

## EXPONENTS OF CLASS GROUPS OF REAL QUADRATIC FUNCTION FIELDS

KALYAN CHAKRABORTY AND ANIRBAN MUKHOPADHYAY

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. We show that there are  $\gg q^{l/(2g)}$  polynomials  $D \in \mathbb{F}_q[t]$  with  $\deg(D) \leq l$  such that the ideal class group of the real quadratic extensions  $\mathbb{F}_q(t, \sqrt{D})$  has an element of order  $g$ .

### 1. INTRODUCTION

In a recent paper R. Murty [4] shows that if  $g$  is a fixed integer  $\geq 3$ , then the number of imaginary quadratic fields with absolute discriminant  $\leq x$  and whose class group contains an element of order  $g$  is  $\gg x^{1/2+1/g}$ . He also proved that the number of such real quadratic fields is  $\gg x^{1/(2g)}$ . Let  $q$  be a power of an odd prime. Let  $R = \mathbb{F}_q[t]$  be the polynomial ring over the finite field  $\mathbb{F}_q$  of  $q$  elements, and let  $\mathbb{F}_q^*$  be the group of nonzero elements of  $\mathbb{F}_q$ . Let  $\mathbb{F}_q(t)$  be the field of fractions of  $R$ . If  $D \in R$  is squarefree, then we consider the quadratic extension  $\mathbb{F}_q(t, \sqrt{D})$  of  $\mathbb{F}_q(t)$ . For preliminaries and related references we refer to the papers by R. Murty and Cardon [1], Friesen and van Wamelen [3], and for general number theory in function fields we refer to the recently published book by M. Rosen [5].

R. Murty and D. Cardon [1] proved that there are  $\gg q^{l(1/2+1/g)}$  quadratic extensions  $\mathbb{F}_q(t, \sqrt{D})$  of  $\mathbb{F}_q(t)$  with  $\deg(D) \leq l$  whose ideal class group has an element of order  $g$ . This result is the function field analogue of the result of R. Murty for imaginary quadratic fields.

A quadratic function field  $K = \mathbb{F}_q(t, \sqrt{D})$  is said to be real if  $\infty$  splits completely in  $K$ , and imaginary otherwise. It follows from proposition 14.6 of Rosen [5, p. 248] that  $K$  is a real quadratic extension if  $D$  is monic with  $\deg(D)$  even. We prove the following function field analogue of R. Murty's [4] result for real quadratic number fields.

**Theorem 1.** *Let  $q$  be a power of an odd prime, and let  $g$  be a fixed positive integer  $\geq 3$ . Then there are  $\gg q^{l/(2g)}$  real quadratic extensions  $\mathbb{F}_q(t, \sqrt{D})$  of the rational function field  $\mathbb{F}_q(t)$  such that  $\deg(D) \leq l$  and the ideal class group of  $\mathbb{F}_q(t, \sqrt{D})$  has an element of order  $g$ .*

---

Received by the editors September 4, 2002 and, in revised form, April 21, 2003.  
2000 *Mathematics Subject Classification.* Primary 11R58; Secondary 11R29.  
*Key words and phrases.* Class group, real quadratic fields.

2. LEMMAS

The following result, due to Friesen [2], constructs real quadratic extensions of  $\mathbb{F}_q(t)$  whose class group contains an element of order  $g$ .

**Lemma 1.** *Let  $g$  be a positive integer, and let  $m \in R$  be monic. Let  $D = m^{2g} + a^2$  with  $a \in \mathbb{F}_q^*$ . If  $D$  is squarefree, then the class group of  $\mathbb{F}_q(t, \sqrt{D})$  contains an element of order  $g$ .*

In fact, as a corollary he also shows that there exist infinitely many such quadratic extensions of  $\mathbb{F}_q(t)$  whose class group contains an element of order  $g$ . We are going to find a lower bound for the number of squarefree polynomials of the form  $D = m^{2g} + a^2$  as  $m$  varies over monic polynomials of degree  $k$ . We follow the method of Murty and Cardon [1]. We begin by introducing some notation similar to that of [1]. Let  $s(h)$  be 1 or 0 according as  $h$  is squarefree or not. Also define

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

Our aim is to estimate the sum

$$\sum_{\deg(m)=k} s(m^{2g} + a^2).$$

The following sieving inequality is obvious.

