Bull. Korean Math. Soc. **50** (2013), No. 4, pp. 1357–1365
http://dx.doi.org/10.4134/BKMS.2013.50.4.1357

CLASS NUMBER DIVISIBILITY OF QUADRATIC FUNCTION FIELDS IN EVEN CHARACTERISTIC

Sunghan Bae and Hwanyup Jung

Abstract. We find a lower bound on the number of real/inert imaginary/ramified imaginary quadratic extensions of the function field $\mathbb{F}_q(t)$ whose ideal class groups have an element of a fixed order, where q is a power of 2.

1. Introduction

Let $k = \mathbb{F}_q(t)$ be the rational function field over the finite field $\mathbb{F}_q$ and $\mathbb{A} = \mathbb{F}_q[t]$. Let ∞ be the infinite place of k associated to $(1/t)$. Throughout the paper, by a quadratic function field, we always mean a quadratic extension of k. A quadratic function field F is said to be real if ∞ splits in F, and imaginary otherwise. Assume that q is odd. Then any quadratic function field F can be written as $F = k(\sqrt{D})$, where D is a square-free polynomial in $\mathbb{A}$. Let $\mathcal{O}_F$ be the integral closure of $\mathbb{A}$ in F. In [2], Murty and Cardon proved that there are $\gg q^{\ell(\frac{1}{2}+\frac{1}{g})}$ imaginary quadratic function fields $F = k(\sqrt{D})$ such that $\deg D \leq \ell$ and the ideal class group of $\mathcal{O}_F$ has an element of order g. This result is the function field analogue of the result of Murty for imaginary quadratic fields ([5]). In [4], Friesen proved the existence of infinitely many real quadratic function fields F whose ideal class numbers are divisible by a given positive integer g. In [3], using the Friesen's result, Chakraborty and Mukhopadhyay proved that there are $\gg q^{\frac{\ell}{2g}}$ real quadratic function fields $F = k(\sqrt{D})$ such that $\deg D \leq \ell$ and the ideal class group of $\mathcal{O}_F$ has an element of order g.

The aim of this paper is to study the same problem in even characteristic case. Assume that q is a power of 2. Then any quadratic function field F of k can be written as $F = k(y)$, where y is a zero of $\mathbf{x}^2 + A\mathbf{x} + B = 0$ with $A, B \in \mathbb{A}$. Here, we can always assume that A is monic and (A, B) satisfies

Received October 26, 2012.
2010 *Mathematics Subject Classification.* 11R18, 11R29, 11R58.
Key words and phrases. class number divisibility, quadratic function field, even characteristic.
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST)(No. 2012-0000798).

some property, so that we have $\mathcal{O}_F = \mathbb{A}[y]$ and A is uniquely determined since the discriminant of F over k is A^2 (see §2, Lemma 2.1). Write $d(F) = \deg A$.

We now state the results of this paper.

Theorem 1.1. *Let q be a power of 2, and let g be a fixed positive integer ≥ 2. Then there are $\gg q^{\nu(g,\ell)}$ real quadratic function fields F of $k = \mathbb{F}_q(t)$ such that $d(F) \leq \ell$ and the ideal class group of $\mathcal{O}_F$ contains an element of order g, where $\nu(g,\ell)$ is $\frac{\ell}{2g}$ or $\frac{\ell}{g+1}$ according as g is odd or even.*

An imaginary quadratic function field F of k is said to be inert or ramified according as ∞ inerts or ramifies in F.

Theorem 1.2. *Let q be a power of 2, and let g be a fixed positive integer ≥ 2. Then there are $\gg q^{\frac{\ell}{g}}$ inert imaginary quadratic function fields F of $k = \mathbb{F}_q(t)$ such that $d(F) \leq \ell$ and the ideal class group of $\mathcal{O}_F$ contains an element of order g.*

Theorem 1.3. *Let q be a power of 2, and let g be a fixed positive integer ≥ 2. Then there are $\gg q^{\frac{\ell}{g-1}}$ ramified imaginary quadratic function fields F of $k = \mathbb{F}_q(t)$ such that $d(F) \leq \ell$ and the ideal class group of $\mathcal{O}_F$ contains an element of order g.*

2. Preliminaries

Let q be a power of 2, and $\mathbb{F}_q$ be the finite field of q elements. Let $k = \mathbb{F}_q(t), \mathbb{A} = \mathbb{F}_q[t]$, ∞ be the infinite place of k associated to $(1/t)$ and $k_\infty = \mathbb{F}_q((1/t))$ be the completion of k at ∞. For $0 \neq A \in \mathbb{A}$, let $sgn(A)$ be the leading coefficient of A.

