Canad. Math. Bull. Vol. **49** (3), 2006 pp. 448–463

A Lower Bound on the Number of Cyclic Function Fields With Class Number Divisible by n

Allison M. Pacelli

Abstract. In this paper, we find a lower bound on the number of cyclic function fields of prime degree l whose class numbers are divisible by a given integer n. This generalizes a previous result of D. Cardon and R. Murty which gives a lower bound on the number of quadratic function fields with class numbers divisible by n.

1 Introduction

The divisibility of the class number is an important problem for both number fields and function fields. In 1801, Gauss proved [8] that the class number of a quadratic number field is divisible by the exact power 2^t, where t is the number of primes dividing the discriminant of the field. In the mid-1800's, Kummer [9] related the divisibility of the class number of a cyclotomic field to a special case of Fermat's Last Theorem. In particular, he showed that there are no non-trivial solutions in integers to the equation $x^p + y^p = z^p$ for regular primes p, that is, those primes p not dividing the class number of $K = \mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root of unity.

In the twentieth century, much progress was made on the question of divisibility of class numbers. For example, in 1922 Nagell [12] proved that for any integer n, infinitely many imaginary quadratic number fields have class number divisible by n. The analogous result for real quadratic number fields was proven in 1969 by Yamamoto [15] and for real quadratic function fields in 1992 by Friesen [7]. In 1983, Cohen and Lenstra [4] conjectured something stronger, namely that for any integer n, as $x \to \infty$, a positive fraction of quadratic number fields with discriminant $< x$ should have class number divisible by n. Their argument has been generalized to number fields of any degree [2] and to function fields [6] as well, but the conjecture has not been proven yet in any of these cases.

In 1999, however, Murty [11] was able to construct a lower bound on the number of imaginary quadratic number fields with class number divisible by n; namely, he showed that if $n > 2$ is an integer, then there are more than a positive constant times $x^{\frac{1}{2}+\frac{1}{n}}$ imaginary quadratic number fields with discriminant $\leq x$ and class number divisible by n (this bound has been improved by K. Soundararajan [14], Yu [16] and Luca [10] for the case n even, and Chakraborty and Murty [3] and Byeon and Koh [1] for the case $n = 3$). Then in 2001, Murty and Cardon [2] proved the analogous result for function fields to show that if q is a power of an odd prime, and n is a fixed

Received by the editors July 8, 2004; revised December 3, 2004.
AMS subject classification: 11R29, 11R58.

integer > 2, then there exist more than a positive constant times $q^{x(\frac{1}{2}+\frac{1}{n})}$ quadratic extensions $\mathbb{F}_q(T, \sqrt{D})$ of $\mathbb{F}_q(T)$ with $\deg(D) \le x$ and class number divisible by n. In this paper, we extend the latter result to cyclic extensions $\mathbb{F}_q(T, \sqrt[l]{D})$ of $\mathbb{F}_q(T)$ where l is a prime dividing $q-1$.

Let q be a power of an odd prime, and let $\mathbb{F}_q$ be the field with q elements. Fix a transcendental element T over $\mathbb{F}_q$ so that $\mathbb{F}_q(T)$ is the rational function field. If K is any extension of $\mathbb{F}_q(T)$, then denote by $\mathcal{O}_K$ the integral closure of $\mathbb{F}_q[T]$ in K. We write Cl_K to denote the ideal class group of $\mathcal{O}_K$, and h_K to denote the class number. We use the notation $f(x) \gg g(x)$ to mean that there exists a positive constant c with $f(x) > cg(x)$. The main result is as follows:

Theorem 1 *Let l be a prime dividing $q-1$. If n is a fixed positive integer that satisfies*

(i) $n > l^2 - l$,

(ii) *n has no prime divisors less than l, and*

(iii) $\frac{1}{l} - \frac{1}{n} > \frac{\log 2}{\log q}$,

then there are $\gg q^{x(\frac{1}{l}+\frac{1}{n})}$ cyclic extensions $K = \mathbb{F}_q(T)(\sqrt[l]{D})$ of $\mathbb{F}_q(T)$ with $\deg(D) \le x$ and h_K divisible by n.

Notice that when $l = 2$, the first condition states that $n > 2$ as in [2]. The second condition is trivial in that case, and the third condition of the theorem implies that $q > 2^l$, which also reduces to the condition $q \ge 5$ in [2]. If $q > 2^l$, but n is an integer that fails to satisfy one of the three conditions in Theorem 1, it is still possible to compute a lower bound on the number of cyclic extensions $\mathbb{F}_q(T, \sqrt[l]{D})$ of $\mathbb{F}_q(T)$ with class number divisible by n; the new bound is $q^{x(1/l\,+\,1/nt)}$ for some $t > 1$.

As in [2], we show first that if f and g are monic elements of $\mathbb{F}_q[T]$, $-a \in \mathbb{F}_q^{\times}$ is not an l-th power, $\deg(f^n) > \deg(g^l)$, and $D = g^l - af^n$ is l-th power free, then the class group of $\mathbb{F}_q(T, \sqrt[l]{D})$ contains an element of order n. We then give a lower bound, using sieve methods, on the number of f and g for which D is l-th power free, and estimate the number of repeated values of D as f and g vary.

