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 $F_q(t)$ whose ideal class groups have an element of a fixed order, where $q$ is a power of 2.

1. Introduction

Let $k = F_q(t)$ be the rational function field over the finite field $F_q$ and $A = F_q[t]$. Let $\infty$ 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 $\infty$ 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 $A$. Let $O_F$ be the integral closure of $A$ in $F$. In [2], Murty and Cardon proved that there are $\gg q^{1/2} \log^2 (1 + \log q)$ imaginary quadratic function fields $F = k(\sqrt{D})$ such that $\deg D \leq \ell$ and the ideal class group of $O_F$ 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 $\gg q^{\frac{1}{1+2g}}$ real quadratic function fields $F = k(\sqrt{D})$ such that $\deg D \leq \ell$ and the ideal class group of $O_F$ 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 $x^2 + Ax + B = 0$ with $A, B \in A$. Here, we can always assume that $A$ is monic and $(A, B)$ satisfies...
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 \( \geq 2 \). 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 \( \frac{\ell + 1}{g+1} \) according as \( g \) is odd or even.

An imaginary quadratic function field \( F \) of \( k \) is said to be inert or ramified according as \( \infty \) inert or ramifies in \( F \).

**Theorem 1.2.** Let \( q \) be a power of 2, and let \( g \) be a fixed positive integer \( \geq 2 \). Then there are \( \gg q^{\ell \nu(g, \ell)} \) 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 \( \geq 2 \). Then there are \( \gg q^{\ell g - 1} \) 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 \( k = \mathbb{F}_q(t), \mathbb{A} = \mathbb{F}_q[t], \infty \) be the infinite place of \( k \) associated to \((1/t)\) and \( k_\infty = \mathbb{F}_q((1/t)) \) be the completion of \( k \) at \( \infty \). For \( 0 \neq A \in \mathbb{A} \), let \( \text{sgn}(A) \) be the leading coefficient of \( A \).

Let \( \Omega \) 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

\[
(2.1) \quad x^2 + Ax + B \equiv 0 \mod P^2
\]

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 \( x^2 + Ax + B = 0 \) 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 \( x^2 + Ax + B = 0 \) 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 \(x^2 + A'x + B' = 0\) with \((A', B') \in \Omega\), then \(O_F = \mathbb{A}[y] = \mathbb{A}[y']\), \(A = A'\), \(y' = y + C\) 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 \(x^2 + Ax + B = 0\) with \((A, B) \in \Omega\). Then we have

(i) \(\infty\) splits in \(F\) if and only if \(\deg(C^2 + AC + B) < 2 \deg A\) for some \(C \in \mathbb{A}\).

(ii) \(\infty\) is inert in \(F\) if and only if \(\deg(C^2 + AC + B) = 2 \deg A\) and \(\sgn(C^2 + AC + B) \not\in \mathcal{P} \mathbb{F}_q\) for some \(C \in \mathbb{A}\), where \(\mathcal{P}(x) = x^2 + x\) is the Artin-Schreier operator.

(iii) \(\infty\) ramifies in \(F\) if and only if \(\deg(C^2 + AC + B) \geq 2 \deg A\) for any \(C \in \mathbb{A}\).

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

1. if \(\deg B < 2 \deg A\), then \(\infty\) splits in \(F\).
2. if \(\deg B = 2 \deg A\) and \(\sgn(B) \not\in \mathcal{P} \mathbb{F}_q\), then \(\infty\) 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 \(\infty\) ramifies in \(F\).

(1) Suppose that \(\deg B < 2 \deg A\). Then the equation
\[
z^2 + z + \frac{B}{A^2} = 0
\]
has two distinct zeros in \(k_\infty\) by Hensel’s Lemma. Put \(x = Az\). Then the equation
\[
x^2 + Ax + B = 0
\]
also has two distinct zeros in \(k_\infty\). Hence \(\infty\) splits in \(F\).

(2) Suppose that \(\deg B = 2 \deg A\) and \(\sgn(B) \not\in \mathcal{P} \mathbb{F}_q\). Then
\[
z^2 + z + \frac{B}{A^2} \equiv z^2 + z + \sgn(B) \mod \frac{1}{t}
\]
is a separable irreducible polynomial modulo \(\frac{1}{t}\). Hence \(\infty\) is inert in \(F\).

(3) Suppose that \(\deg B = 2 \deg A\) and \(\sgn(B) \in \mathcal{P} \mathbb{F}_q\), say \(\sgn(B) = \beta^2 + \beta\) for some \(\beta \in \mathbb{F}_q^\times\). 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 \(\deg B = 2m\) and \(B = \beta^2 t^{2m} + \text{lower terms}\), 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
\[
z^2 + z + \frac{B}{A^2} = 0.
\]
Put \(w = t^{-m-1}z\). Then
\[
w^2 + t^{-m-1}w + t^{-2m-2}B
\]
\[\frac{B}{A^2}\]
is an Eisenstein polynomial at $\infty$. Hence $\infty$ ramifies in $F$. \hfill $\square$

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

$$(A, B) \sim (A', B') \iff A = A'$ and $B' = C^2 + AC + B$ for some $C \in k$.

Let $\tilde{\Omega}$ be the set of equivalence classes with respect to $\sim$. Then we see that there is an one to one correspondence between $\Omega$ 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 $x^2 + Ax + B = 0$.

