EXPONENTS OF CLASS GROUPS OF QUADRATIC FUNCTION FIELDS OVER FINITE FIELDS

DAVID A. CARDON AND M. RAM MURTY

Abstract. We find a lower bound on the number of imaginary quadratic extensions of the function field $\mathbb{F}_q(T)$ whose class groups have an element of a fixed order.

More precisely, let $q \geq 5$ be a power of an odd prime and let g be a fixed positive integer ≥ 3. There are $\gg q^{\ell(\frac{1}{2}+\frac{1}{g})}$ polynomials $D \in \mathbb{F}_q[T]$ with $\deg(D) \leq \ell$ such that the class groups of the quadratic extensions $\mathbb{F}_q(T, \sqrt{D})$ have an element of order g.

1. Introduction

In a recent paper Murty [11] showed that if g is a fixed integer ≥ 3 then the number of imaginary quadratic fields whose absolute discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{\frac{1}{2}+\frac{1}{g}}$. He also showed that the number of real quadratic fields whose discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{\frac{1}{2g}}$.

In this paper we prove the analogous result for function fields rather than number fields in the analog of the imaginary quadratic case.

The problem of divisibility of class numbers for number fields has been studied extensively. Gauss studied the case $g = 2$. The case $g = 3$ was studied by Davenport and Heilbronn [4]. For any g the infinitude of such fields was established by Nagell [12], Honda [9], Ankeny and Chowla [2], Hartung [8], Yamamoto [14], and Weinberger [13]. Assuming the ABC Conjecture Murty [10] obtained a quantitative lower bound on the number of such fields. More recently Murty [11] improved the technique to give the result mentioned earlier without assuming the ABC conjecture. A conjecture of Cohen and Lenstra [3] predicts that as x increases a positive fraction of discriminants $\leq x$ produce quadratic extensions whose class number is divisible by any fixed g.

Interest in function fields was stimulated by the doctoral thesis of E. Artin [1] and the class number problem for function fields has been studied. For example, if g is not divisible by q then Friesen [7] constructed infinitely many polynomials $M \in \mathbb{F}_q[T]$ of even degree such the class groups of the quadratic extensions $\mathbb{F}_q(T, \sqrt{M})$ of the function field $\mathbb{F}_q(T)$ have an element of order

1991 *Mathematics Subject Classification.* Primary: 11R58, Secondary: 11R29.
Key words and phrases. class number, quadratic function field.
Research partially supported by NSERC.

g. Friedman and Washington [6] have studied the Cohen-Lenstra conjecture in the function field case, and Yu [15] has established the Cohen-Lenstra conjecture as the characteristic p tends to infinity for fixed discriminantal degree.

We now state the main result of this paper:

Theorem. *Let $q \geq 5$ be a power of an odd prime and let g be a fixed positive integer ≥ 3. There are $\gg q^{\ell(\frac{1}{2}+\frac{1}{g})}$ quadratic extensions $\mathbb{F}_q(T, \sqrt{D})$ of $\mathbb{F}_q(T)$ with $\deg(D) \leq \ell$ whose class group has an element of order g.*

The remainder of this paper will present the proof as a series of lemmas. The main outline is as follows. We show that if n and m are monic elements of $\mathbb{F}_q[T]$, if $-a \in \mathbb{F}_q^{\times}$ is not a square, if $\deg(m^g) > \deg(n^2)$, and if $D = n^2 - am^g$ is squarefree, then the class group of $\mathbb{F}_q(T, \sqrt{D})$ has an element of order g. Using sieve methods and by letting m and n vary we are able to give a lower bound on the number of m and n such that D is squarefree. Finally, we show that as m and n vary there are relatively few duplicated values of D.

2. Preliminaries

$\mathbb{F}_q$ will denote the finite field with q elements where q is a power of an odd prime. $R = \mathbb{F}_q[T]$ is the polynomial ring with coefficients in $\mathbb{F}_q$ over the indeterminate T and the function field $\mathbb{F}_q(T)$ is the field of fractions of R. We will assume that g is an odd integer that is relatively prime to q.