Let Ω be the set of pairs $(A, B) \in \mathbb{A} \times \mathbb{A}$ such that A is monic and (A, B) satisfies the property that for any irreducible polynomial P dividing A, the congruence

$$\mathbf{x}^2 + A\mathbf{x} + B \equiv 0 \bmod P^2 \tag{2.1}$$

is not solvable in $\mathbb{A}$. Then any quadratic function field F of k can be written as $F = k(y)$, where y is a zero of $\mathbf{x}^2 + A\mathbf{x} + B = 0$ with $(A, B) \in \Omega$ ([6, §1]).

The following lemma is due to Bae (the proof of Lemma 5.1 in [1] given there for real quadratic extension of k is easily seen to be valid for arbitrary quadratic extension of k).

Lemma 2.1. *Let $F = k(y)$ be a quadratic extension of k, where y is a zero of $\mathbf{x}^2 + A\mathbf{x} + B = 0$ with $(A, B) \in \Omega$. Let $\mathcal{O}_F$ be the integral closure of $\mathbb{A}$ in F. Then we have*

(i) $\mathcal{O}_F = \mathbb{A}[y]$.

(ii) *A prime P of $\mathbb{A}$ is ramified in F if and only if P divides A. In fact, the discriminant of F over k is A^2.*

It is easy to see that if $(A, B) \in \Omega$, then $(A, C^2+AC+B) \in \Omega$ for any $C \in \mathbb{A}$. If $F = k(y) = k(y')$, where y' is a zero of $\mathbf{x}^2 + A'\mathbf{x} + B' = 0$ with $(A', B') \in \Omega$, then $\mathcal{O}_F = \mathbb{A}[y] = \mathbb{A}[y']$, $A = A'$, $y' = y + C$ and $B' = C^2 + AC + B$ for some $C \in \mathbb{A}$. The converse is also true.

Lemma 2.2. *Let $F = k(y)$ be a quadratic extension of k, where y is a zero of $\mathbf{x}^2 + A\mathbf{x} + B = 0$ with $(A, B) \in \Omega$. Then we have*

(i) *∞ splits in F if and only if $\deg(C^2+AC+B) < 2 \deg A$ for some $C \in \mathbb{A}$. In this case, we can always choose C so that $\deg(C^2+AC+B) < \deg A$.*
(ii) *∞ is inert in F if and only if $\deg(C^2+AC+B) = 2 \deg A$ and $sgn(C^2+AC+B) \notin \mathcal{P}(\mathbb{F}_q)$ for some $C \in \mathbb{A}$, where $\mathcal{P}(x) = x^2 + x$ is the Artin-Schreier operator.*
(iii) *∞ ramifies in F if and only if $\deg(C^2 + AC + B) > 2 \deg A$ for any $C \in \mathbb{A}$.*

Proof. Consider $\mathcal{S} = \{\deg(C^2+AC+B) : C \in \mathbb{A}\}$. We may assume that $\deg B$ is a minimal among the elements in the set $\mathcal{S}$. We will show that

(1) if $\deg B < 2 \deg A$, then ∞ splits in F.
(2) if $\deg B = 2 \deg A$ and $sgn(B) \notin \mathcal{P}(\mathbb{F}_q)$, then ∞ is inert in F.
(3) if $\deg B = 2 \deg A$ and $sgn(B) \in \mathcal{P}(\mathbb{F}_q)$, then $\deg B$ is not minimal.
(4) if $\deg B > 2 \deg A$, then ∞ ramifies in F.

