EXPONENTS OF CLASS GROUPS
OF REAL QUADRATIC FUNCTION FIELDS (II)

KALYAN CHAKRABORTY AND ANIRBAN MUKHOPADHYAY

(Communicated by Wen-Ching Winnie Li)

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

1. INTRODUCTION

R. Murty [8] showed that if g is an odd positive integer, then for every $\epsilon > 0$, the number of real quadratic fields with discriminant $\le x$ and whose class group contains an element of order g is $\gg x^{1/2g-\epsilon}$. G. Yu [10] improved this result to $\gg x^{1/g-\epsilon}$ for any odd integer g. In a recent work F. Luca [7] shows that the number of such real quadratic fields is $\gg x^{1/G}/\log x$ where $G := \mathrm{lcm}[g, 2]$. This establishes Yu's improvement of Murty's estimate in the cases when g is even. The problem of divisibility of class numbers of quadratic fields has a long history, and the interested reader is referred to the papers of R. Murty [8], K. Chakraborty and R. Murty [6].

We would like to study the same question in the function field setup. We refer to the book of M. Rosen [9] for general number theory in function fields.

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 $\mathbb{F}_q^\star$ be the group of non-zero 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 $\mathbb{F}_q(t)$. A quadratic function field $k = \mathbb{F}_q(t, \sqrt{D})$ is said to be real if ∞ splits completely in k and imaginary otherwise. It follows that k is a real quadratic extension if D is monic with $\deg(D)$ even.

For the history of the divisibility of the class number problem in the case of quadratic function fields and related references we refer to the works of R. Murty and D. Cardon [2], C. Friesen [4], C. Friesen and P. van Wamelen [5]. The present authors recently showed [3] that 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 $\deg(D) \le l$ and the ideal class group of $\mathbb{F}_q(t, \sqrt{D})$ has an element of order g. This result is the function field analogue of R. Murty's [8] result for real quadratic number fields. In this note, generalizing the argument of F. Luca [7] in the function field setup, we improve upon our previous estimate obtained in [3] in the cases when g is even. The result is as follows.

Theorem 1. *Let q be a power of an odd prime and let g be a fixed positive even integer. Then there are $\gg q^{l/g}/l^2$ 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 ideal class group of $\mathbb{F}_q(t, \sqrt{D})$ has an element of order g.*

Remark 1. For odd g, the present method gives a weaker estimate than the one obtained in [3].

2. Lemmas

We start with the following lemma about Pell's equations over $\mathbb{F}_q(t)$. For details about such Pell equations, we refer to [1].

Lemma 1. *For a fixed $D \in \mathbb{F}_q[t]$, define*
$$S = \{x \in \mathbb{F}_q[t] \mid \deg(x) \leq l, \ x^2 - Dy^2 = -1\}.$$
Then $|S| \ll l$.

Proof. Let (x_0, y_0) be a fundamental solution of the Pell equation

(1) $$x^2 - Dy^2 = -1.$$

Suppose $x \in S$. Then (x, y) is a solution of (1) for some $y \in \mathbb{F}_q[t]$. Now from [1], we write
$$x + y\sqrt{D} = \pm(x_0 + y_0\sqrt{D})^m, \text{ for some } m \in \mathbb{Z}.$$
We can assume that $m > 0$; otherwise we change y_0 to $-y_0$. Now we claim that
$$\deg[(x_0 + y_0\sqrt{D})^m + (x_0 - y_0\sqrt{D})^m] = m \deg(x_0).$$
We prove it by induction. The case $m = 1$ is obvious. Thus we suppose $m \geq 2$. First we observe from (1) that $\deg(x_0^2) = \deg(D) + \deg(y_0^2)$. Let $(x_0 + y_0\sqrt{D})^{m-1} = R + T\sqrt{D}$. Then by the induction hypothesis $\deg(R) = (m-1)\deg(x_0)$. Further, (R, T) is also a solution of (1); hence $\deg(R^2) = \deg(T^2 D)$. Now,
$$(x_0 + y_0\sqrt{D})^m + (x_0 - y_0\sqrt{D})^m = 2(x_0 R + y_0 T D).$$
We see that
$$\deg(T^2 y_0^2 D^2) = \deg(T^2 D) + \deg(y_0^2 D) = \deg(R^2) + \deg(x_0^2).$$
This implies $\deg(y_0 T D) = \deg(x_0 R)$. Thus
$$\deg[(x_0 + y_0\sqrt{D})^m + (x_0 - y_0\sqrt{D})^m] = \deg(x_0 R),$$
and the claim follows.

Therefore, we have
$$m \deg(x_0) = \deg[(x_0 + y_0\sqrt{D})^m + (x_0 - y_0\sqrt{D})^m] = \deg(x) \leq l.$$
Hence S can have at most $l/\deg(x_0)$ elements, which proves the lemma. $\square$

Let $\left(\frac{\cdot}{P}\right)_r$ denote the r-th power Legendre symbol for an irreducible monic polynomial P and a positive integer r. We set
$$\mathcal{P} = \{P \in \mathbb{F}_q[t] \mid P \text{ is irreducible and } \left(\frac{2}{P}\right)_r \neq 1 \ \forall r|g, \ r \text{ prime}\}.$$

For $P \in \mathcal{P}$, write $P^g + 1 = Dz^2$. We consider the field $k = \mathbb{F}_q(t, \sqrt{D})$. Let $\mathcal{O}_k$ and h_k be the ring of integers and the class number of k respectively. Now we have the following lemma about divisibility of h_k.

Lemma 2. g *divides* h_k.