The symbol p will always represent a monic irreducible polynomial in R. The symbols n and m will also be monic (but not necessarily irreducible) polynomials in R of degrees j and k respectively. The expression $\sum_m f(m)$ would mean to sum $f(m)$ over all monic polynomials m of fixed degree k. If a and b are elements of R, then (a, b) represents the greatest common (monic) divisor of a and b. If a and b are ordinary integers then (a, b) will denote the greatest common divisor in the usual sense.

3. Class groups with elements of order g

In the following lemma we construct quadratic extensions of $\mathbb{F}_q(T)$ whose class groups contain elements of order g.

Lemma 1. *Let g be a positive integer ≥ 3. Assume $n, m \in R$ are monic, $-a \in \mathbb{F}_q^{\times}$ is not a square, $\deg(m^g) > \deg(n^2)$, and $D = n^2 - am^g$ is squarefree. Then the class group for $\mathbb{F}_q(T, \sqrt{D})$ has an element of order g.*

Proof. First we note that $(n, m) = 1$ because if there were a common factor of n and m then D would not be squarefree. We factor am^g as

$$am^g = n^2 - D = (n + \sqrt{D})(n - \sqrt{D}).$$

Suppose $I|(n + \sqrt{D})$ and $I|(n - \sqrt{D})$. Then $n + \sqrt{D} \in I$ and $n - \sqrt{D} \in I$ which implies that $n, D \in I$ and $I = R = \mathbb{F}_q[T]$. Thus the ideals $(n + \sqrt{D})$

and $(n-\sqrt{D})$ are relatively prime. Therefore

$$(m)^g = (n+\sqrt{D})(n-\sqrt{D}) = \mathfrak{a}^g\mathfrak{a}'^g$$

where $\mathfrak{a}$ and $\mathfrak{a}'$ are ideals such that $(n+\sqrt{D}) = \mathfrak{a}^g$ and $(n-\sqrt{D}) = \mathfrak{a}'^g$. Taking norms we find that $N(m) = q^{2\deg(m)} = N(\mathfrak{a})^2$ so that $N(\mathfrak{a}) = q^{\deg(m)}$. Now suppose that $\mathfrak{a}^r$ is principal for some $r < g$:

$$\mathfrak{a}^r = (u + v\sqrt{D}).$$

Then

$$N(\mathfrak{a})^r = q^{r\deg(m)} = N(u+v\sqrt{D}) = q^{\deg(u^2-v^2D)}$$

and because the leading coefficient of v^2D is not a square this is

$$\begin{aligned}&\geq q^{\deg(D)} = q^{\deg(n^2-am^g)} = q^{\deg(m^g)}\\ &= N(\mathfrak{a})^g.\end{aligned}$$

This is a contradiction unless $r = g$. □

4. How often is $D = n^2 - am^g$ squarefree?

In light of Lemma 1 we would like to construct a lower bound on the number of squarefree expressions $D = n^2 - am^g$ as n and m vary such that $\deg(n) = j$ and $\deg(m) = k$ and $\deg(m^g) > \deg(n^2)$. Regarding k as the independent parameter we will maximize the number of possible values of D by choosing j to be the optimally large value $j = \lfloor gk/2 \rfloor$ if gk is odd or $j = \lfloor gk/2 \rfloor - 1$ if gk is even. Let $s(h)$ be 1 or 0 according as h is squarefree or not. Also let

$$s_z(h) = \begin{cases} 1 & \text{if } d^2 \text{ does not divide } h \text{ whenever } 1 \leq \deg(d) \leq z \\ 0 & \text{otherwise.}\end{cases}$$

We would like estimate the sum

$$\sum_{\substack{\deg(m)=k\\ \deg(n)=j}} s(n^2 - am^g).$$

Lemma 2. *By counting expressions $n^2 - am^g$ that are squarefree in the small factors we obtain the following sieving inequality:*

$$\sum_{m,n} s_z(n^2-am^g) \geq \sum_{m,n} s(n^2-am^g) \geq \sum_{m,n} s_z(n^2-am^g) - \sum_{\substack{m,n,p\\ \deg(p)>z\\ n^2-am^g\equiv 0(p^2)}} 1.$$