(1) Suppose that $\deg B < 2 \deg A$. Then the equation

$$\mathbf{z}^2 + \mathbf{z} + \frac{B}{A^2} = 0$$

has two distinct zeros in k_∞ by Hensel's Lemma. Put $\mathbf{x} = A\mathbf{z}$. Then the equation

$$\mathbf{x}^2 + A\mathbf{x} + B = 0$$

also has two distinct zeros in k_∞. Hence ∞ splits in F.

(2) Suppose that $\deg B = 2 \deg A$ and $sgn(B) \notin \mathcal{P}(\mathbb{F}_q)$. Then

$$\mathbf{z}^2 + \mathbf{z} + \frac{B}{A^2} \equiv \mathbf{z}^2 + \mathbf{z} + sgn(B) \bmod 1/t$$

is a separable irreducible polynomial modulo $1/t$. Hence ∞ is inert in F.

(3) Suppose that $\deg B = 2 \deg A$ and $sgn(B) \in \mathcal{P}(\mathbb{F}_q)$, say $\mathrm{sgn}(B) = \beta^2 + \beta$ for some $\beta \in \mathbb{F}_q^*$. Then $\deg((\beta A)^2 + A(\beta A) + B) < \deg B$, so $\deg B$ is not minimal.

(4) Suppose that $\deg B > 2 \deg A$. If $\deg B$ is even, say $\deg B = 2n$ and $B = \beta^2 t^{2n} + \text{lower terms}$, then $\deg((\beta t^n)^2 + A(\beta t^n) + B) < \deg B$. So $\deg B$ must be odd. Let $\deg B - 2 \deg A = 2m + 1$. Consider the equation

$$\mathbf{z}^2 + \mathbf{z} + \frac{B}{A^2} = 0.$$

Put $\mathbf{w} = t^{-m-1}\mathbf{z}$. Then

$$\mathbf{w}^2 + t^{-m-1}\mathbf{w} + t^{-2m-2}\frac{B}{A^2}$$

is an Eisenstein polynomial at ∞. Hence ∞ ramifies in F. $\square$

Remark 2.3. We can give an equivalence relation $\sim$ on the set Ω as follow;

$$(A, B) \sim (A', B') \Leftrightarrow A = A' \text{ and } B' = C^2 + AC + B \text{ for some } C \in \mathbb{A}.$$

Let $\widetilde{\Omega}$ be the set of equivalence classes with respect to $\sim$. Then we see that there is an one to one correspondence between $\widetilde{\Omega}$ and the set of all quadratic extensions of k. We also can show that for any real quadratic extension F of k, there is a unique $(A, B) \in \Omega$ such that $\deg B < \deg A$ and $F = k(y)$, where y is a zero of $\mathbf{x}^2 + A\mathbf{x} + B = 0$.

Let $A(t) \in \mathbb{A}$ be one of the following polynomials $t^{2g} + t^g + 1, t^g + 1$ with g odd or $t^g + t + 1$. It is easy to see that A is square-free. Let $\mathcal{M}_k(A)$ be the set of monic polynomials $U \in \mathbb{A}$ of degree k such that $A(U)$ is square-free. Following the same argument as in [3, §2] with $A(t)$, we get the following lemma.

Lemma 2.4. $|\mathcal{M}_k(A)| \gg q^k$.

Lemma 2.5. *Let g be a positive integer. Let $A(t) = t^g + t + 1 \in \mathbb{A}$ and $\mathcal{M}_k(A)$ be the set of monic polynomials $U \in \mathbb{A}$ of degree k such that $A(U)$ is square-free. For $U, V \in \mathcal{M}_k(A)$, if $A(U) = A(V)$, then $U = V$ or $U + V \in \mathbb{F}_q^*$. Hence there are at most q times repetitions on $A(U)$.*