2 Constructing an Element of Order n in the Class Group

Lemma 1 *Let n be a positive integer with $n > l^2 - l$, and suppose that $l \mid (q-1)$. Assume that $f, g \in \mathbb{F}_q[T]$ are monic, $-a \in \mathbb{F}_q^{\times}$ is not an l-th power, $\deg(f^n) > \deg(g^l)$, and $D = g^l - af^n$ is l-th power free. Then the class group of $K = \mathbb{F}_q(T, \sqrt[l]{D})$ contains an element of order n.*

Proof Notice that f and g are relatively prime, because any common factor would also divide D to the l-th power. Let ζ_l be a primitive l-th root of unity. The ideal (af^n) factors as follows:

$$(1) \qquad (f^n) = (af^n) = (g^l - D) = (g - \sqrt[l]{D})(g - \zeta_l \sqrt[l]{D}) \cdots (g - \zeta_l^{l-1} \sqrt[l]{D}).$$

We claim that the ideals on the right-hand side of (1) are pairwise relatively prime. To see that this is true, suppose that I is a prime ideal dividing both $(g - \zeta_l^j \sqrt[l]{D})$ and

$(g - \zeta_l^i \sqrt[l]{D})$ for some $0 \le i < j \le l-1$. Then

$$\sqrt[l]{D}(\zeta_l^i - \zeta_l^j) = (g - \zeta_l^j \sqrt[l]{D}) - (g - \zeta_l^i \sqrt[l]{D}) \in I,$$
$$g(\zeta_l^{j-i} - 1) = \zeta_l^{j-i}(g - \zeta_l^i \sqrt[l]{D}) - (g - \zeta_l^j \sqrt[l]{D}) \in I.$$

Since $\zeta_l^i - \zeta_l^j$ and $\zeta_l^{j-i} - 1$ are nonzero constants, it follows that $g, \sqrt[l]{D} \in I$. But this contradicts the fact that f and g are relatively prime, so the ideals on the right-hand side of (1) must, in fact, be pairwise relatively prime as claimed.

As a result, there exist ideals $\mathfrak{a} = \mathfrak{a}_0, \mathfrak{a}_1, \dots, \mathfrak{a}_{l-1}$ with $\mathfrak{a}_i^n = (g - \zeta_l^i \sqrt[l]{D})$. We shall show that $\mathfrak{a}$ has order n in the class group. Since all of the $\mathfrak{a}_i$'s are conjugate, they have equal norm. Let $|\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{b}|$ denote the norm of $\mathfrak{b} \subset \mathcal{O}_K$, and let $N(\nu)$ denote the norm from K down to $\mathbb{F}_q(T)$ of an element ν in K. By (1), then,

$$|\mathfrak{a}^n|^l = |(f^n)| = q^{nl\deg(f)},$$

and so, $|\mathfrak{a}| = q^{\deg(f)}$. If the order of $\mathfrak{a}$ is not n, then $\mathfrak{a}^r$ is principal for some $r < n$. Let r be the order of $\mathfrak{a}$ so that $r \mid n$.

For any $h \in \mathbb{F}_q[T]$, let $\{h\}$ denote the l-th power free part of h and $[h]$ an l-th root of $\frac{h}{\{h\}}$. Then $h = \{h\}[h]^l$. By [13, Theorem 1.2], an integral basis for $\mathcal{O}_K$ consists of

$$\left\{ 1, \frac{\sqrt[l]{D}}{[D]}, \frac{\sqrt[l]{D}^2}{[D^2]}, \dots, \frac{\sqrt[l]{D}^{l-1}}{[D^{l-1}]} \right\}.$$

Let $\nu \in \mathcal{O}_K$ be such that $\mathfrak{a}^r = (\nu)$, and write

$$\nu = \sum_{i=0}^{l-1} \nu_i \frac{\sqrt[l]{D^i}}{[D^i]}$$

for some $\nu_i \in \mathbb{F}_q[T]$.

Now since the leading coefficient $-a$ of D is not an l-th power, the prime at infinity is either totally ramified or inert in K. Let k_∞ denote the completion of $\mathbb{F}_q(T)$ at ∞. It follows that the only units in K are the roots of unity. Because $(\nu)^{n/r} = \mathfrak{a}^n$, it follows that $\omega\nu^{n/r} = g - \sqrt[l]{D}$ for some root of unity ω. This implies that $\nu \notin \mathbb{F}_q(T)$ since $\sqrt[l]{D} \notin \mathbb{F}_q(T)$. As a result, we can choose i, $1 \le i \le l-1$, such that $\nu_i \ne 0$. Let $\sigma_j(\sqrt[l]{D}) = \zeta_l^j \sqrt[l]{D}$, $0 \le j \le l-1$, be the l elements of $\mathrm{Gal}(K/\mathbb{F}_q(T))$, and notice that

$$N(\nu) = \prod_{j=0}^{l-1} (\sigma_j(\nu)).$$

We claim that $\deg(N(\nu)) \ge \frac{1}{l-1}\deg(D)$. Assuming this for a moment, the lemma is proved by noticing that

$$q^{r\deg(f)} = |\mathfrak{a}|^r = |(\nu)| = |N(\nu)| = q^{\deg(N(\nu))} \ge q^{\frac{\deg(D)}{l-1}} = q^{\frac{\deg(g^l - af^n)}{l-1}} = q^{\frac{n\deg(f)}{l-1}},$$

which implies that

$$\frac{n}{r} \le l - 1.$$

But $\frac{n}{r}$ is an integer dividing n, so by hypothesis we must have that $n = r$, as desired.