With an appropriate choice of z (depending on k) we will show that for large k

$$\begin{aligned}&\#\{\text{distinct squarefree values of } n^2 - am^g\}\\ &\sim \sum_{m,n} s(n^2 - am^g) \sim \sum_{m,n} s_z(n^2 - am^g)\\ &\gg q^{j+k}.\end{aligned}$$

Several auxiliary functions will be useful for estimating the terms in Lemma 2. Define the Möbius μ function on the nonzero elements of R. If $h \in R$ has factorization $ap_1^{\alpha_1} \cdots p_t^{\alpha_t}$ where $a \in \mathbb{F}_q$ and the p_i are irreducible monic polynomials in R then

$$\mu(h) = \begin{cases} 1 & \text{if } h \in \mathbb{F}_q^\times, \\ (-1)^t & \text{if } \alpha_i = 1 \text{ for all } i, \\ 0 & \text{otherwise.} \end{cases}$$

For $z \geq 1$ let

$$P(z) = \prod_{\substack{\text{irreducible } p \\ \deg(p) \leq z}} p$$

and let

$$N_{m,z}(j) = \sum_{\deg(n)=j} s_z(n^2 - am^g).$$

For fixed $m, h \in R$ let

$$\rho_m(h) = \#\{n \in R/hR \,:\, n^2 - am^g \equiv 0(h)\}.$$

Thus $\rho_m(h)$ is the number of $n \in R/hR$ satisfying the congruence $n^2 - am^g \equiv 0 \pmod h$.

We will use the following elementary estimate several times:

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

Proof. Since $q^u = \sum_{d|u} d\,\pi(d)$, the upper bound is clear. ☐

Lemma 4.

(1) $\rho_m(d_1 d_2) = \rho_m(d_1)\rho_m(d_2)$ *if d_1 and d_1 are coprime.*
(2) $\rho_m(p^2) = q^{\deg(p)}$ *if p is irreducible and p divides m.*
(3) $\rho_m(p^2) \leq 2$ *if p is irreducible and p does not divide m.*
(4) $\rho_m(d^2) \leq 2^{\nu(d)} q^{\deg(m)}$ *for squarefree d where $\nu(d)$ is the number of distinct monic irreducible polynomials of degree ≥ 1 that divide d.*

Proof. The multiplicativity of ρ_m is an immediate consequence of the Chinese remainder theorem.

Suppose that n satisfies $n^2 - am^g \equiv 0(p^2)$ with p dividing m. Then p divides n. There are exactly $q^{\deg(p)}$ multiples of p modulo p^2.

Suppose that n satisfies $n^2 - am^g \equiv 0(p^2)$ but that p does not divide m. The solution n must be a 'lift' of a solution modulo p. That is $n = n_1 + pt$ where $n_1^2 - am^g \equiv 0(p)$. We know there are at most two solutions of the congruence modulo p. Then

$$0 \equiv (n_1 + pt)^2 - am^g \equiv (n_1^2 - am^g) + 2n_1pt \pmod{p^2}$$

implies

$$0 \equiv \frac{n_1^2 - am^g}{p} + 2n_1t \pmod{p}.$$

When p does not divide n and $(2, q) = 1$ there is a unique $t \pmod{p}$ satisfying the last congruence. Thus the solution $n_1 \pmod{p}$ gives rise to a unique solution $n \pmod{p^2}$. Therefore, in this case, $\rho_n(p) \leq 2$.

Now let $\nu(d)$ represent the number of distinct nonconstant monic polynomials dividing d where d is squarefree. Then

$$\rho_m(d) = \prod_{\substack{p|d \\ p|m}} \rho_m(p^2) \prod_{\substack{p|d \\ (p,m)=1}} \rho_m(p^2) \leq \prod_{\substack{p|d \\ p|m}} q^{\deg(p)} \prod_{\substack{p|d \\ (p,m)=1}} 2 \leq 2^{\nu(d)} q^{\deg(m)}.$$

□

The following lemma tells us a choice of z that allows the sieve in Lemma 2 to yield interesting information.

