ACTA ARITHMETICA
151.4 (2012)

On the 4-rank of ideal class groups of quadratic function fields

by

Sunghan Bae (Taejon) and Hwanyup Jung (Cheongju)

1. Introduction and statement of the results. In [CL84], Cohen and Lenstra have built a probabilistic model to guess the frequency of some algebraic properties of the narrow class group $\mathcal{C}_D$ of the ring of integers of the quadratic fields $\mathbb{Q}(\sqrt{D})$, where D is a fundamental discriminant. One of the consequences of the Cohen–Lenstra heuristics is to describe the distribution of the values of $\mathrm{rk}_p(\mathcal{C}_D)$ as D ranges over the set of positive or negative discriminants, and p is a fixed odd prime. These heuristics do not concern the special prime $p = 2$. In [Ge87], Gerth extended these heuristics to the case $p = 2$ by considering $\mathrm{rk}_p(\mathcal{C}_D^2)$. Recently Fouvry and Klüners [FK07] have proved Gerth's extensions of some of the conjectures in [CL84].

Let us describe the results of Fouvry and Klüners more precisely. Let $f(D)$ be a real valued function defined over the set of fundamental discriminants D. Then $\mathcal{M}^+(f(D))$ is, by definition, the mean value of $f(D)$ over positive fundamental discriminants D if

$$\lim_{X\to+\infty} \frac{\sum_{0<D<X} f(D)}{\sum_{0<D<X} 1} = \mathcal{M}^+(f(D)).$$

$\mathcal{M}^-(f(D))$ is defined similarly for negative fundamental discriminants. Consider the following conjectures of Cohen–Lenstra extended to $p = 2$ by Gerth:

Conjecture 1 ([CL84, (C6), (C10)], [Ge87]). *For every prime number p and every integer $r \geq 0$,*

$$\mathcal{M}^+\Big(\prod_{0\leq i<r} (p^{\mathrm{rk}_p(\mathcal{C}_D^2)} - p^i)\Big) = p^{-r} \quad \textit{and} \quad \mathcal{M}^-\Big(\prod_{0\leq i<r} (p^{\mathrm{rk}_p(\mathcal{C}_D^2)} - p^i)\Big) = 1.$$

2010 *Mathematics Subject Classification*: 11R11, 11R29, 11R49, 11R58.
Key words and phrases: 4-ranks of class groups, quadratic function fields, negative Pell equation.

DOI: 10.4064/aa151-4-1

In [FK07], Fouvry and Klüners have proved that Conjecture 1 is true for $p = 2$ and every integer $r \geq 0$. Let $\mathcal{N}(h, p)$ denote the number of subspaces of $\mathbb{F}_p^h$. For the proof, Conjecture 1 is modified as follows:

CONJECTURE 2. *Let p be a prime number and h be a nonnegative integer. Then*

$$\mathcal{M}^+(p^{h\,\mathrm{rk}_p(\mathcal{C}_D^2)}) = p^{-h}(\mathcal{N}(h+1,p) - \mathcal{N}(h,p))$$

and

$$\mathcal{M}^-(p^{h\,\mathrm{rk}_p(\mathcal{C}_D^2)}) = \mathcal{N}(h,p).$$

Then they proved that Conjecture 2 is true for $p = 2$ and any integer $h \geq 0$.

Another conjecture of Cohen–Lenstra, extended to $p = 2$ by Gerth, concerns the density of the fundamental discriminants D with fixed $\mathrm{rk}_p(\mathcal{C}_D^2)$.

CONJECTURE 3 ([CL84, (C5), (C9)], [Ge87]). *Let r be a nonnegative integer and p be a prime number. Then the density of the positive (resp. negative) fundamental discriminants D such that $\mathrm{rk}_p(\mathcal{C}_D^2) = r$ is equal to*

$$\frac{\eta_\infty(p)}{p^{r(r+1)}\eta_r(p)\eta_{r+1}(p)} \quad \left(\textit{resp. } \frac{\eta_\infty(p)}{p^{r^2}\eta_r(p)^2}\right),$$

where $\eta_h(t) := \prod_{j=1}^{h}(1 - t^{-j})$ for $0 \leq h \leq +\infty$.