To prove the claim above, we first show that

$$\sum_{j=0}^{l-1} \zeta_l^{-ji} \sigma_j(\nu) = \frac{l\nu_i \sqrt[l]{D}^i}{[D^i]}.$$

To see this, note that

$$\sum_{j=0}^{l-1} \zeta_l^{jk-ji} = 1 + \zeta_l^{k-i} + (\zeta_l^{k-i})^2 + (\zeta_l^{k-i})^3 + \cdots + (\zeta_l^{k-i})^{l-1} \tag{2}$$
$$= \begin{cases} l & \text{if } k = i, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\begin{aligned}
\sum_{j=0}^{l-1} \zeta_l^{-ji} \sigma_j(\nu) &= \sum_{j=0}^{l-1} \zeta_l^{-ji} \sigma_j\Big(\sum_{k=0}^{l-1} \nu_k \frac{\sqrt[l]{D^k}}{[D^k]}\Big) \\
&= \sum_{j=0}^{l-1} \zeta_l^{-ji} \sum_{k=0}^{l-1} \frac{\nu_k}{[D^k]} (\zeta_l^j \sqrt[l]{D})^k \\
&= \sum_{j=0}^{l-1} \sum_{k=0}^{l-1} \frac{\nu_k}{[D^k]} \zeta_l^{jk-ji} \sqrt[l]{D}^k \\
&= \sum_{k=0}^{l-1} \Big(\sum_{j=0}^{l-1} \zeta_l^{jk-ji}\Big) \frac{\nu_k}{[D^k]} \sqrt[l]{D}^k \\
&= \frac{l\nu_i \sqrt[l]{D}^i}{[D^i]}.
\end{aligned}$$

Let $\mathfrak{p}_\infty$ denote the sole prime in K lying above ∞. For all j, $0 \le j \le l-1$,

$$\operatorname{ord}_{\mathfrak{p}_\infty}(\nu) = \operatorname{ord}_{\mathfrak{p}_\infty}(\sigma_j(\nu)) = \operatorname{ord}_{\mathfrak{p}_\infty}(\zeta_l^{-ji}\sigma_j(\nu)).$$

Then

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{p}_\infty}(v) &= \min\{\operatorname{ord}_{\mathfrak{p}_\infty}(\zeta_l^{-ji}\sigma_j(v))\}_{0\le j\le l-1} \\
&\le \operatorname{ord}_{\mathfrak{p}_\infty}\left(\sum_{j=0}^{l-1}\zeta_l^{-ji}\sigma_j(v)\right) \\
&= \operatorname{ord}_{\mathfrak{p}_\infty}\left(\frac{lv_i\sqrt[l]{D}^{\,i}}{[D^i]}\right) \\
&= \operatorname{ord}_{\mathfrak{p}_\infty}(v_i) + \operatorname{ord}_{\mathfrak{p}_\infty}(\sqrt[l]{D}^{\,i}) - \operatorname{ord}_{\mathfrak{p}_\infty}([D^i]).
\end{aligned}$$

Since $v_i \in \mathbb{F}_q[T]$, we know $\operatorname{ord}_{\mathfrak{p}_\infty}(v_i) < 0$; therefore

$$\operatorname{ord}_{\mathfrak{p}_\infty}(v) < \operatorname{ord}_{\mathfrak{p}_\infty}(\sqrt[l]{D}^{\,i}) - \operatorname{ord}_{\mathfrak{p}_\infty}([D^i]). \tag{3}$$

Since $\mathfrak{p}_\infty$ is the only prime lying over ∞, the same inequality holds for each conjugate of v. Summing (3) over the conjugates of v gives that

$$\operatorname{ord}_{\mathfrak{p}_\infty}(N(v)) < \operatorname{ord}_{\mathfrak{p}_\infty}(D^i) - \operatorname{ord}_{\mathfrak{p}_\infty}([D^i]^l). \tag{4}$$

Notice that because $N(v)$, D^i, and $[D^i]^l$ are all in $\mathbb{F}_q[T]$, and $\mathfrak{p}_\infty$ is the only prime above ∞, we can replace $\mathfrak{p}_\infty$ by ∞ in (4) to get

$$\operatorname{ord}_\infty(N(v)) < \operatorname{ord}_\infty\left(\frac{D^i}{[D^i]^l}\right) = \operatorname{ord}_\infty\left(\{D^i\}\right).$$

Therefore $\deg(N(v)) > \deg(\{D^i\})$. To finish the proof of the claim, we will show that $\deg(\{D^i\}) \ge \frac{\deg(D)}{l-1}$. Define

$$\operatorname{rad}(D) = \prod_{\substack{p\mid D \\ p \text{ monic,irred}}} p.$$

First, we claim that $\operatorname{rad}(D)$ divides $\{D^i\}$ for $1 \le i \le l-1$. To see that this is true, observe that if $p \mid D$, then $\operatorname{ord}_p(D) < l$ since D is l-th power free. Then $i \operatorname{ord}_p(D)$ is not divisible by l, which implies that p divides $\{D^i\}$. This is true for all p dividing D and therefore proves the claim. Finally, notice that since D is l-th power free, $D \mid (\operatorname{rad}(D))^{l-1}$. Then

$$\deg(D) \le (l-1)\deg(\operatorname{rad}(D)) \le (l-1)\deg(\{D^i\}).$$

This completes the proof. ∎

3 When Is $D = g^l - af^n$ l-th power Free?

We need to find a lower bound on the number of D satisfying the hypotheses of Lemma 1. We proceed as in [2]. First, let $k = \deg(f)$, and set

$$j = \begin{cases} \lfloor \frac{nk}{l} \rfloor & \text{if } l \nmid nk, \\ \frac{nk}{l} - 1 & \text{if } l \mid nk. \end{cases}$$

We will consider only those polynomials g with $\deg(g) = j$, so that $\deg(f^n) > \deg(g^l)$. The expression $\sum_f$ will always be used to denote the sum over all monic f of fixed degree k.