Lemma 5. *Given any $\epsilon > 0$ we can choose κ (independently of m) so that if $z = \kappa \log(k)$ then*

$$N_{m,z}(j) = q^j \prod_{\deg(p) \leq z} (1 - \rho_m(p^2) q^{-\deg(p^2)}) + O(q^{(1+\epsilon)k}).$$

Proof. Let $N_{m,z}(j) = \sum_{\deg(n)=j} s_z(n^2 - am^g)$. Then

$$N_{m,z}(j) = \sum_{\deg(n)=j} \sum_{\substack{d \text{ monic} \\ d^2|(n^2-am^g, P(z))}} \mu(d) = \sum_{\substack{d \\ d^2|P(z)}} \mu(d) \sum_{\substack{\deg(n)=j \\ n^2-am^g \equiv 0(d^2)}} 1.$$

If $j \geq \deg(d^2)$ then

$$\sum_{\substack{\deg(n)=j \\ n^2-am^g \equiv 0(d^2)}} 1 = \rho_m(d^2) q^{j-\deg(d^2)},$$

while if $j \leq \deg(d^2)$ then

$$\sum_{\substack{\deg(n)=j \\ n^2-am^g \equiv 0(d^2)}} 1 \leq \rho_m(d^2).$$

Thus

$$\begin{aligned} N_{m,z}(j) &= \sum_{d|P(z)} \mu(d)\{\rho_m(d^2)q^{j-\deg(d^2)} + O(\rho_m(d^2))\} \\ &= q^j \prod_{\deg(p)\le z} (1-\rho_m(p^2)q^{-\deg(p^2)}) + \sum_{d|P(z)} O(\rho_m(d^2)). \end{aligned}$$

Now

$$\begin{aligned} \sum_{d|P(z)} \rho_n(d^2) &\le q^{\deg(m)} \sum_{d|P(z)} 2^{\nu(d)} \\ &= q^{\deg(m)} \prod_{\deg(p)\le z} (1+2) \\ &\le q^{\deg(m)} 3^{q^z}. \end{aligned}$$

Given any $\epsilon > 0$ we can choose κ such that if $z = \kappa \log(k)$ then the last expression is bounded by $q^{\epsilon k}$ for sufficiently large k. Therefore for sufficiently large k we have

$$N_{m,z}(j) = q^j \prod_{\deg(p)\le z} (1-\rho_m(p^2)q^{-\deg(p^2)}) + O(q^{(1+\epsilon)k}).$$

□

Lemma 6. *We have the lower bound*

$$\sum_{m,n} s_z(n^2 - am^g) = \sum_m N_{m,z}(j) \gg q^{j+k}.$$

Proof. We notice that

$$\begin{aligned} \prod_{\deg(p)\le z} (1-\rho_m(p^2)q^{-\deg(p^2)}) &= \prod_{\substack{p|m \\ \deg(p)\le z}} (1-q^{-\deg(p)}) \prod_{\substack{(p,m)=1 \\ \deg(p)\le z}} (1-\rho_m(p^2)q^{-\deg(p^2)}) \\ &\ge \prod_{\substack{p|m \\ \deg(p)\le z}} (1-q^{-\deg(p)}) \prod_{\text{all } p} (1-2q^{-\deg(p^2)}) \\ &\gg \prod_{p|m} (1-q^{-\deg(p)}) = \sum_{d|m} \mu(d) q^{-\deg(d)}. \end{aligned}$$

Then we sum over m

$$\begin{aligned} &\sum_{\deg(m)=k} \prod_{\deg(p)\le z} (1-\rho_m(p^2)q^{-\deg(p^2)}) \\ &\gg \sum_{\deg(m)=k} \sum_{d|m} \mu(d) q^{-\deg(d)} = \sum_{\deg(d)\le k} \mu(d) q^{-\deg(d)} \cdot q^{k-\deg(d)} \\ &= q^k \sum_{\deg(d)\le k} \mu(d) q^{-2\deg(d)} = q^k\{(1-q^{-1}) + O(q^{-k})\} \gg q^k. \end{aligned}$$