In [FK06], Fouvry and Klüners have shown that if for some prime number p, Conjecture 1 is true for every integer $r \geq 0$, then Conjecture 3 is also true for this p for every integer $r \geq 0$. Thus, Conjecture 3 is true for $p = 2$ and every integer $r \geq 0$.

Let d be a square-free positive integer and consider the negative Pell equation

$$x^2 - dy^2 = -1. \tag{1.1}$$

Write D for the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$. Then the solvability of the negative Pell equation (1.1) is equivalent to $\mathcal{N}(\epsilon_D) = -1$, where ϵ_D is the fundamental unit of $\mathbb{Q}(\sqrt{D})$ and $\mathcal{N}$ is the norm map from $\mathbb{Q}(\sqrt{D})$ to $\mathbb{Q}$. Let $\mathcal{D}$ be the set of special discriminants, i.e.

$$\mathcal{D} = \{D > 0 : p \,|\, D \Rightarrow p \equiv 1 \text{ or } 2 \bmod 4\}.$$

For $X > 1$, we denote by $\mathcal{D}(X)$ the cardinality of $\mathcal{D} \cap [0, X]$ and by $\mathcal{D}^-(X)$ the cardinality of $\{D \in \mathcal{D} : 0 < D < X, \mathcal{N}(\epsilon_D) = -1\}$. Let us introduce the constants

$$c_1 := \frac{9}{8\pi} \prod_{p \equiv 1 \bmod 4} (1 - p^{-2})^{1/2} \quad \text{and} \quad \alpha := \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{+\infty} (1 + 2^{-j})^{-1}.$$

It is well known that $\mathcal{D}(X)$ is asymptotic to $c_1 X/\sqrt{\log X}$. In [St93], Stevenhagen proposed the following two conjectures:

CONJECTURE 4. *As $X \to +\infty$, we have $\mathcal{D}^-(X) \sim (1-\alpha)\mathcal{D}(X)$.*

CONJECTURE 5. *The number of square-free positive integers $d < X$ for which (1.1) is solvable is asymptotic to $(1-\alpha)\mathcal{X}$, where $\mathcal{X} = \frac{4}{3}c_1 X/\sqrt{\log X}$.*

In a recent paper [FK10], Fouvry and Klüners have proved that as $X \to +\infty$,

$$(\alpha - o(1))\mathcal{D}(X) \le \mathcal{D}^-(X) \le (2/3 + o(1))\mathcal{D}(X)$$

and deduced an asymptotic lower bound $(\alpha - o(1))\mathcal{X}$ and an upper bound $(2/3+o(1))\mathcal{X}$ for the number of square-free positive integers d $(0 < d \le X)$ for which (1.1) is solvable.

In this article we consider the analogous problems in the function field setting. Let $\mathrm{k} := \mathbb{F}_q(T)$, where q is a power of an odd prime number p and $\mathbb{A} := \mathbb{F}_q[T]$. For convenience, we fix the following subsets of $\mathbb{A}$: $\mathbb{A}^+ := \{A \in \mathbb{A} : A \text{ is monic}\}$, $\mathbb{A}^{+,o} := \{A \in \mathbb{A}^+ : A \text{ is square-free}\}$ and $\mathbb{A}^+_{\mathrm{irr}} := \{P \in \mathbb{A}^+ : P \text{ is irreducible}\}$. For any integer $n \ge 0$, we also write $\mathbb{A}^+_n := \{A \in \mathbb{A}^+ : \deg A = n\}$, $\mathbb{A}^{+,o}_n := \mathbb{A}^{+,o} \cap \mathbb{A}^+_n$ and $\mathbb{A}^+_{\mathrm{irr},n} := \mathbb{A}^+_{\mathrm{irr}} \cap \mathbb{A}^+_n$. Let k_∞ be the completion of k at $\infty := (1/T)$ and $\mathrm{sgn} : \mathrm{k}^*_\infty \to \mathbb{F}^*_q$ be the sign map such that $\mathrm{sgn}(A)$ is the leading coefficient of A for all $0 \ne A \in \mathbb{A}$. Write $\overline{\mathrm{sgn}}(x) := \mathrm{sgn}(x)^{(q-1)/2}$. For a finite extension K of k and a place ν of K lying above ∞, we define $\overline{\mathrm{sgn}}_\nu(x) := \overline{\mathrm{sgn}}(N_{\nu/\infty}(x))$, where $N_{\nu/\infty}$ denotes the norm map from the completion K_ν of K at ν to k_∞. An element $x \in \mathrm{K}^*$ is called *totally positive* if $\overline{\mathrm{sgn}}_\nu(x) = 1$ for any $\nu \,|\, \infty$. Throughout the paper we only consider field extensions of k contained in $\mathrm{k}_\infty(\sqrt[q-1]{-1/T})$. The case when $q \equiv 3 \bmod 4$ is very close to the classical case, but the case when $q \equiv 1 \bmod 4$ is different (cf. [BJ, Lemma 2.2] or Lemma 2.6 below). Our main results in this paper concern the case when $q \equiv 3 \bmod 4$. But the results in Sections 3 and 4 hold for any odd q.