For $h \in \mathbb{F}_q[T]$, define

$$s(h) = \begin{cases} 1 & \text{if } h \text{ is } l\text{-th power free,} \\ 0 & \text{otherwise,} \end{cases}$$

$$s_z(h) = \begin{cases} 1 & \text{if } d^l \nmid h \text{ whenever } 1 \le \deg(d) \le z, \\ 0 & \text{otherwise.} \end{cases}$$

We will use the following lemma with an appropriate choice of z, dependent on k, to show that for large k, the number of distinct l-th power free values of D of degree nk is approximately

$$\sum_{f,g} s_z(g^l - af^n) \sim \sum_{f,g} s(g^l - af^n) \gg q^{j+k}.$$

Lemma 2

$$\sum_{f,g} s_z(g^l - af^n) \ge \sum_{f,g} s(g^l - af^n) \ge \sum_{f,g} s_z(g^l - af^n) - \sum_{\substack{f,g,p \\ \deg(p)>z \\ p^l \mid g^l - af^n}} 1.$$

Proof For the first inequality, notice that for fixed f and g, if $g^l - af^n$ is l-th power free, then $s_z(g^l - af^n) = 1 = s(g^l - af^n)$. If $g^l - af^n$ is not l-th power free, then $s(g^l - af^n) = 0 \le s_z(g^l - af^n)$.

The second inequality also follows from considering, for fixed f and g, the two cases in which $g^l - af^n$ is or is not l-th power free. If $g^l - af^n$ is l-th power free, then $s(g^l - af^n) = 1 = s_z(g^l - af^n)$ and $\sum_{\deg(p)>z, g^l - af^n \equiv 0 \pmod{p^l}} 1 \ge 0$, so

$$s(g^l - af^n) \ge s_z(g^l - af^n) - \sum_{\substack{\deg(p)>z \\ g^l - af^n \equiv 0 \pmod{p^l}}} 1.$$

If $g^l - af^n$ is not l-th power free, write $g^l - af^n = p_1^{e_1} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} \cdots p_t^{e_t}$, where $e_i \ge l$ for $1 \le i \le r$ and $e_i < l$ for $r+1 \le i \le t$. If $s_z(g^l - af^n) = 0$, then

$$s(g^l - af^n) = 0 \ge - \sum_{\substack{\deg(p)>z \\ g^l - af^n \equiv 0 \pmod{p^l}}} 1 = s_z(g^l - af^n) - \sum_{\substack{\deg(p)>z \\ g^l - af^n \equiv 0 \pmod{p^l}}} 1.$$

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

If $s_z(g^l - af^n) = 1$, then $\deg(p_i) > z$ for some $i \le r$, so

$$\sum_{\substack{\deg(p)>z \\ g^l - af^n \equiv 0 \pmod{p^l}}} 1 \ge 1,$$

which implies

$$s(g^l - af^n) = 0 \ge s_z(g^l - af^n) - \sum_{\substack{\deg(p)>z \\ g^l - af^n \equiv 0 \pmod{p^l}}} 1. \qquad \blacksquare$$

The following lemma will also be important later on.

Lemma 3 *If $\pi(u)$ is the number of monic, irreducible polynomials in $\mathbb{F}_q[T]$ of degree $u > 0$, then $\pi(u) \le \frac{q^u}{u}$.*

Proof Since $q^u = \sum_{c|u} c\pi(c) = \sum_{c|u, c<u} c\pi(c) + u\pi(u) \ge u\pi(u)$, the result follows. $\blacksquare$

For fixed $f, d \in \mathbb{F}_q[T]$, define

$$\rho_f(d) = \#\{g \in \mathbb{F}_q[T]/d\mathbb{F}_q[T] \mid g^l - af^n \equiv 0 \pmod{d}\}.$$

Lemma 4 *For d, d_1, d_2, and $p \in \mathbb{F}_q[T]$, with d square free and p irreducible, we have*

(i) $\rho_f(d_1 d_2) = \rho_f(d_1)\rho_f(d_2)$ *if d_1 and d_2 are relatively prime;*
(ii) $\rho_f(p^l) = q^{(l-1)\deg(p)}$ *if $p \mid f$;*
(iii) $\rho_f(p^l) \le l$ *if $p \nmid f$;*
(iv) $\rho_f(d^l) \le l^{\nu(d)} q^{(l-1)\deg(f)}$, *where $\nu(d)$ is the number of distinct non-constant, monic, irreducible polynomials dividing d.*

Proof The first statement follows from the Chinese remainder theorem.
For the second statement, let

$$S = \{g \in \mathbb{F}_q[T]/p^l\mathbb{F}_q[T] \mid g^l - af^n \equiv 0 \pmod{p^l}\}.$$

Since p is irreducible, $p \mid f$, and $n \ge l$, then $g \in S$ if and only if $p \mid g$. So $\rho_f(p^l) = \#S = q^{(l-1)\deg(p)}$.

Next, suppose that $p \nmid f$, and $g^l - af^n \equiv 0 \pmod{p^l}$. Let g_i be such that $g \equiv g_i \pmod{p^i}$ for $1 \le i \le l-1$. Then $g_i^l - af^n \equiv 0 \pmod{p^i}$. If $i = 1$, the congruence has at most l solutions. It is a standard fact that each of these solutions modulo p lifts uniquely to a solution $\bmod\, p^l$ since p does not divide f or g.

Finally, for the fourth statement, if d is square free, then

$$\begin{aligned}\rho_f(d^l) &= \prod_{\substack{p\mid d\\ p\mid f}} \rho_f(p^l) \prod_{\substack{p\mid d\\ p\nmid f}} \rho_f(p^l)\\ &\le \prod_{\substack{p\mid d\\ p\mid f}} q^{(l-1)\deg(p)} \prod_{\substack{p\mid d\\ p\nmid f}} l\\ &\le q^{(l-1)\deg(f)} l^{\nu(d)}.\end{aligned}$$

■

For the rest of the paper, the expression $\prod_p$ will denote the product over monic, irreducible polynomials p. Define

$$N_{f,z}(j) = \sum_{\deg(g)=j} s_z(g^l - af^n) \quad \text{and} \quad P(z) = \prod_{\deg(p)\le z} p.$$