Proof. It is known that $\mathcal{O}_k$ has a basis of the form $\{1, \sqrt{D}\}$. Clearly P splits completely in $\mathcal{O}_k$ as D is a square modulo P. Let $P\mathcal{O}_k = \pi_1 \pi_2$ where π_1 and π_2 are two ideals of $\mathcal{O}_k$. Thus

$$\pi_1^g \pi_2^g = P^g \mathcal{O}_k = \langle 1 + z\sqrt{D} \rangle \langle 1 - z\sqrt{D} \rangle.$$

Since $\langle 1 + z\sqrt{D} \rangle$ and $\langle 1 - z\sqrt{D} \rangle$ are relatively coprime, we can assume that $\pi_1^g = \langle 1 + z\sqrt{D} \rangle$. If we denote the order of π_1 in the class group of k by $\mathrm{Ord}(\pi_1)$, then $\mathrm{Ord}(\pi_1)$ divides g. It is now enough to prove that $\mathrm{Ord}(\pi_1) = g$. If not, suppose $\mathrm{Ord}(\pi_1) = l$, where $l|g$ and $l < g$. Then we can find a prime number r dividing g/l such that $\pi_1^g = \langle \alpha^r \rangle$ with $\alpha := u + v\sqrt{D}$; $u, v \in \mathbb{F}_q[t]$. Since π_1^g is a principal ideal generated by $1 + z\sqrt{D}$, we can write

$$(2) \qquad\qquad 1 + z\sqrt{D} = \epsilon \alpha^r \zeta^s$$

where ζ is the fundamental unit of $\mathcal{O}_k$ and $\epsilon = \pm 1$. Without loss of generality, we can assume that $s < 0$ and $\epsilon = 1$. Considering the norm of both sides of (2), we get

$$-P^g = 1 - Dz^2 = N(1 + z\sqrt{D}) = N(\alpha)^r.$$

This implies $u^2 - v^2 D = -P^{g/r}$. Putting $s = -s_1$, we rewrite (2) as $(1 + z\sqrt{D})\zeta^{s_1} = \alpha^r$. Clearly, $(P^{g/2}, z)$ is a solution of (1), so $P^{g/2} + z\sqrt{D} = \zeta^{r_0}$, for some $r_0 \in \mathbb{Z}$. Thus we get

$$(1 + z\sqrt{D})^{r_0}(\zeta^{r_0})^{s_1} = \alpha^{r_0 r} = (u + v\sqrt{D})^{r_0 r}.$$

This implies

$$(1 + \sqrt{P^g + 1})^{r_0}(P^{g/2} + \sqrt{P^g + 1})^{s_1} = (u + \sqrt{u^2 + P^{g/r}})^{r_0 r}.$$

Hence,

$$\begin{aligned}
(1 \;\; + \;\; &\sqrt{P^g + 1})^{r_0}(P^{g/2} + \sqrt{P^g + 1})^{s_1} \\
+ \;\; &(1 - \sqrt{P^g + 1})^{r_0}(P^{g/2} - \sqrt{P^g + 1})^{s_1} \\
= \;\; &(u + \sqrt{u^2 + P^{g/r}})^{r_0 r} + (u - \sqrt{u^2 + P^{g/r}})^{r_0 r}.
\end{aligned}$$

Reading the above equation modulo P, we get

$$2 \equiv (2u)^{r_0 r} \text{ modulo } P.$$

This is a contradiction as 2 is not an r-th power modulo P, by definition of $\mathcal{P}$. Hence the lemma follows. $\qquad\qquad\square$

3. Proof of the theorem

We consider the quadratic extensions $\mathbb{F}_q(t, \sqrt{D})$ of $\mathbb{F}_q(t)$ for $P \in \mathcal{P}$. By Lemma 1, the number of $P \in \mathcal{P}$ giving the same D is $\ll l$. By the Chebotarev density theorem in the function field, it follows that

$$|\mathcal{P}| \gg \frac{q^{l/g}}{l}.$$

This completes the proof of the theorem.

Acknowledgements

References

[1] Asako Nakamura: Pell's equation on function fields. (in Japanese), *Sugaku*, **54**, no. 3(1995), 308–313. MR1929899 (2003g:11026)

[2] David A. Cardon and M. Ram Murty: Exponents of class groups of quadratic function fields over finite fields, *Canadian Math. Bulletin*, Vol.**44** (2001), no. 4, 398-407. MR1863632 (2002g:11164)

[3] Kalyan Chakraborty and Anirban Mukhopadhyay: Exponents of class groups of real quadratic function fields, *Proc. Amer. Math. Soc.* **132** (2004), 1951–1955. MR2053965 (2005a:11182)

[4] Christian Friesen : Class number divisibility in real quadratic function fields, *Canad. Math. Bull.*, Vol.**35**(3), (1992), 361–370. MR1184013 (93h:11130)

[5] Christian Friesen and Paul van Wamelen: Class numbers of real quadratic function fields, *Acta Arith.* **81** (1997), no. 1, 45-55. MR1454155 (98d:11141)

[6] K. Chakraborty and M. Ram Murty: On the number of real quadratic fields with class number divisible by 3, *Proc. Amer. Math. Soc.* **131** (2002), no. 1, 41-44. MR1929021 (2003m:11184)

[7] Florian 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. MR1999181 (2004g:11099)

[8] 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. MR1691322 (2000b:11123)

[9] Michael Rosen: Number Theory in Function Fields, *Graduate Texts in Mathematics*, **210**. Springer-Verlag, 2002. MR1876657 (2003d:11171)

[10] Gang Yu: A note on the divisibility of class numbers of real quadratic fields, *J. Number Theory* **97** (2002), 35-44. MR1939135 (2003m:11187)

Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, India
E-mail address: kalyan@mri.ernet.in

Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India
E-mail address: anirban@imsc.res.in