For any $1 \ne D \in \mathbb{A}^{+,o}$, let $\mathrm{k}_D := \mathrm{k}(\sqrt{\bar{D}})$, where $\bar{D} := (-1)^{\deg D} D$, and $\mathcal{O}_D$ be the integral closure of $\mathbb{A}$ in k_D. Let $\mathcal{C}l_D$ be the ideal class group of $\mathcal{O}_D$. Let $\mathcal{C}_D$ be the narrow ideal class group of $\mathcal{O}_D$, that is, the quotient group of fractional ideals of $\mathcal{O}_D$ modulo principal fractional ideals generated by totally positive elements of k_D.

1.1. Results on the 4-rank of the narrow ideal class group $\mathcal{C}_D$. Let $f(D)$ be a real valued function defined on $\mathbb{A}^{+,o}$. We say that $\mathcal{M}^+(f(D))$ is the mean value of $f(D)$ over $\mathbb{A}^{+,o}_{\mathrm{even}} := \{D \in \mathbb{A}^{+,o} : \deg D \text{ is even}\}$ if

$$\lim_{\substack{n \to +\infty \\ n \text{ even}}} \frac{\sum_{D \in \mathbb{A}^{+,o}_n} f(D)}{\sum_{D \in \mathbb{A}^{+,o}_n} 1} = \mathcal{M}^+(f(D)).$$

We define similarly $\mathcal{M}^-(f(D))$ for $\mathbb{A}^{+,o}_{\mathrm{odd}} := \mathbb{A}^{+,o} \setminus \mathbb{A}^{+,o}_{\mathrm{even}}$. As in the classical case, we formulate the following conjectures:

CONJECTURE 6. *For every prime number $\ell \neq p$ and every integer $r \geq 0$ we have*

- $\mathrm{Conj}^+(\ell, r)$: $\mathcal{M}^+(\prod_{0\leq i<r}(\ell^{\mathrm{rk}_\ell(\mathcal{C}_D^2)} - \ell^i)) = \ell^{-r}$.
- $\mathrm{Conj}^-(\ell, r)$: $\mathcal{M}^-(\prod_{0\leq i<r}(\ell^{\mathrm{rk}_\ell(\mathcal{C}_D^2)} - \ell^i)) = 1$.

CONJECTURE 7. *Let $\ell \neq p$ be a prime number and a be an integer. Then*

- $\mathrm{Conj}^+_{\mathrm{mod}}(\ell, h)$: $\mathcal{M}^+(\ell^{h\,\mathrm{rk}_\ell(\mathcal{C}_D^2)}) = \ell^{-h}(\mathcal{N}(h+1,\ell) - \mathcal{N}(h,\ell))$.
- $\mathrm{Conj}^-_{\mathrm{mod}}(\ell, h)$: $\mathcal{M}^-(\ell^{h\,\mathrm{rk}_\ell(\mathcal{C}_D^2)}) = \mathcal{N}(h,\ell)$.