**Lemma 2.**

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

We now define a few functions which will be used in the proof. If  $h \in R$  has the factorisation  $ap_1^{\alpha_1} \cdots p_r^{\alpha_r}$  where  $a \in \mathbb{F}_q$  and  $p_i$  are irreducible monic polynomials in  $R$ , then

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

For  $z \geq 1$  let

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

and

$$M_z(k) = \sum_{\deg(m)=k} s_z(m^{2g} + a^2).$$

For fixed  $h \in R$  we also define

$$\rho(h) = \#\{m \in R/hR : m^{2g} + a^2 \equiv 0(h)\}.$$

We state without proof the following elementary estimate.

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

The next lemma gives some properties of the function  $\rho$  defined above.

**Lemma 4.** (i)  $\rho(h_1h_2) = \rho(h_1)\rho(h_2)$  if  $h_1$  and  $h_2$  are coprime.  
 (ii)  $\rho(p^2) \leq 2g$ .

*Proof.* The multiplicativity of  $\rho$  is an immediate consequence of the Chinese remainder theorem.

Let us suppose that  $m^{2g} + a^2 \equiv 0(p^2)$ . Then the solution must be a lift of a solution modulo  $p$ , i.e.,  $m = m_1 + ph$ , where  $m_1^{2g} + a^2 \equiv 0(p)$ . There are at most  $2g$  solutions of this last congruence modulo  $p$ . We have

$$0 \equiv (m_1 + ph)^{2g} + a^2 \equiv m_1^{2g} + a^2 + 2gm_1^{2g-1}ph \pmod{p^2}.$$

Thus

$$0 \equiv \frac{m_1^{2g} + a^2}{p} + 2gm_1^{2g-1}h \pmod{p}.$$

Since  $p$  does not divide  $m$  and  $(g, 2) = 1$ , there is a unique solution for  $h$  modulo  $p$ . Thus a solution  $m_1$  modulo  $p$  gives rise to a unique solution modulo  $p^2$ . Therefore  $\rho(p^2) \leq 2g$ . □

The following lemma estimates the main term with a specific choice of  $z$ .

**Lemma 5.** *We have the lower bound*

$$M_z(k) \gg q^k$$

for sufficiently large  $k$  and for a specific choice of  $z$  depending on  $k$ .

*Proof.* We have

$$\begin{aligned} M_z(k) &= \sum_{\substack{m \\ \deg(m)=k}} s_z(m^{2g} + a^2) = \sum_{\deg(m)=k} \sum_{\substack{d \text{ monic} \\ d^2 | (m^{2g} + a^2, P(z))}} \mu(d) \\ &= \sum_{d^2 | P(z)} \sum_{\substack{m \\ \deg(m)=k \\ d^2 | m^{2g} + a^2}} 1. \end{aligned}$$

If  $k \geq \deg(d^2)$ , then

$$\sum_{\substack{m \\ \deg(m)=k \\ d^2 | m^{2g} + a^2}} 1 = \rho(d^2)q^{k - \deg(d^2)},$$

and if  $k < \deg(d^2)$ , we have

$$\sum_{\substack{m \\ \deg(m)=k \\ d^2 | m^{2g} + a^2}} 1 = \rho(d^2).$$

Thus

$$\begin{aligned} M_z(k) &= \sum_{d^2 | P(z)} \mu(d) \left\{ \rho(d^2)q^{k - \deg(d^2)} + \rho(d^2) \right\} \\ &= q^k \prod_{\substack{p \\ \deg(p) \leq z}} \left( 1 - \rho(p^2)q^{-\deg(p^2)} \right) + \sum_{d | P(z)} O(\rho(d^2)). \end{aligned}$$

Defining  $\nu(d)$  to be the number of monic irreducible polynomials dividing  $d$ , we get

$$\begin{aligned} \sum_{d|P(z)} \rho(d^2) &\leq \sum_{d|P(z)} (2g)^{\nu(d)} \\ &= \prod_{\substack{p \\ \deg(p) \leq z}} (1 + 2g) \leq (3g)^{q^z}. \end{aligned}$$

Hence given any  $\epsilon > 0$  we can choose  $c$  so that if  $z = c \log(k)$ , then

$$\sum_{d|P(z)} \rho(d^2) = O(q^{\epsilon k}).$$

Now

$$\prod_{\substack{p \\ \deg(p) \leq z}} \left(1 - \rho(p^2)q^{-\deg(p^2)}\right) \geq \prod_{\substack{p \\ \deg(p) \leq z}} \left(1 - 2gq^{-2\deg(p)}\right).$$

The last product is convergent as  $z \rightarrow \infty$ . Thus

$$M_z(k) \gg q^k.$$

□

Now we estimate the other term of the inequality of Lemma 2.