Proof. Suppose $A(U) = A(V)$ with $U, V \in \mathcal{M}_k(A)$ $(U \neq V)$. Let $W = U + V$. Then $\deg W < k$. From $A(V) = (U + W)^g + (U + W) + 1 = A(U)$, we get

$$\sum_{h=0}^{g-1} \binom{g}{h} U^h W^{g-h} = W. \tag{2.2}$$

Clearly $\deg U^{h_1} W^{g-h_1} < \deg U^{h_2} W^{g-h_2}$ for any $0 \leq h_1 < h_2 \leq g - 1$, since $\deg W < k = \deg U$. Let n be the largest one among $0 \leq h \leq g - 1$ such that $\binom{g}{h} \neq 0$. If $n > 0$, then the degree of left hand side in (2.2) is equal to $nk + (g - n) \deg W$, which is greater than $\deg W$. Hence $n = 0$ and $W^g = W$, so $W \in \mathbb{F}_q^*$. Therefore, there are at most q times repetitions on $A(U)$. $\square$

3. Proof of Theorem 1.1

Let g be a positive integer ≥ 2. Let $U \in \mathbb{A}$ be a monic polynomial,

$$A = \begin{cases} U^{2g} + U^g + 1 & \text{if } g \text{ is odd,} \\ U^{g+1} + 1 & \text{if } g \text{ is even,} \end{cases}$$

and $B = U^g$. Let y satisfy the equation $\mathbf{x}^2 + A\mathbf{x} + B = 0$. Then $F = k(y)$ is a real quadratic extension of k by Lemma 2.2.

Lemma 3.1. *Let A, B, y be as above. If A is square-free, then $\mathcal{O}_F = \mathbb{A}[y]$.*

Proof. By Lemma 2.1, we need to show that for any irreducible divisor P of A, the congruence (2.1) has no solution in $\mathbb{A}$. Suppose that D is a solution of (2.1). First consider the case that g is odd, so $A = U^{2g} + U^g + 1$. Since $P|A = B^2 + B + 1$, we have $D \equiv B + 1 \bmod P$. Then

$$(B + 1)^2 + A(B + 1) + B \equiv 0 \bmod P^2.$$

But

$$(B + 1)^2 + A(B + 1) + B = A(B + 1) + (B^2 + B + 1) = A(B + 1) + A = AB,$$

which cannot be divisible by P^2 since A is square-free and $P \nmid B$, and we get a contradiction.

Now, we consider the case that g is even, so $A = U^{g+1} + 1$. Then $D \equiv U^{g/2} \bmod P$, so

$$0 \equiv D^2 + AD + B \equiv AU^{g/2} \bmod P^2,$$

which is impossible since A is square-free and $P \nmid U$. □

Lemma 3.2. *Let A, B, y be as above. If A is square-free, then the ideal class group of $\mathcal{O}_F$ contains an element of order g.*

Proof. From a straightforward computation, the continued fraction of y is

$$\begin{cases} [\overline{A : B + 1, B + 1}] & \text{if } g \text{ is odd,} \\ [\overline{A : U, A/(U + 1), U}] & \text{if } g \text{ is even,} \end{cases}$$

and

$$\begin{cases} q_{3i} = 1, q_{3i+1} = q_{3i+2} = U^g & \text{if } g \text{ is odd,} \\ q_{4i} = 1, q_{4i+1} = q_{4i+3} = U^g, q_{4i+2} = U + 1 & \text{if } g \text{ is even,} \end{cases} \tag{3.1}$$

where q_h is the denominator of h-th iterate of y. Now

$$\mathcal{N}(y) = y(y + A) = B = U^g,$$

where $\mathcal{N}$ is the norm map from F to k. Let $U = \prod_i P_i^{e_i}$. Since

$$\mathbf{x}^2 + A\mathbf{x} + B \equiv \mathbf{x}^2 + \mathbf{x} \equiv \mathbf{x}(\mathbf{x} + 1) \bmod P_i,$$

P_i splits in F. Say $P_i\mathcal{O}_F = \mathfrak{P}_i\mathfrak{P}_i'$. Since $P_i|y$, choose $\mathfrak{P}_i|y$. Then $\mathfrak{P}_i^{e_ig}||y$, and $y\mathcal{O}_F = \prod_i \mathfrak{P}_i^{e_ig}$. Let $\mathfrak{A} = \prod_i \mathfrak{P}_i^{e_i}$. Then as in [4], we see that $\mathcal{N}(\mathfrak{A}) = \alpha U$ with $\alpha \in \mathbb{F}_q^*$.

