Sigma_2 \cap \Sigma_p = \mathbb{Q}$ for all $p \mid m$. ∎

LEMMA 11. *Every quadratic subfield of $\Sigma_{p_1} \cdots \Sigma_{p_t}$ is contained in the compositum of the quadratic subfields of $\Sigma_{p_1}, \ldots, \Sigma_{p_t}$.*

Proof. Let $p = p_1$, $p_1 \neq 2, 3$, and let $K_1 = \Sigma_{p_1}$ with unique quadratic subfield $\mathbb{Q}(\sqrt{d})$, and let $K_2 = \Sigma_{p_2} \cdots \Sigma_{p_t}$. Let $\mathbb{Q}(\sqrt{d_i})$ be the unique quadratic subfield of Σ_{p_i}. Let G_1 denote the Galois group of K_1, so that G_1 is isomorphic to the metacyclic group of order $p(p-1)$. Let G_2 denote the Galois group of K_1K_2/K_2, so G_2 is isomorphic to the Galois group of K_1 over $K_1 \cap K_2$. We claim that $K_2(\sqrt{d})$ is the unique quadratic intermediate field of the extension K_1K_2/K_2. The result then follows by induction. If $t = 2$, then suppose that there is a quadratic field $\mathbb{Q}(\sqrt{m})$ with $\mathbb{Q}(\sqrt{m}) \subset K_1K_2$ and $\mathbb{Q}(\sqrt{m}) \not\subset \mathbb{Q}(\sqrt{d}, \sqrt{d_2})$. Then $\sqrt{m} \notin K_2$, since $K_2 = \Sigma_{p_2}$ has unique quadratic field $\mathbb{Q}(\sqrt{d_2})$. Hence $K_2(\sqrt{m})$ is a quadratic extension of K_2, and by the claim, $K_2(\sqrt{m}) = K_2(\sqrt{d})$. Thus $\sqrt{m/d} \in K_2$, so $\sqrt{m/d} \in \mathbb{Q}(\sqrt{d_2})$ since $\mathbb{Q}(\sqrt{d_2})$ is the unique quadratic subfield of K_2. So

$$\sqrt{m} = \sqrt{d}\sqrt{m/d} \in \mathbb{Q}(\sqrt{d}, \sqrt{d_2}),$$

a contradiction. This proves the base case. Now let $M = \mathbb{Q}(\sqrt{d_2}) \cdots \mathbb{Q}(\sqrt{d_t})$; by induction, any quadratic subfield of K_2 is contained in M. Suppose $\mathbb{Q}(\sqrt{m}) \subseteq K_1K_2$ and $\mathbb{Q}(\sqrt{m}) \not\subseteq \mathbb{Q}(\sqrt{d})M$. It follows that $\sqrt{m} \notin K_2$, so $K_2(\sqrt{m})$ is a quadratic subfield of K_1K_2/K_2. By the claim, then, $K_2(\sqrt{m}) = K_2(\sqrt{d})$, so $\sqrt{m/d} \in K_2$. Then $\sqrt{m/d} \in M$, so

$$\sqrt{m} = \sqrt{d}\sqrt{m/d} \in \mathbb{Q}(\sqrt{d})M,$$

a contradiction.

To prove the claim, it suffices to show that G_2 has only one subgroup with index 2. Let P be the p-Sylow subgroup of G_1, that is, P is the unique subgroup of G_1 of order p. First suppose that $P \cap G_2$ is trivial. Then

$$G_2 \cong G_2/(G_2 \cap P) \hookrightarrow G_1/P.$$

Since G_1/P is cyclic, it follows that G_2 is cyclic, and must therefore contain at most one subgroup of index 2.

It remains to consider the case that $P \subset G_2$. If H is any subgroup of G_2 of index 2, then $P \subset H$. The second isomorphism theorem implies that

$$G_2/H \cong (G_2/P)/(H/P).$$

The group on the right is a quotient of G_2/P which is cyclic of order dividing $p-1$. Thus G_2/H is a quotient of a cyclic group, so there can only be one H of any particular index.

Note that if $K_1 = \Sigma_2$, then K_1 is itself quadratic, so the result is trivial. ∎

For convenience, we summarize what we have proven about the unique quadratic subfield of Σ_p.

