Indivisibility of class numbers of imaginary quadratic function fields

Dongho Byeon (Seoul) *†‡

Abstract. We show that for an odd prime number l, there are infinitely many imaginary quadratic extensions F over the rational function field $K = \mathbb{F}_q(T)$ such that the class number of F is not divisible by l.

1 Introduction

Let p be an odd prime number, q a power of p and $\mathbb{F}_q$ the finite field with cardinality q. Let T be an indeterminate and $K = \mathbb{F}_q(T)$ the rational function field. Let $A = \mathbb{F}_q[T]$ and $A^{(1)}$ be the set of all non-zero monic polynomials in A.

There have been many works on the divisibility of class numbers of function fields F over K. For examples, Friesen [3], Cardon and Murty [1], respectively, proved that there are infinitely many real and imaginary, respectively, quadratic extensions F over K such that the class number of F is divisible by l, which is a function field analogue of well-known result on the quadratic number fields.

However, much less is known on the indivisibility. In [6], Kimura proved that there are infinitely many quadratic extensions F over K such that the class number of F is not divisible by 3. For an odd prime number l, Ichimura [5] constructed infinitely many imaginary quadratic extensions F over K such that the class number of F is not divisible by l, when the order of q mod l in the multiplicative group $(\mathbb{Z}/l\mathbb{Z})^*$ is odd or $l = p$.

In this paper, we shall show the following theorem.

*2000 *Mathematics Subject Classification*: Primary 11R58; Secondary 11R11, 11R29.

†This work was supported by KRF-2005-070-C00004.

‡The author also holds joint appointment in the Research Institute of Mathematics, Seoul National University.

Theorem 1.1 *Let l be an odd prime number. Then there are infinitely many imaginary quadratic extensions F over K such that the class number of F is not divisible by l.*

Theorem 1.1 is a function field analogue of Hartung's work [4] on the imaginary quadratic number fields. To prove this theorem, following Hartung's idea in [4], we shall use the class number relation over function fields which is developed by Yu [8].

Remark. For number field case, the Cohen-Lenstra heuristics imply that if l is an odd prime number, then the probability l does not divide the class number of imaginary quadratic number field is

$$\prod_{i=1}^{\infty}(1-\frac{1}{l^i}).$$

For function field case, Lee [Section 3.3, 7] shows that the Friedman and Washington's conjectures [2] for the function field analogue of the Cohen-Lenstra heuristics imply that if l ($\neq p$) is an odd prime number, then the probability l does not divide the class number of imaginary quadratic function field is also

$$\prod_{i=1}^{\infty}(1-\frac{1}{l^i}).$$

2 Class number relation

For details, we refer to the paper of Yu [8]. Let $D \in A$ be a fundamental discriminant. Let $F = K(\sqrt{D})$ be the quadratic extension over $K = \mathbb{F}_q(T)$ and $\mathcal{O}_{Df^2} = A + A\sqrt{Df^2}$ the order of conductor $f \in A^{(1)}$ in F. The order of the finite group $\mathrm{Pic}(\mathcal{O}_{Df^2})$ is called the *class number* of discriminant Df^2 and is denoted by $h(Df^2)$.

From now on, we assume that $F = K(\sqrt{D})$ is imaginary, i.e., the place ∞ of K does not split in F. We also say that D and Df^2 are imaginary discriminants. Then we can define $\omega(Df^2) := \sharp\mathcal{O}^*_{Df^2}/(q-1)$ and $h'(Df^2) := h(Df^2)/\omega(Df^2)$. Let χ_D be the usual Kronecker character satisfying for prime $P \in A^{(1)}$, $\chi_D(P) = 1$ if P splits in F, $\chi_D(P) = 0$ if P ramifies in F and $\chi_D(P) = -1$ otherwise. For an element $x \in A$, we let $|x| := q^{\deg x}$.

Then for any fundamental imaginary discriminant D and conductor f, we have

$$h'(Df^2) = h'(D)|f|\prod_{P|f}(1-\frac{\chi_D(P)}{|P|}),$$

where the product runs over primes $P \in A^{(1)}$ dividing f. We define the Hurwitz class number $H(Df^2)$ as

$$H(Df^2) := \sum_{\substack{f' \in A^{(1)} \\ f' | f}} h'(Df'^2).$$

Yu obtained the following class number relation.

Theorem 2.1 *(Yu [8]) For any m in $A^{(1)}$,*

$$\sum_{\substack{t \in A \\ \mu \in K^*/K^{*2}}} H(t^2 - \mu m)$$

$$= \sum_{\substack{d \in A^{(1)} \\ d | m}} \max(|d|, |m/d|) - \sum_{\substack{d \in A^{(1)} \\ d | m \\ \deg d = 1/2 \deg m}} |m|^{-1/2} \frac{|m| - |m - d^2|}{q-1},$$

where the first sum runs over all such pairs $(t, \mu) \in A \times K^*/K^{*2}$ that $t^2 - \mu m$ is an imaginary discriminant or $t^2 - \mu m = 0$.

3 Proof of Theorem 1.1

For the case $l = p$, Ichimura already constructed infinitely many imaginary quadratic extensions F over K such that the class number of F is not divisible by l (See Theorem 3 in [5]). So in this section we consider the case $l \neq p$. We can choose m to satisfy the following;

(i) m is a prime in $A^{(1)}$ with odd degree M,
(ii) $\chi_D(m) = -1$ for all imaginary fundamental discriminant D with degree $\leq N$.

Then from the class number relation in Theorem 2.1 and the condition (i), we have

$$\sum_{\substack{t \in A \\ \mu \in K^*/K^{*2}}} H(t^2 - \mu m) = 2q^M.$$

Since $l \neq p$, there is a pair $(t, \mu) \in A \times K^*/K^{*2}$ such that

$$H(t^2 - \mu m) \not\equiv 0 \pmod{l}.$$

We can write

$$t^2 - \mu m = D_{t,\mu} f^2$$

for some imaginary fundamental discriminant $D_{t,\mu}$ and conductor f. By the definition of h' and Hurwitz class number, we have

$$h(D_{t,\mu}) \not\equiv 0 \pmod{l}.$$

From the condition (ii), the degree of $D_{t,\mu} > N$. Since N can be arbitrarily large, there are infinitely many imaginary fundamental discriminants D whose class number $h(D)$ is not divisible by l. □

Acknowledgement The authors thank the referee for some helpful suggestions.

References

[1] D. A. Cardon and M. R. Murty, Exponents of class groups of quadratic function fields over finite fields, Canadian Math. Bull. **44** (2001), 398–407.

[2] E. Friedman and L. Washington, On the distribution of divisor class groups of curves over a finite field, Theorie des nombres (Quebec, PQ, 1987), 227–239, de Gruyter, Berlin, 1989.

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

[4] 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.

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

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

[7] Y. Lee, Cohen-Lenstra heuristics and the Spiegelungssatz, Dissertation, Brown University, 1999.

[8] J. K. Yu, A class number relation over function fields, J. Number Theory **54** (1995), 318–340.

Department of Mathematics, Seoul National University
Seoul 151-747, Korea
E-mail: dhbyeon@math.snu.ac.kr