Suppose that $\mathfrak{A}^r$ is principal for some $r < g$. Then

$$||\mathcal{N}(\mathfrak{A}^r)|| = ||U||^r < ||U||^g < ||A||,$$

where we use the same $\mathcal{N}$ for the norm map on ideals. Applying Lemma 5.4 in [1], we have $\mathcal{N}(\mathfrak{A}^r) = \beta q_i$ for some $i \geq 0$ with $\beta \in \mathbb{F}_q^*$. Since $q_i \in \{1, U^g\}$ or $q_i \in \{1, U + 1, U^g\}$ according as g is even or odd, and $\mathcal{N}(\mathfrak{A}) = \alpha U$, we get a contradiction. So the order of the ideal class of $\mathfrak{A}$ is g. □

Let $A(t) \in \mathbb{A}$ be $t^{2g}+t^g+1$ or $t^{g+1}+1$ according as g is odd or even. By Lemma 2.4, there are $\gg q^k$ monic polynomials $U \in \mathbb{A}$ of degree k such that $A(U)$ is square-free. Now we check the repetitions on $A(U)$. It is easy to see that for $U, V \in \mathcal{M}_k(A)$, we have

$$A(U)=A(V) \Leftrightarrow \begin{cases} U=V \text{ or } U^g+V^g=1 & \text{if } g \text{ is odd,} \\ U=V & \text{if } g \text{ is even.} \end{cases}$$

Moreover, when g is odd, we can see that for $U, V, W \in \mathcal{M}_k(A)$, $U^g+V^g = U^g+W^g=1$ holds only if $V=W$. So there are at most double repetitions on $A(U)$. Thus there are $\gg q^{\nu(g,\ell)}$ monic square-free polynomials $A(U)$ with $\deg A(U) \leq \ell$, where $\nu(g,\ell)$ is $\frac{\ell}{2g}$ or $\frac{\ell}{g+1}$ according as g is odd or even. By Lemma 3.2, the corresponding real quadratic function fields $F=k(y)$ have elements of order g in their ideal class groups. We remark that distinct choice of $A(U)$ gives rise to distinct real quadratic extension $F=k(y)$. This completes the proof of Theorem 1.1.

4. Proof of Theorem 1.2

Let g be a positive integer ≥ 2. Let $U \in \mathbb{A}$ be a monic polynomial,

$$A=\begin{cases} U^g+1 & \text{if } g \text{ is odd,} \\ U^g+U+1 & \text{if } g \text{ is even,} \end{cases}$$

and $B=\gamma U^{2g}$, where $\gamma \in \mathbb{F}_q \setminus \mathcal{P}(\mathbb{F}_q)$ with $\mathcal{P}(x)=x^2+x$. Let y satisfy the equation $\mathbf{x}^2+A\mathbf{x}+B=0$. Then, by Lemma 2.2, we see that $F=k(y)$ is an inert imaginary quadratic extension of k.

Lemma 4.1. *Let A, B, y be as above. If A is square-free, then $\mathcal{O}_F=\mathbb{A}[y]$.*

Proof. We have to show that for any irreducible polynomial P dividing A, the congruence (2.1) is not solvable in $\mathbb{A}$. Suppose that D is a solution of (2.1). Then $D \equiv \beta U^g \bmod P$ for $\beta \in \mathbb{F}_q^*$ with $\beta^2=\gamma$. Then

$$0 \equiv D^2+AD+B \equiv \beta U^g A \bmod P^2, \tag{4.1}$$

which is impossible, since A is square-free and $(A,U)=1$. □

Lemma 4.2. *Let A, B, y be as above. If A is square-free, then the ideal class group of $\mathcal{O}_F$ contains an element of order g.*

Proof. Note that $\mathcal{N}(y)=y(y+A)=B=\gamma U^{2g}$. Let $U=\prod_i P_i^{e_i}$. Since

$$\mathbf{x}^2+A\mathbf{x}+B \equiv \mathbf{x}^2+\mathbf{x} \equiv \mathbf{x}(\mathbf{x}+1) \bmod P_i,$$

P_i splits in F. Choose a prime ideal $\mathfrak{P}_i$ of $\mathcal{O}_F$ lying over P_i such that $\mathfrak{P}_i | y$. Let $\mathfrak{A}=\prod_i \mathfrak{P}_i^{e_i}$. Then $\mathfrak{A}^{2g}=y\mathcal{O}_F$ and $\mathfrak{A}'^{2g}=(y+A)\mathcal{O}_F$. As before, $\mathcal{N}(\mathfrak{A})=\alpha U$ with $\alpha \in \mathbb{F}_q^*$.