**Lemma 6.**

$$\sum_{\substack{m,p \\ \deg(p) > z \\ m^{2g} + a^2 \equiv 0(p^2)}} 1 = o(q^k).$$

*Proof.* We write

$$\sum_{\substack{m,p \\ \deg(p) > z \\ m^{2g} + a^2 \equiv 0(p^2)}} 1 = \sum_{\substack{p \\ \deg(p) > z}} H_p,$$

where

$$H_p = \sum_{\substack{m \\ m^{2g} + a^2 \equiv 0(p^2)}} 1.$$

If  $k \geq \deg(p^2)$ , we have  $H_p = \rho(p^2)q^{k-\deg(p^2)} \leq 2gq^{k-\deg(p^2)}$ . If  $k < \deg(p^2)$ , then  $H_p = \rho(p^2) \leq 2g$ . We observe that  $p^2$  divides  $m^{2g} + a^2$ , and this implies that  $p$  divides its formal derivative  $2gm^{2g-1}m'$ , where  $m'$  is the formal derivative of  $m$ . Since  $(p, m) = 1$ , we conclude that  $p$  divides  $m'$ . Thus  $\deg(p) \leq \deg(m') < \deg(m) = k$ . Combining all these, we get

$$\begin{aligned} \sum_{\substack{m,p \\ \deg(p) > z \\ m^{2g} + a^2 \equiv 0(p^2)}} 1 &= \sum_{\substack{p \\ z < \deg(p) < k}} H_p \\ &\leq \sum_{z < \deg(p) < k} (2g(q^{k-\deg(p^2)} + 1)) \\ &= 2gq^k \sum_{z < \deg(p) < k} q^{-\deg(p^2)} + 2g \sum_{z < \deg(p) < k} 1 \\ &\ll \frac{q^{k-z}}{z} + \frac{q^k}{k} = o(q^k). \end{aligned}$$

□

## 3. PROOF OF THE THEOREM

We have shown that for a fixed  $k$  there are  $\gg q^k$  monic squarefree polynomials  $D = m^{2g} + a^2$ . Thus there are  $\gg q^{l/(2g)}$  such polynomials  $D$  with  $\deg(D) \leq l$ . By Lemma 1 the corresponding real quadratic extensions  $\mathbb{F}_q(t, \sqrt{D})$  have an element of order  $g$  in their class groups. We observe that distinct choices of  $m$  give rise to distinct real quadratic function fields  $\mathbb{F}_q(t, \sqrt{D})$ . This completes the proof of the theorem.

## ACKNOWLEDGMENT

We thank C. Friesen for making his Ph.D. thesis available to us.

## REFERENCES

- [1] David A. Cardon and M. Ram Murty, *Exponents of class groups of quadratic function fields over finite fields*, Canadian Math. Bulletin **44** (2001), no. 4, 398–407. MR **2002g**:11164
- [2] Christian Friesen, *Class number divisibility in real quadratic function fields*, Canadian Math. Bulletin **35** (1992), no. 3, 361–370. MR **93h**:11130
- [3] Christian Friesen and Paul van Wamelen, *Class numbers of real quadratic function fields*, Acta Arith. **81** (1997), no. 1, 45–55. MR **98d**:11141
- [4] M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in Number Theory (University Park, PA, 1997), Math. Appl. **467**, Kluwer Acad. Publ., Dordrecht, 1999, 229–239. MR **2000b**:11123
- [5] Michael Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics **210**, Springer-Verlag, Berlin, 2002. MR **2003d**:11171

HARISH-CHANDRA RESEARCH INSTITUTE, CHHATNAG ROAD, JHUSI, ALLAHABAD 211 019, INDIA  
E-mail address: [kalyan@mri.ernet.in](mailto:kalyan@mri.ernet.in)

HARISH-CHANDRA RESEARCH INSTITUTE, CHHATNAG ROAD, JHUSI, ALLAHABAD 211 019, INDIA  
E-mail address: [anirban@mri.ernet.in](mailto:anirban@mri.ernet.in)  
Current address: The Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600113, India  
E-mail address: [anirban@imsc.res.in](mailto:anirban@imsc.res.in)