LEMMA 12. *The unique quadratic subfield of Σ_p is*

$$\begin{cases} \mathbb{Q}(\sqrt{p}), & p \equiv 1 \pmod 4; \\ \mathbb{Q}(\sqrt{3p}), & p \equiv 3 \pmod 4,\ p \neq 3; \\ \mathbb{Q}(\sqrt{\gamma^2 - 3\gamma + 9}), & p = 2;\ \textit{ramified at } 2, \\ & \qquad \textit{unramified at } 3, 5 \textit{ and all odd } p \mid m. \end{cases}$$

Notice that for $p \neq 2, 3$, the quadratic subfield of Σ_p is unramified at 2.

THEOREM 7. *Let $p_1, \ldots, p_t$ be the distinct primes dividing m, and suppose that $p_1 < \cdots < p_t$. Then*

$$\Sigma_{p_1} \cap \Sigma_{p_2}\Sigma_{p_3}\cdots\Sigma_{p_t} = \mathbb{Q}.$$

Proof. For ease of notation, let $L = \Sigma_{p_2}\Sigma_{p_3}\cdots\Sigma_{p_t}$. First we will show that $p_1 \nmid [\Sigma_{p_1} \cap L : \mathbb{Q}]$. Suppose that $[\Sigma_{p_1} \cap L : \mathbb{Q}] = p_1 r$ for some positive integer r, and let x_1 be any root of $f_{p_1}(x)$. In this case, we see that $\mathbb{Q}(x_1) \subset \Sigma_{p_1} \cap L$; otherwise, $\mathbb{Q}(x_1) \cap (\Sigma_{p_1} \cap L) = \mathbb{Q}$, and so,

$$[\Sigma_1 : \mathbb{Q}] \geq [\mathbb{Q}(x_1) : \mathbb{Q}][\Sigma_{p_1} \cap L : \mathbb{Q}] = p_1^2 r > p_1(p_1 - 1),$$

a contradiction. Thus L contains all roots of $f_{p_1}(x)$, so L contains the splitting field Σ_{p_1} of $f_{p_1}(x)$. Suppose first that $p_1 \neq 2, 3$. Then Σ_{p_1} contains the unique quadratic subfield, $\mathbb{Q}(\sqrt{p_1})$ or $\mathbb{Q}(\sqrt{3p_1})$, both of which are ramified at p_1. But by Lemma 11, every quadratic subfield of L is contained in the compositum of fields of the form $\mathbb{Q}(\sqrt{p_i})$ or $\mathbb{Q}(\sqrt{3p_i})$, $2 \leq i \leq t$, and is thus unramified outside the set $\{3, p_2, \ldots, p_t\}$. This is a contradiction, and so we see that $p_1 \nmid [\Sigma_{p_1} \cap L : \mathbb{Q}]$ for $p_1 \neq 2, 3$. Next, suppose that $p_1 = 2$. Again by Lemma 11, every quadratic subfield of L will be ramified at at least one

of $3, 5, p_2, \ldots, p_t$, all of which are unramified in Σ_2. So $p_1 \nmid [\Sigma_{p_1} \cap L : \mathbb{Q}]$ for $p_1 = 2$. Finally, if $p_1 = 3$, then the unique quadratic subfield of Σ_{p_1} is ramified at 2, but by Lemma 11, every quadratic subfield of L is unramified at 2. Therefore, in this case as well, Σ_{p_1} and L cannot contain the same quadratic field, so $p_1 \nmid [\Sigma_{p_1} \cap L : \mathbb{Q}]$.

Thus p_1 is relatively prime to $[\Sigma_{p_1} \cap L : \mathbb{Q}]$, so $[\Sigma_{p_1} \cap L : \mathbb{Q}]$ divides $p_1 - 1$. Consequently, the Galois group of $(\Sigma_{p_1} \cap L)/\mathbb{Q}$ is cyclic. If $[\Sigma_{p_1} \cap L : \mathbb{Q}]$ is even, then $\Sigma_{p_1} \cap L$ contains a unique quadratic subfield. But as seen above, Σ_{p_1} and L cannot contain the same quadratic field. Thus $[\Sigma_{p_1} \cap L : \mathbb{Q}]$ is odd, and it follows that $\Sigma_{p_1} \cap L \subset R_{p_1}$ if $p_1 \neq 2, 3$. In this case, p_1 is totally ramified in $\Sigma_{p_1} \cap L$, and p_1 is the only prime ramified in $\Sigma_{p_1} \cap L$. Let $d = [\Sigma_{p_1} \cap L : \mathbb{Q}]$, so d is odd, and $d \mid (p_1 - 1)/2$. We need to show that $d = 1$.