Summing the expression in Lemma 5 as m varies such that $\deg(m) = k$ and applying the last inequality gives the lemma: $\sum_m N_{m,z}(j) \gg q^{j+k}$. $\square$

Lemma 7. $\sum_m \nu(m) \ll \log(k) q^k$

Proof.

$$\sum_m \nu(m) \leq \sum_{\substack{p \\ \deg(p) \leq k}} q^{k-\deg(p)} \leq q^k \sum_{u \leq k} q^{-u} \cdot \frac{q^u}{u} \ll \log(k) q^k.$$

$\square$

Lemma 8.

$$\sum_{\substack{m,n,p \\ \deg(p) > z \\ n^2 - am^g \equiv 0 (p^2)}} 1 = o(q^{i+j}).$$

Proof. We may write

$$\sum_{\substack{m,n,p \\ \deg(p) > z \\ n^2 - am^g \equiv 0 (p^2)}} 1 = \sum_m \sum_{\substack{p \\ \deg(p) > z}} M_{m,p}(j)$$

where

$$M_{m,p}(j) = \sum_{\substack{n \\ n^2 - am^g \equiv 0 (p^2)}} 1.$$

Because $M_{m,p}(j) = \rho_m(p^2) q^{j-\deg(p^2)}$ if $j \geq \deg(p^2)$ and $M_{m,p}(j) \leq \rho_m(p^2)$ if $j < \deg(p^2)$ we obtain an upper bound on $M_{m,p}(j)$

$$M_{m,p}(j) \leq \begin{cases} 2(q^{j-\deg(p^2)} + 1) & \text{if } (p,m) = 1, \\ q^{j-\deg(p)} & \text{if } p | m. \end{cases}$$

Summing over irreducible p results in

$$\begin{aligned} \sum_{z < \deg(p) \leq j} M_{m,p}(j) &\leq \sum_{\substack{z < \deg(p) \leq j \\ (p,m) = 1}} 2(q^{j-\deg(p^2)} + 1) + \sum_{\substack{z < \deg(p) \leq j \\ p | m}} q^{j-\deg(p)} \\ &\ll \frac{q^{j-z}}{z} + \frac{q^j}{j} + \nu(m) q^{j-z}. \end{aligned}$$

Then summing the last expression over m gives

$$\begin{aligned}\sum_m \sum_p M_{m,p}(j) &\ll \frac{q^{j+k-z}}{z} + \frac{q^{j+k}}{j} + q^{j-z}\sum_m \nu(m)\\ &\ll \frac{q^{j+k-z}}{z} + \frac{q^{j+k}}{j} + \log(k)q^{j+k-z}\\ &\ll q^{j+k}(\frac{1}{zq^z} + \frac{1}{j} + \frac{\log(k)}{q^z})\\ &= o(q^{j+k}).\end{aligned}$$

□

We have now shown (Lemmas 2, 6, and 8) that the number of squarefree values of $n^2 - am^g$ as m and n vary is

$$\sum_{m,n} s(n^2 - am^g) \gg q^{j+k}.$$

It remains to be shown that there is not too much duplication among the expressions $n^2 - am^g$.

Lemma 9. *The number of squarefree elements of the form $n^2 - am^g$ with $\deg(n) = j$ and $\deg(m) = k$ that are representable in more than one way is $o(q^{j+k})$.*

Proof. Let S be the collection of pairs (m, n) of monic polynomials m and n with $\deg(n) = j$ and $\deg(m) = k$ such that $n^2 - am^g$ is representable in more than one way. We will determine an upper bound for $|S|$ thereby proving the lemma. Let m_1 and m_2 be fixed unequal polynomials such that

$$n_1^2 - am_1^g = n_2^2 - am_2^g$$

for some n_1 and n_2. Then

$$a(m_1^g - m_2^g) = n_1^2 - n_2^2 = (n_1 - n_2)(n_1 + n_2)$$

which shows that the choices for n_1 and n_2 are determined by the divisors of $a(m_1^g - m_2^g)$. Since $\deg(m_1^g - m_2^g) < gk$, the worst possible case is when $a(m_1^g - m_2^g)$ is divisible by $gk - 1$ distinct monic linear factors. In this worst case the number of (not necessarily monic) divisors is

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

Notice that q is fixed but that we vary k. So, this is a very crude upper bound on the number of divisors when k is large relative to q.