Lemma 5 *Given any $\epsilon > 0$, we can choose κ so that if $z = \kappa \ln(k)$, then*

$$N_{f,z}(j) = q^j \prod_{\deg(p)\le z} (1 - \rho_f(p^l) q^{-\deg(p^l)}) + O(q^{(l-1+\epsilon)k}).$$

Proof First, observe that

$$s_z(g^l - af^n) = \sum_{\substack{d \text{ monic}\\ d^l\mid(g^l-af^n, P(z)^l)}} \mu(d).$$

To see this, notice that if $g^l - af^n$ is l-th power free, then $s_z(g^l - af^n) = 1$ and $\mu(1) = 1$ is the only term in the sum. Also, if $z < \deg(p_i)$ for all p_i with p_i^l dividing $g^l - af^n$, then $s_z(g^l - af^n) = 1$, and again, $\mu(1) = 1$ is the only term in the sum. Otherwise, $s_z(g^l - af^n) = 0$. Let r be the number of distinct primes that both divide $g^l - af^n$ to a power $\ge l$ and have degree at most z. Then

$$\sum_{\substack{d \text{ monic}\\ d^l\mid(g^l-af^n, P(z)^l)}} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = 0.$$

Thus

$$\begin{aligned}N_{f,z}(j) &= \sum_{\deg(g)=j} \sum_{\substack{d \text{ monic}\\ d^l\mid(g^l-af^n, P(z)^l)}} \mu(d)\\ &= \sum_{\substack{d \text{ monic}\\ d\mid P(z)}} \mu(d) \sum_{\substack{\deg(g)=j\\ g^l-af^n\equiv 0 \pmod{d^l}}} 1.\end{aligned}$$

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

There are two possibilities for the sum on the right. If $j \geq \deg(d^l)$, then

$$\sum_{\substack{\deg(g)=j \\ g^l - af^n \equiv 0 \pmod{d^l}}} 1 = \rho_f(d^l) \cdot \#\{g \mid \deg(g) = j \text{ and } g \equiv g_0 \pmod{d^l}\},$$

where g_0 is a given polynomial mod d^l with $g_0^l - af^n \equiv 0 \,(\mathrm{mod}\, d^l)$. If $g = g_0 + sd^l$, then $\deg(s) = j - \deg(d^l)$, so there are $q^{j-\deg(d^l)}$ such s that are monic. Thus

$$\sum_{\substack{\deg(g)=j \\ g^l - ag^n \equiv 0 \pmod{d^l}}} 1 = \rho_f(d^l) q^{j-\deg(d^l)}.$$

If, on the other hand, $j < \deg(d^l)$, then $\sum_{\deg(g)=j, g^l - af^n \equiv 0 \pmod{d^l}} 1 \leq \rho_f(d^l)$. Therefore, putting the two cases together yields

$$\begin{aligned} N_{f,z}(j) &= \sum_{d \mid P(z)} \mu(d) \big[\rho_f(d^l) q^{j-\deg(d^l)} + O(\rho_f(d^l)) \big] \\ &= q^j \sum_{d \mid P(z)} \mu(d) \rho_f(d^l) q^{-\deg(d^l)} + \sum_{d \mid P(z)} O(\rho_f(d^l)) \\ &= q^j \prod_{\deg(p) \leq z} (1 - \rho_f(p^l) q^{-\deg(p^l)}) + O(\rho_f(d^l)), \end{aligned}$$

where the product is over all monic p. From Lemma 4, we have

$$\begin{aligned} \sum_{d \mid P(z)} \rho_f(d^l) &\leq \sum_{d \mid P(z)} l^{\nu(d)} q^{(l-1)\deg(f)} = q^{(l-1)k} \sum_{d \mid P(z)} l^{\nu(d)} = q^{(l-1)k} \prod_{\deg(p) \leq z} (l+1) \\ &\leq q^{(l-1)k} (l+1)^{q^z}. \end{aligned}$$

Choose $\kappa < \frac{1}{\ln(q)}$. Then for any $\epsilon > 0$, and for sufficiently large k,

$$\begin{aligned} k^{\kappa \ln(q)} &\ll \epsilon k \frac{\ln(q)}{\ln(l+1)} \\ e^{k^{\kappa \ln(q)} \ln(l+1)} &\ll e^{\epsilon k \ln(q)} \\ (l+1)^{e^{(\ln(k))\kappa \ln(q)}} &\ll q^{\epsilon k} \\ (l+1)^{q^{\kappa \ln(k)}} &\ll q^{\epsilon k} \\ (l+1)^{q^z} &\ll q^{\epsilon k} \end{aligned}$$

Therefore, for sufficiently large k, we have

$$N_{f,z}(j) = q^j \prod_{\deg(p) \leq z} (1 - \rho_f(p^l) q^{-\deg(p^l)}) + O(q^{(l-1+\epsilon)k}),$$

as desired. ∎

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

Lemma 6

$$\sum_{f,g} s_z(g^l - af^n) = \sum_{\deg(f)=k} N_{f,z}(j) \gg q^{j+k}.$$

Proof Notice that the equality above follows from the definitions of s_z and $N_{f,z}$. We also have that

$$\begin{aligned}
\prod_{\deg(p)\le z} (1-\rho_f(p^l)q^{-\deg(p^l)}) &= \prod_{\substack{p|f\\ \deg(p)\le z}} (1-q^{(l-1)\deg(p)}q^{-l\deg(p)}) \\
&\quad \times \prod_{\substack{(p,f)=1\\ \deg(p)\le z}} (1-\rho_f(p^l)q^{-\deg(p^l)}) \\
&\ge \prod_{\substack{p|f\\ \deg(p)\le z}} (1-q^{-\deg(p)}) \prod_{\substack{(p,f)=1\\ \deg(p)\le z}} (1-lq^{-\deg(p^l)}) \\
&\ge \prod_{\substack{p|f\\ \deg(p)\le z}} (1-q^{-\deg(p)}) \prod_{\text{all } p} (1-lq^{-\deg(p^l)}) \\
&\gg \prod_{\substack{p|f\\ \deg(p)\le z}} (1-q^{-\deg(p)}) \\
&\ge \prod_{p|f} (1-q^{-\deg(p)}) \\
&= \sum_{d|f} \mu(d)q^{-\deg(d)}.
\end{aligned}$$