Consider the composite field

$$K = (\Sigma_{p_1} \cap L) R_{p_2} \cdots R_{p_t}.$$

Note that $(\Sigma_{p_1} \cap L) \cap R_{p_2} \cdots R_{p_t} = \mathbb{Q}$, since p_1 is totally ramified in $\Sigma_{p_1} \cap L$ and p_1 is unramified in $R_{p_2} \cdots R_{p_t}$. Thus $[K : R_{p_2} \cdots R_{p_t}] = d$. Now $K \subset L$, so d divides $[L : R_{p_2} \cdots R_{p_t}]$. But $[L : R_{p_2} \cdots R_{p_t}]$ divides $2^{t-1} p_2 \cdots p_t$. If $d \neq 1$, then since d is odd, after renaming, $d = p_2 \cdots p_r$ for some $r \leq t$. Thus

$$p_2 \mid d \mid (p_1 - 1)/2,$$

which is a contradiction as $p_2 > p_1$. This completes the proof that $\Sigma_{p_1} \cap L = \mathbb{Q}$ for $p_1 \neq 2$. If $p_1 = 2$, then we must have $d = 1$ since d is an odd integer dividing $p_1 - 1$. ∎

THEOREM 8 (Jordan [16]). *Let G be a group acting on a finite set X with cardinality n. If $n \geq 2$, and G acts transitively on X, then there is an element $g \in G$ which acts on X without a fixed point.*

THEOREM 9. *For any positive integer $m > 1$, there are a positive density of primes q for which there exists a $\gamma \in \mathbb{Z}$ satisfying conditions* (i)–(iii) *from Section* 2. *Moreover, if q satisfies the hypotheses, then so does q^r for all odd integers r with $(r, m) = 1$.*

Proof. Let $p_1, \ldots, p_t$ be the primes dividing m with $p_1 < \cdots < p_t$. First we claim that if G_i is the Galois group of $\Sigma_{p_i}/\mathbb{Q}$, then $G_1 \times \cdots \times G_{p_t}$ is the Galois group of $\Sigma_{p_1} \cdots \Sigma_{p_t}$ over $\mathbb{Q}$. Clearly, $G_{t-1} \times G_t$ is the Galois group of $\Sigma_{p_{t-1}} \Sigma_{p_t}$, since $\Sigma_{p_{t-1}} \cap \Sigma_{p_t} = \mathbb{Q}$. For induction, suppose that $G_2 \times \cdots \times G_t$ is the Galois group of $\Sigma_{p_2} \cdots \Sigma_{p_t}$ over $\mathbb{Q}$. By Theorem 7, $\Sigma_{p_1} \cap \Sigma_{p_2} \Sigma_{p_3} \cdots \Sigma_{p_t} = \mathbb{Q}$, so $G_1 \times \cdots \times G_t$ is the Galois group of $\Sigma_{p_1} \cdots \Sigma_{p_t}$ over $\mathbb{Q}$, as claimed. Since each Σ_{p_i} is totally real, we also have

$$\mathbb{Q}(\zeta_3) \cap \Sigma_{p_1} \Sigma_{p_2} \cdots \Sigma_{p_t} = \mathbb{Q}.$$

So if G is the Galois group of $\mathbb{Q}(\zeta_3)/\mathbb{Q}$, then $G \times G_1 \times \cdots \times G_t$ is the Galois group of $\mathbb{Q}(\zeta_3)\Sigma_{p_1} \cdots \Sigma_{p_t}$ over $\mathbb{Q}$.

Now to prove the theorem, it suffices, by Lemma 7, to show that there are a positive density of primes q such that $q \equiv 2 \pmod 3$ and f_{p_i} has no roots modulo q for all i. We apply Theorem 2 to the polynomials $x^2 + x + 1, f_{p_1}, \ldots, f_{p_t}$. Let $d_1 = (2)$, so that $x^2 + x + 1$ decomposes modulo q with decomposition type d_1 (i.e. $x^2 + x + 1$ is irreducible modulo q) if and only if $q \equiv 2 \pmod 3$. For $1 \leq i \leq t$, the Galois group G_i acts transitively on the roots of f_{p_i}, so by Theorem 8, there exists a σ_i in G_i such that σ_i acts without fixed points. By Theorem 5, σ_i corresponds to a possible decomposition type d_i for f_{p_i} with no linear factors. By Theorem 2, there are a positive density of primes q such that the polynomials decompose as desired; each such q satisfies the hypotheses of Theorem 1.