Suppose that $\mathfrak{A}^r$ is principal for some $r<g$, say $\mathfrak{A}^r=(C+Dy)$. Then

$$q^{r \deg U}=||\mathcal{N}(\mathfrak{A}^r)||=||\mathcal{N}(C+Dy)||=||C^2+ACD+BD^2||, \tag{4.2}$$

since $N(C+Dy) = (C+Dy)(C+D(y+A)) = C^2+ACD+BD^2$. Since $r < g$, we must have $\deg C^2 = \deg BD^2$ or $\deg ACD = \deg BD^2$ or $\deg C^2 = \deg ACD$. In any case $\deg C = \deg DU^g = \deg D + g \deg U$. Furthermore, let c and d be the leading coefficients of C and D, respectively. Then we must have $c^2 + cd + \gamma d^2 = 0$, which implies that $\gamma = \mathcal{P}(c/d)$, contradicting the choice of γ. Thus, $g \le r|2g$, and so r is divisible by g. Then the ideal class of $\mathfrak{A}$ or $\mathfrak{A}^2$ is of order g. □

Let $A(t) \in \mathbb{A}$ be $t^g + 1$ or $t^g + t + 1$ according as g is odd or even. By Lemma 2.4, there are $\gg q^k$ monic polynomials U of degree k such that $A(U)$ is square-free. Now we check the repetitions on $A(U)$. When g is odd, it can be easily shown that for $U, V \in \mathcal{M}_k(A)$, $A(U) = A(V)$ if and only if $U = V$. So, by Lemma 2.5, there are at most q times repetitions on $A(U)$. Thus there are $\gg q^{\frac{\ell}{g}}$ monic square-free polynomials $A(U)$ with $\deg A(U) \le \ell$. By Lemma 4.2, the corresponding inert imaginary quadratic extensions $F = k(y)$ have an element of order g in their ideal class groups. We remark that distinct choice of $A(U)$ give rise to distinct inert imaginary quadratic extension $F = k(y)$. This completes the proof of Theorem 1.2.

5. Proof of Theorem 1.3

Let g be a positive integer ≥ 2. Let $U \in \mathbb{A}$ be a monic polynomial, $A = U^{g-1} + U + 1$ and $B = U^{2g-1} + U^g + U^4 + U^3 + U^2$. Let y satisfy the equation $\mathbf{x}^2 + A\mathbf{x} + B = 0$, and $F = k(y)$. For any $C \in \mathbb{A}$, we have that $\deg(C^2 + AC + B) = \deg C^2 > 2 \deg A$ if $\deg C > \deg A$, and $\deg(C^2 + AC + B) = \deg B > 2 \deg A$ if $\deg C \le \deg A$. Hence, by Lemma 2.2, we see that $F = k(y)$ is a ramified imaginary quadratic extension of k.

Lemma 5.1. *Let A, B, y be as above. If A is square-free, then $\mathcal{O}_F = \mathbb{A}[y]$.*

Proof. We have to show that for any irreducible polynomial P dividing A, the congruence (2.1) is not solvable in $\mathbb{A}$. Suppose that D is a solution of (2.1). Since

$$B \equiv U(U+1)^2 + U(U+1) + U^4 + U^3 + U^2 \equiv U^4 \bmod P,$$

we see that $D \equiv U^2 \bmod P$. Then

$$\begin{aligned} 0 \equiv D^2 + AD + B &\equiv AU^2 + U^{2g-1} + U^g + U^3 + U^2 \\ &\equiv A^2U + AU^2 + AU \equiv A(U^2 + U) \bmod P^2, \end{aligned}$$

which is impossible, since A is square-free and $P \nmid (U^2 + U)$. □

Lemma 5.2. *Let A, B, y be as above and assume that $\deg U$ is odd. If A is square-free, then the ideal class group of $\mathcal{O}_F$ contains an element of order g.*