Summing over f, we see that

$$\begin{aligned}
\sum_{\deg(f)=k} \prod_{\deg(p)\le z} (1-\rho_f(p^l)q^{-\deg(p^l)}) &\gg \sum_{\deg(f)=k} \sum_{d|m} \mu(d)q^{-\deg(d)} \\
&= \sum_{\deg(d)\le k} \mu(d)q^{-\deg(d)}q^{k-\deg(d)} \\
&= q^k \sum_{\deg(d)\le k} \mu(d)q^{-2\deg(d)} \\
&= q^k \sum_{i=0}^{k} \Big(\sum_{\deg(d)=i} \mu(d)q^{-2i} \Big) \\
&= q^k(1-q^{-1}) \\
&\gg q^k.
\end{aligned}$$

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

Thus by Lemma 5,

$$\begin{aligned}\sum_{\deg(f)=k} N_{f,z}(j) &= \sum_{\deg(f)=k}\Big[q^j \prod_{\deg(p)\le z}(1-\rho_f(p^l)q^{-\deg(p^l)}) + O(q^{(l-1+\epsilon)k})\Big]\\ &\gg q^{j+k} + O\Big(\sum_{\deg(f)=k} q^{(l-1+\epsilon)k}\Big)\\ &= q^{j+k} + O(q^{(l+\epsilon)k}).\end{aligned}$$

It remains to show that $q^{j+k} + O(q^{(l+\epsilon)k}) \gg q^{j+k}$.

For $\epsilon < \frac{1}{l} - \frac{1}{k}$, we have $k(\frac{1}{l} - \epsilon) > 1$. Then

$$k\Big(l-1+\frac{1}{l}\Big) - 1 > k(l+\epsilon-1), \quad \text{so} \quad \frac{k}{l}(l^2-l+1) - 1 > k(l+\epsilon-1).$$

But we also know that

$$j \ge \frac{nk}{l} - 1 \ge \frac{k}{l}(l^2-l+1) - 1 > k(l+\epsilon-1).$$

Thus

$$\begin{aligned}q^{j+k} + O(q^{(l+\epsilon)k}) &= q^{j+k}\big[1 + O(q^{(l+\epsilon-1)k-j)})\big]\\ &= q^{j+k}\big[1 + O(q^{(l+\epsilon-1-j/k)k})\big]\\ &\gg q^{j+k}.\end{aligned}$$

■

Lemma 7

$$\sum_{\deg(f)=k} \nu(f) \ll \ln(k) q^k.$$

Proof First notice that $\sum_{\deg(f)=k} \nu(f) \le \sum_{\deg(p)\le k} q^{k-\deg(p)}$, since for a fixed $p \mid f$, the contribution of p to the sum is the number of monic polynomials r with $f = rp$. But we also have

$$\sum_{\deg(p)\le k} q^{k-\deg(p)} \le q^k \sum_{u\le k} q^{-u}\pi(u) \le q^k \sum_{u \le k}\frac{1}{u} \ll q^k \ln(k),$$

which completes the proof. ■

Lemma 8

$$\sum_{\substack{f,g,p\\ \deg(p)>z\\ g^l - af^n \equiv 0 \pmod{p^l}}} 1 = o(q^{j+k}).$$

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

Proof Let
$$M_{f,p}(j) = \sum_{\substack{\deg(g)=j \\ g^l - af^n \equiv 0 \pmod{p^l}}} 1,$$
so that the sum in question is $\sum_f \sum_{\deg(p)>z} M_{f,p}(j)$. If $j \geq \deg(p^l)$, then $M_{f,p}(j) = \rho_f(p^l) q^{j-\deg(p^l)}$, while if $j < \deg(p^l)$, then $M_{f,p}(j) \leq \rho_f(p^l)$. With Lemma 4, this gives
$$M_{f,p}(j) \leq \begin{cases} l(q^{j-\deg(p^l)} + 1) & \text{if } p \nmid f, \\ q^{j-\deg(p)} & \text{if } p \mid f \text{ and } j \geq \deg(p^l), \\ q^{(l-1)\deg(p)} & \text{if } p \mid f \text{ and } j < \deg(p^l). \end{cases}$$
Summing over irreducible p gives that
$$\sum_{z<\deg(p)\leq j} M_{f,p}(j) \leq \sum_{\substack{z<\deg(p)\leq j \\ p\nmid f}} l\,(q^{j-\deg(p^l)} + 1) + \sum_{\substack{z<\deg(p)\leq j \\ p\mid f \\ \deg(p)\leq j/l}} q^{j-\deg(p)}$$
$$+ \sum_{\substack{z<\deg(p)\leq j \\ p\mid f \\ \deg(p)>j/l}} q^{(l-1)\deg(p)}.$$
We consider each of the three sums above separately. For the first, we have
$$\begin{aligned}\sum_{\substack{z<\deg(p)\leq j \\ p\nmid f}} l\,(q^{j-\deg(p^l)} + 1) &\ll \sum_{i>z}^{j} \frac{q^i}{i}(q^{j-li} + 1) \\ &\ll \frac{q^{j-lz}q^z}{z}\Bigl(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots\Bigr) + \frac{q^j}{j}\Bigl(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots\Bigr) \\ &\ll \frac{q^{j-lz}q^z}{z} + \frac{q^j}{j}.\end{aligned}$$
For the second sum, we have
$$\sum_{\substack{z<\deg(p)\leq j \\ p\mid f \\ \nu(p)\leq j/l}} q^{j-\deg(p)} \leq \nu(f) q^{j-z}.$$
Finally, for the third sum, suppose $p_1, \ldots, p_l$ are distinct primes dividing f with $\deg(p_i) > j/l$. Then $\deg(p_1) + \cdots + \deg(p_l) \leq \deg(f) = k$. But $\deg(p_1) + \cdots + \deg(p_l) > l(j/l) = j > k$. So at most $l-1$ distinct primes occur in the sum, each with degree at most k. Thus
$$\sum_{\substack{z<\deg(p)\leq j \\ p\mid f \\ \deg(p)>j/l}} q^{(l-1)\deg(p)} \leq (l-1) q^{(l-1)k}.$$