Also, notice that if q has the desired properties, so does q^r if r is odd and r and m are relatively prime. Certainly, $q^r \equiv 2 \pmod 3$ if r is odd. Moreover, if $f(x) \in \mathbb{Z}[x]$ has degree p dividing m, and $f(x)$ has no roots in $\mathbb{F}_q$, then suppose for contradiction that θ is a root of $f(x)$ in $\mathbb{F}_{q^r}$. Then $[\mathbb{F}_{q^r}(\theta) : \mathbb{F}_q] = r$, but $p = [\mathbb{F}_q(\theta) : \mathbb{F}_q]$ divides $[\mathbb{F}_{q^r}(\theta) : \mathbb{F}_q]$, contradicting the fact that $(r, m) = 1$. Thus if f_{p_i} has no roots in $\mathbb{F}_q$, then f_{p_i} has no roots in F_{q^r}. ∎

Remark. We have shown the existence of a positive density of q for which the main result is true. It is possible to find the density exactly. A prime q satisfies conditions (i)–(iii) if the f_p's have no roots modulo q. This is equivalent to the condition that there exists an element of the Galois group of the splitting field Σ_p with no fixed points. For $p \neq 4$, the Galois group of f_p is isomorphic to the metacyclic group of order $p(p-1)$. If $\sigma_{a,b}$ is defined by

$$\sigma_{a,b}(i) = ai + b \quad \text{for } a \in \mathbb{F}_p^\times,\ b \in \mathbb{F}_p,$$

then it is not hard to see that $\sigma_{a,b}$ has no fixed points if and only if $a = 1$ and $b \neq 0$. Thus $p - 1$ elements of the Galois group of f_p have no fixed points, and so the density of primes for which f_p has no roots modulo q is $1/p = (p-1)/p(p-1)$. The Galois group of f_4 is S_4, and one easily checks that exactly 9 of the 24 elements in S_4 have no fixed points, so the density of primes for which f_4 has no roots modulo q is $3/8$. Thus the density of primes for which each of the f_p's has no roots modulo q is

$$\delta = \begin{cases} \displaystyle\prod_{p \mid m} \frac{1}{p}, & 4 \nmid m, \\ \displaystyle\frac{3}{8} \prod_{p \mid m} \frac{1}{p}, & 4 \mid m. \end{cases}$$

If $4 \nmid m$, then we see that $\delta \geq 1/m$, and $\delta = 1/m$ if m is square-free.

Acknowledgments. The first author would like to thank Florian Luca for several helpful discussions.

References

[1] J. D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra 204 (2006), 316–333.

[2] —, *Results of Cohen–Lenstra type for quadratic function fields*, in: Computational Arithmetic Geometry, Contemp. Math. 463, Amer. Math. Soc., Providence, RI, 2008, 1–7.

[3] 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.

[4] B. Datskovsky and D. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. 386 (1988), 116–138.

[5] M. Daub, J. Lang, M. Merling, A. M. Pacelli, N. Pitiwan, and M. Rosen, *Function fields with class number indivisible by a prime ℓ*, preprint.

[6] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. London Ser. A 322 (1971), 405–420.

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

[8] F. G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsber. Akad. Wiss. Berlin 1896, 689–703; Gesammelte Abh. II, Springer, Berlin, 1968, 719–733.

[9] 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.

[10] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, New York, 1981.

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

[12] —, *Trace formulae and imaginary quadratic fields*, Math. Ann. 288 (1990), 605–612.

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

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

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

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

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

[18] 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.

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

[20] H. W. Lenstra and P. Stevenhagen, *Chebotarëv and his density theorem*, Math. Intelligencer 18 (1996), no. 2, 26–37.

[21] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 140–150.

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

[23] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compos. Math. 119 (1999), 1–11.
[24] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo ℓ*, Ann. of Math. 147 (1998), 453–470; Corrigendum, ibid. 148 (1998), 361.
[25] A. M. Pacelli, *Abelian subgroups of any order in class groups of global function fields*, J. Number Theory 106 (2004), 26–49.
[26] —, *The prime at infinity and the rank of the class group in global function fields*, ibid. 116 (2006), 311–323.
[27] D. Shanks, *The simplest cubic fields*, Math. Comp. 28 (1974), 1137–1157.
[28] P. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory 5 (1973), 237–241.
[29] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

Department of Mathematics
Williams College
Williamstown, MA 01267, U.S.A.
E-mail: Allison.Pacelli@williams.edu
http://www.williams.edu/Mathematics/apacelli/

Department of Mathematics
Brown University
Providence, RI 02912, U.S.A.
E-mail: Michael_Rosen@brown.edu

Received on 15.5.2008
and in revised form on 29.1.2009 (5708)