There are q^k choices for m_1. Given m_1, the number of choices for n_1 is bounded by the number of choices for m_2 times the number of divisors of $m_1^g - m_2^g$. Thus the set S contains $O(q^{2k}2^{gk})$ pairs. Since $j = \lfloor gk/2 \rfloor$ or $\lfloor gk/2 \rfloor - 1$ and $q \geq 5$, we obtain $|S| = O(q^{2k}2^{gk}) = o(q^{j+k})$. □

We have now shown that there are $\gg q^{j+k}$ distinct values of $D = n^2 - am^g$. Since $j = \lfloor gk/2 \rfloor$ or $j = \lfloor gk/2 \rfloor - 1$ there are $\gg q^{gk(\frac{1}{2}+\frac{1}{g})}$ distinct values of D. Therefore there are $\gg q^{\ell(\frac{1}{2}+\frac{1}{g})}$ quadratic extensions $\mathbb{F}_q(T, \sqrt{D})$ of $\mathbb{F}_q(T)$ such that $\deg(D) \leq \ell$.

This completes the proof of the theorem stated at the beginning.

Acknowledgment. We wish to thank Yu-Ru Liu for her willingness to go over the details of this paper with the first author. Also we are grateful to the reviewer for suggesting an improvement to the proof of the theorem.

References

[1] E. Artin, *Quadratische Körper im Gebiet der höheren Kongruenzen I, II*, Math. Zeitschrift **19** (1924) 153-246.
[2] N. Ankeny and S. Chowla, *On the divisibility of the class numbers of quadratic fields*, Pacific Journal of Math., **5** (1955) p. 321-324.
[3] H. Cohen and H.W. Lenstra Jr., *Heuristics on class groups of number fields*, Springer Lecture Notes, **1068** in Number Theory Noordwijkerhout 1983 Proceedings.
[4] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields, II*, Proc. Royal Soc., A **322** (1971), p. 405-420.
[5] R. Gupta and M. Ram Murty, *Class groups of quadratic functions fields*, in preparation.
[6] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over finite fields*, in Théorie des nombres (Quebec, PQ 1987), p. 227-239, de Gruyter, Berlin, 1989.
[7] Christian Friesen, *Class number divisibility in real quadratic function fields*, Canad. Math. Bull., Vol. **35**(3), 1992, p. 361-370.
[8] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by* 3, J. Number Theory, **6** (1974), 276-278.
[9] T. Honda, *A few remarks on class numbers of imaginary quadratic fields*, Osaka J. Math., **12** (1975), 19-21.
[10] M. Ram Murty, *The ABC conjecture and exponents of class groups of quadratic fields*, Contemporary Mathematics, Volume **210**, 1998, pages 85-95.
[11] M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in Number Theory (University Park, PA, 1997), 229-239, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999.
[12] T. Nagell, *Über die Klassenzahl imaginär quadratischer Zahlkörper*, Abh. Math. Seminar Univ. Hamburg, **1** (1922), p. 140-150.
[13] P. Weinberger, *Real Quadratic Fields with Class Numbers Divisible by n*, Journal of Number Theory, **5** (1973) p. 237-241.
[14] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math., **7** (1970) 57-76.
[15] Jiu-Kang Yu, *Toward the Cohen-Lenstra conjecture in the function field case*, preprint.

David A. Cardon, Department of Mathematics, Brigham Young University, Provo, Utah 84602, USA

E-mail address: `cardon@math.byu.edu`

M. Ram Murty, Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, CANADA

E-mail address: `murty@mast.queensu.ca`