Let $A(t) \in k$ 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 $U \in k$ 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 $A(t) = t^g + t + 1 \in k$ and $\mathcal{M}_k(A)$ be the set of monic polynomials $U \in k$ 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

$$\sum_{h=0}^{g-1} \binom{g}{h} u^h w^{g-h} = W.$$  

Clearly $\deg u^{g_1} w^{g_2} < \deg u^{h_1} w^{g-h_2}$ 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 $A(U)$. \hfill $\square$

### 3. Proof of Theorem 1.1

Let $g$ be a positive integer $\geq 2$. Let $U \in k$ 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 $x^2 + Ax + B = 0$. 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 $\mathcal{O}_F = k[y]$. 

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 \( A \). 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 \( D \equiv B + 1 \mod P \). Then
\[
(B + 1)^2 + A(B + 1) + B \equiv 0 \mod P^2.
\]
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 \( A = Ug + 1 + 1 \). Then
\[
D \equiv \frac{Ug}{2} \mod P,
\]
so
\[
0 \equiv D^2 + AD + B \equiv \frac{AUg}{2} \mod P^2,
\]
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
\[
\begin{align*}
[A : B + 1, B + 1] & \text{ if } g \text{ is odd,} \\
[A : U, A/(U + 1), U] & \text{ if } g \text{ is even,}
\end{align*}
\]
and
\[
(3.1) \begin{cases}
q_{3i} = 1, q_{3i+1} = q_{3i+2} = U^g & \text{if } g \text{ is odd,} \\
q_{4i} = 1, q_{4i+1} = q_{4i+3} = U^g, q_{4i+2} = U + 1 & \text{if } g \text{ is even,}
\end{cases}
\]
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 \( U = \prod P_i^{e_i} \). Since
\[
x^2 + Ax + B \equiv x^2 + x \equiv x(x + 1) \mod P_i,
\]
\( P_i \) splits in \( F \). Say \( P_i \mathcal{O}_F = \mathfrak{p}_i \mathfrak{p}'_i \). Since \( P_i \mid y \), choose \( \mathfrak{p}_i \mid y \). Then \( \mathfrak{p}'_i \mathcal{O}_F = \prod \mathfrak{p}'_i \). Let \( \mathfrak{A} = \prod \mathfrak{p}'_i \). Then as in [4], we see that \( \mathcal{N}(\mathfrak{A}) = \alpha U \) with \( \alpha \in F^* \).

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 \( \beta \in F^*_q \). 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

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

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 $\frac{g}{2g}$ or $\frac{g}{2g} + 1$ 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 $\geq 2$. 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 $x^2 + Ax + B = 0$. 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

$$(4.1) \quad 0 \equiv D^2 + AD + B \equiv \beta U^g A \bmod P^2,$$

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

**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 $U = \prod_i P_i^{\epsilon_i}$. Since

$$x^2 + Ax + B \equiv x^2 + x \equiv x(x+1) \bmod P_i,$$

$P_i$ 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 $\mathfrak{A} = \prod_i \mathfrak{p}_i^{\epsilon_i}$. 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 $\mathfrak{A}^r = (C + D y)$. Then

$$(4.2) \quad q^{-\deg U} = \|\mathcal{N}(\mathfrak{A}^r)\| = \|\mathcal{N}(C + D y)\| = \|\mathfrak{A}^2 + ACD + BD^2\|,$$
Lemma 5.1. Let $A$ be a square-free monic polynomial, $A = U^{r-1} + U + 1$ and $B = U^{2g-1} + U^g + U^4 + U^3 + U^2$. Let $y$ satisfy the equation $x^2 + Ax + B = 0$, 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 $\deg C \leq \deg A$. Hence, by Lemma 2.2, we see that $F = k(y)$ is a ramified imaginary quadratic extension of $k$.

5. Proof of Theorem 1.3

Let $g$ be a positive integer $\geq 2$. 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 $x^2 + Ax + B = 0$, 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 $\deg C \leq \deg A$. 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

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

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

$$0 \equiv D^2 + AD + B \equiv AU^2 + U^{2g-1} + U^g + U^3 + U^2 \equiv A^2 U + AU + U \equiv A(U^2 + U) \mod P^2,$$

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

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

$$x^2 + Ax + B \equiv x^2 + x \equiv x(x + 1) \mod P_i,$$
$P_i$ splits in $F$. Choose a prime ideal $\mathfrak{P}_i$ of $O_F$ 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 $\mathfrak{A}^{2g} = (y + U^g + U^2)O_F$ and $\mathfrak{A}^{2g} = (y + U^g + U^2 + A)O_F$. As before, $N(\mathfrak{A}) = \alpha U$ with $\alpha \in \mathbb{F}_q^*$.

Suppose that $\mathfrak{A}^r$ is principal for some $r < g$, say $\mathfrak{A}^r = (C + Dy)$. Then (5.1)

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

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 $\mathfrak{A}^{2g}$ is of order $g$. \hfill \Box

Let $A(t) = t^{g-1} + t + 1 \in \mathbb{F}_q[t]$. 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 $\gg q^{\frac{k}{2g}}$ monic square-free polynomials $A(U)$ with $\deg A(U) \leq t$. 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


Sunghan Bae
Department of Mathematics
KAIST
Taejon 305-701, Korea
E-mail address: sshbae@kaist.ac.kr
Hwanyup Jung
Department of Mathematics Education
Chungbuk National University
Cheongju 361-763, Korea
E-mail address: hyjung@chungbuk.ac.kr