Putting this together, we now have

$$(5) \qquad \sum_{z<\deg(p)\leq j} M_{f,p}(j) \ll \frac{q^{j-lz}q^z}{z} + \frac{q^j}{j} + \nu(f)q^{j-z} + q^{(l-1)k}.$$

Because $n > l^2 - l$, it follows that $q^{(l-1)k-j} \to 0$ as $j, k \to \infty$. Therefore, summing (3) over f yields the desired result:

$$\begin{aligned}\sum_f \sum_{\deg(p)>z} M_{f,p}(j) &\ll \frac{q^k q^{j-lz}q^z}{z} + \frac{q^{j+k}}{j} + q^{lk} + q^{j-z}\sum_f \nu(f)\\ &\ll \frac{q^{j+k+(1-l)z}}{z} + \frac{q^{j+k}}{j} + q^{lk} + q^{j-z}q^k\ln(k)\\ &= q^{j+k}\Big(\frac{1}{zq^{(l-1)z}} + \frac{1}{j} + q^{(l-1)k-j} + \frac{\ln(k)}{q^z}\Big)\\ &= o(q^{j+k})\end{aligned}$$

■

4 Duplication

We have already shown that there are $\gg q^{j+k}$ l-th power free values of $g^l - af^n$ as f and g vary. The next lemma examines how many values are duplicated.

Lemma 9 *The number of elements of $\mathbb{F}_q(T)$ of the form $g^l - af^n$ with $\deg(g) = j$ and $\deg(f) = k$ that are representable in more than one way is $o(q^{j+k})$.*

Proof Let S be the collection of pairs (f, g) of monic polynomials with $\deg(f) = k$, $\deg(g) = j$, and $g^l - af^n$ representable in more than one way. If f_1, f_2 are fixed, distinct polynomials such that $g_1^l - af_1^n = g_2^l - af_2^n$ for some g_1 and g_2, then

$$a(f_1^n - f_2^n) = g_1^l - g_2^l = (g_1 - g_2)(g_1 - \zeta_l g_2)\cdots(g_1 - \zeta_l^{l-1}g_2).$$

The choices for g_1 and g_2 are therefore determined by the divisors of $a(f_1^n - f_2^n)$. Since $\deg(f_1^n - f_2^n) < nk$, then $a(f_1^n - f_2^n)$ is divisible by at most $nk - 1$ distinct, monic, linear factors, in which case the number of divisors is

$$(q-1)\sum_{\nu=0}^{nk-1}\binom{nk-1}{\nu} = (q-1)2^{nk-1}.$$

This is a very rough estimate of an upper bound on the number of divisors of $a(f_1^n - f_2^n)$ when k is large relative to q. With q^k choices for f_1, q^k choices for f_2, and at most $(q-1)2^{nk-1}$ choices for g_1 and g_2, it follows that $\#S = O(q^{2k}2^{nk})$.

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

To see that $\#S = o(q^{j+k})$, we just need to show that $q^{k-j}2^{nk} \to 0$ as $k \to \infty$ since this would imply

$$q^{2k}2^{nk} = q^{j+k}(q^{k-j}2^{nk}) = o(q^{j+k}).$$

Now $\frac{1}{l} - \frac{1}{n} > \frac{\log 2}{\log q}$ by assumption, so $(\log q)(\frac{1}{l} - \frac{1}{n}) > \log 2$. It follows that $q^{\frac{n}{l}-1} > 2^n$. Then

$$\frac{2^n}{q^{\frac{n}{l}-1}} < 1,$$

and so,

$$\left(\frac{2^n}{q^{\frac{n}{l}-1}}\right)^k \to 0$$

as $k \to \infty$. The result follows because

$$q^{k-j}2^{nk} \le q^{k+1-\frac{nk}{l}}2^{nk} = q\left(\frac{2^n}{q^{\frac{n}{l}-1}}\right)^k \to 0. \qquad \blacksquare$$

5 Conclusion

We have shown that there are $\gg q^{j+k}$ distinct values of $D = g^l - af^n$ such that $\mathbb{F}_q(T, \sqrt[l]{D})$ has an element of order n in its class group. Since $j = \lfloor \frac{nk}{l} \rfloor$ or $j = \frac{nk}{l} - 1$, then there are $\gg q^{nk(\frac{1}{l}+\frac{1}{n})}$ distinct values of D with an element of order n in the class group of $\mathbb{F}_q(T, \sqrt[l]{D})$. Thus, there are $\gg q^{x(\frac{1}{l}+\frac{1}{n})}$ distinct function fields $\mathbb{F}_q(T, \sqrt[l]{D})$ with $\deg(D) \le x$ and class number divisible by n.