Proof. Note that $\mathcal{N}(y + U^g + U^2) = U^{2g}$. Let $U = \prod_i P_i^{e_i}$. Since

$$\mathbf{x}^2 + A\mathbf{x} + B \equiv \mathbf{x}^2 + \mathbf{x} \equiv \mathbf{x}(\mathbf{x}+1) \bmod P_i,$$

P_i splits in F. Choose a prime ideal $\mathfrak{P}_i$ of $\mathcal{O}_F$ lying over P_i such that $\mathfrak{P}_i|(y + U^g + U^2)$. Let $\mathfrak{A} = \prod_i \mathfrak{P}_i^{e_i}$. Then $\mathfrak{A}^{2g} = (y + U^g + U^2)\mathcal{O}_F$ and $\mathfrak{A}'^{2g} = (y + U^g + U^2 + A)\mathcal{O}_F$. As before, $\mathcal{N}(\mathfrak{A}) = \alpha U$ with $\alpha \in \mathbb{F}_q^*$.

Suppose that $\mathfrak{A}^r$ is principal for some $r < g$, say $\mathfrak{A}^r = (C + Dy)$. Then

$$q^{r \deg U} = ||\mathcal{N}(\mathfrak{A}^r)|| = ||\mathcal{N}(C + Dy)|| = ||C^2 + ACD + BD^2||, \tag{5.1}$$

since $N(C + Dy) = (C + Dy)(C + D(y + A)) = C^2 + ACD + BD^2$. Since $r < g$, we must have (1) $\deg C^2 = \deg BD^2$ or (2) $\deg ACD = \deg BD^2$ or (3) $\deg C^2 = \deg ACD$. The case (1) cannot happen, since we assumed that $\deg U$ is odd. In case (2), we have $\deg C = g \deg U + \deg D$, and so $\deg C^2 > \deg ACD = \deg BD^2 > r \deg U$, which contradicts to (5.1). In case (3), we have $\deg C = (g - 1) \deg U + \deg D$. Then $\deg BD^2 > \deg C^2$, and we get a contradiction to (5.1). Thus, $g \leq r|2g$, and so r is divisible by g. Then the ideal class of $\mathfrak{A}$ or $\mathfrak{A}^2$ is of order g. □

Let $A(t) = t^{g-1} + t + 1 \in \mathbb{A}$. By Lemma 2.4, there are $\gg q^k$ monic polynomials U of degree k such that $A(U)$ is square-free. By Lemma 2.5, there are at most q times repetitions on $A(U)$. Thus there are $\gg q^{\frac{\ell}{g-1}}$ monic square-free polynomials $A(U)$ with $\deg A(U) \leq \ell$. By Lemma 5.2, the corresponding ramified imaginary quadratic extensions $F = k(y)$ have an element of order g in their ideal class groups. We remark that distinct choice of $A(U)$ give rise to distinct ramified imaginary quadratic extension $F = k(y)$. This completes the proof of Theorem 1.3.

References

[1] S. Bae, *Real quadratic function fields of Richaud-Degert type with ideal class number one*, Proc. Amer. Math. Soc. **140** (2012), no. 2, 403–414.

[2] D. A. Cardon and M. R. 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 A. Mukhopadhyay, *Exponents of class groups of real quadratic function fields*, Proc. Amer. Math. Soc. **132** (2004), no. 7, 1951–1955.

[4] C. Friesen, *Class number divisibility in real quadratic function fields*, Canad. Math. Bull. **35** (1992), no. 3, 361–370.

[5] R. 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.

[6] R. J. Zuccherato, *The continued fraction algorithm and regulator for quadratic function fields of characteristic* 2, J. Algebra **190** (1997), no. 2, 563–587.

Sunghan Bae
Department of Mathematics
KAIST
Taejon 305-701, Korea
E-mail address: shbae@kaist.ac.kr

Hwanyup Jung
Department of Mathematics Education
Chungbuk National University
Cheongju 361-763, Korea
E-mail address: hyjung@chungbuk.ac.kr