Note that the third condition on n, q, and l in Theorem 1 is not that restrictive. If q is large enough, then it requires little more than $n > l^2 - l$. Consider the case of $l = 3$. If $q = 9$, then the theorem gives a bound on the number of cubic function fields with class number divisible by an odd integer n with $n \ge 55$. If $q = 16$, then n can be any odd integer with $n \ge 13$. If $q = 64$, then n can be any odd integer with $n \ge 7$. Also note that if the class group of a function field K contains an element of order n, then it also contains elements of order r for each r dividing n. This expands further the set of n to which the theorem applies.

If $n < l^2 - l$ so that Theorem 1 does not apply, it is still possible to determine a lower bound on the number of cyclic function fields of the form $K = \mathbb{F}_q(T, \sqrt[l]{D})$ with class number divisible by n. The following result holds.

Theorem 2 *Let q be a power of an odd prime and l a prime dividing $q - 1$. Assume that $q > 2^l$. Let n be an integer with prime factorization $n = p_1^{e_1} \cdots p_s^{e_s}$. If m_i is the smallest integer with $m_i \ge \frac{\log(l-1)}{\log(p_i)}$, then set $t = p_1^{m_1} \dots p_s^{m_s}$. If nt fails to satisfy one of the following conditions, then replace t by a suitable multiple of $p_1^{m_1} \cdots p_s^{m_s}$ so that it does satisfy the conditions:*

(i) $nt > l^2 - l$,

(ii) $\frac{1}{l} - \frac{1}{nt} > \frac{\log 2}{\log q}$.

Then there are $\gg q^{x(\frac{1}{l}+\frac{1}{nt})}$ cyclic extensions $\mathbb{F}_q(T, \sqrt[l]{D})$ of $\mathbb{F}_q(T)$ with $\deg(D) \le x$ whose class numbers are divisible by n.

https://doi.org/10.4153/CMB-2006-044-7 Published online by Cambridge University Press

The proof of Theorem 2 is nearly the same as the proof of Theorem 1. To construct an element of order n in the class group of $\mathbb{F}_q(T, \sqrt[l]{D})$, first apply Lemma 1 to the integer $p_i^{e_i+m_i}$ instead of n for each prime p_i dividing n. In the proof of the lemma, it is shown that if r is the order of $\mathfrak{a}$, then

$$\frac{n}{r} \leq l - 1,$$

where $r \mid n$. Replacing n with $p_i^{e_i+m_i}$, we can write $r = p_i^{b_i}$ for some b_i with $b_i \leq e_i + m_i$. Thus $p_i^{e_i+m-b_i} \leq l - 1$, and so,

$$b_i \geq e_i + m_i - \frac{\log(l-1)}{\log(p_i)} > e_i.$$

We have constructed an element of order $p_i^{b_i}$ in the class group of $\mathbb{F}_q(T, \sqrt[l]{D})$, so the class number of $\mathbb{F}_q(T, \sqrt[l]{D})$ is divisible by p^{e_i}. Repeating the argument for each prime dividing n shows that the class number of $\mathbb{F}_q(T, \sqrt[l]{D})$ is divisible by n. Applying the rest of the proof of Theorem 1 to nt rather than n proves Theorem 2.

Acknowledgments I would like to thank my advisor Michael Rosen for his guidance and encouragement as I worked on my dissertation. I would also like to thank Ram Murty for his continued support, and the referee for his helpful comments.

References

[1] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by 3.* Manuscripta Math. **111**(2003), no. 2, 261–263.
[2] D. Cardon and R. Ram Murty, *Exponents of class groups of quadratic function fields over finite fields.* Canad. Math. Bull. **44**(2001), no. 4, 398–407.
[3] K. Chakraborty and M. Ram Murty, *On the number of real quadratic fields with class number divisible by 3.* Proc. Amer. Math. Soc. **131**(2003), no. 1, 41–44.
[4] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields.* In: Number Theory, Lecture Notes in Math. 1068, Springer, Berlin, 1984, pp. 33–62.
[5] H. Cohen and J. Martinet, *Class groups of number fields: numerical heuristics.* Math. Comp. **48**(1987), no. 177, 123–137.
[6] E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over a finite field.* In: Théorie des nombres, de Gruyter, Berlin, 1989, pp. 227–239.
[7] C. Friesen, *Class number divisibility in real quadratic function fields.* Canad. Math. Bull. **35**(1992), no. 3, 361–370.
[8] C. F. Gauss, *Disquisitiones Arithmeticae.* Leipzig, 1801.
[9] E. Kummer, *Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche [sic] Anzahl Primzahlen λ.* Monatsber. Akad. Wiss. Berlin, 1847, 132-141, 305-319.
[10] F. Luca, *A note on the divisibility of class numbers of real quadratic fields.* C. R. Math. Acad. Sci. Soc. R. Can. **25**(2003), no. 3, 71–75.
[11] M. R. Murty, *Exponents of class groups of quadratic fields.* In: Topics in Number Theory, Math. Appl. 467, Kluwer Academic. Publishers, Dordrecht, 1999, pp. 229–239.
[12] T. Nagell, *Uber die Klassenzahl imaginar quadratischer Zahlkorper.* Abh. Math. Sem. Univ. Hamburg **1**(1922), 140–150.
[13] M. Rosen, *Average value of class numbers in cyclic extensions of the rational function field.* In: Number Theory, CMS Conf. Proc. 15, American Mathematical Society, Providence, RI, 1995, pp. 307–323.
[14] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields.* J. London Math. Soc. **61**(2000), no. 3, 681–690.

[15] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields.* Osaka J. Math. **7**(1970), 57–76.
[16] G. Yu, *A note on the divisibility of class numbers of real quadratic fields.* J. Number Theory **97**(2002), no. 1, 35–44.

Department of Mathematics
Williams College
Williamstown, MA 01267
e-mail: Allison.Pacelli@williams.edu