CONJECTURE 8. *Let r be a nonnegative integer and $\ell \neq p$ be a prime number. Then the density of $D \in \mathbb{A}^{+,o}_{\mathrm{even}}$ (resp. $D \in \mathbb{A}^{+,o}_{\mathrm{odd}}$) such that $\mathrm{rk}_\ell(\mathcal{C}_D^2) = r$ is equal to*

$$\frac{\eta_\infty(\ell)}{\ell^{r(r+1)}\eta_r(\ell)\eta_{r+1}(\ell)} \quad \left(\textit{resp. } \frac{\eta_\infty(\ell)}{\ell^{r^2}\eta_r(\ell)^2}\right).$$

For any positive integers n and h, we define

$$S(n,h) := \sum_{D\in\mathbb{A}_n^{+,o}} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)},$$

where $\mathrm{rk}_4(\mathcal{C}_D) = \mathrm{rk}_2(\mathcal{C}_D^2)$ denotes the 4-rank of $\mathcal{C}_D$. In §6, we shall prove

THEOREM 1.1. *Assume that $q \equiv 3 \bmod 4$. For any positive integers n, h and any positive real ϵ, we have*

$$S(n,h) = \begin{cases} \mathcal{N}(h,2)q^n(1-1/q) + O_{h,\epsilon}(q^n n^{-2^{-h}+\epsilon}) & \textit{if } n \textit{ is odd,} \\ 2^{-h}(\mathcal{N}(h+1,2) - \mathcal{N}(h,2))q^n(1-1/q) + O_{h,\epsilon}(q^n n^{-2^{-h}+\epsilon}) & \\ & \textit{if } n \textit{ is even.} \end{cases}$$

Since $|\mathbb{A}_n^{+,o}| = q^n(1-1/q)$ (cf. [Ro02, Proposition 2.1]), Theorem 1.1 immediately yields

COROLLARY 1.2. *Assume that $q \equiv 3 \bmod 4$. Then the conjectures $\mathrm{Conj}^+_{\mathrm{mod}}(2,h)$ and $\mathrm{Conj}^-_{\mathrm{mod}}(2,h)$ are true for any positive integer h.*

It can be easily shown that Proposition 1 of [FK07] remains valid in the function field case too, that is, for a prime number $\ell \neq p$ and positive integer r_0, $\mathrm{Conj}^+(\ell, r)$ (resp. $\mathrm{Conj}^-(\ell, r)$) is true for every $0 \leq r \leq r_0$ if and only if $\mathrm{Conj}^+_{\mathrm{mod}}(\ell, r)$ (resp. $\mathrm{Conj}^-_{\mathrm{mod}}(\ell, r)$) is true for every $0 \leq r \leq r_0$. Thus Corollary 1.2 implies

COROLLARY 1.3. *Assume that $q \equiv 3 \bmod 4$. Then the conjectures $\mathrm{Conj}^+(2,r)$ and $\mathrm{Conj}^-(2,r)$ are true for every integer $r \geq 0$.*

As in Theorem 1 and 2 of [FK06], we can show that if, for some prime number $\ell \neq p$, Conjecture 6 is true for every integer $r \geq 0$, then Conjecture 8 is also true for this ℓ for every integer $r \geq 0$. In the proof we need

to replace $N(X,r) = |\{D : 0 < \pm D < X, \mathrm{rk}_p(\mathcal{C}_D^2) = r\}|$ by $N(n,r) := |\{D \in \mathbb{A}_n^{+,o} : \mathrm{rk}_p(\mathcal{C}_D^2) = r\}|$ and X appearing as denominators by q^n (cf. §4 and §5 in [FK06]). Thus we have

COROLLARY 1.4. *Assume that $q \equiv 3 \bmod 4$. Then Conjecture 8 is true for $\ell = 2$ and all integers $r \geq 0$.*

1.2. Results on the negative Pell equation. Let $D \in \mathbb{A}^{+,o}$ be of even degree, and γ be a fixed generator of $\mathbb{F}_q^*$. We call the equation

$$X^2 - DY^2 = \gamma \tag{1.2}$$

a *negative Pell equation*. As in the classical case, the solvability of (1.2) is equivalent to $\mathcal{N}(\epsilon_D) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$, where ϵ_D is a fundamental unit of k_D and $\mathcal{N}$ is the norm map from k_D to k. Clearly (1.2) is solvable only if $\deg P$ is even for any $P \in \mathbb{A}_{\mathrm{irr}}^+$ dividing D. Note that when $q \equiv 3 \bmod 4$, the solvability of (1.2) is the same as the solvability of $X^2 - DY^2 = -1$. Let $\mathcal{D} := \{D \in \mathbb{A}^{+,o} : \deg P \text{ is even for any } P \in \mathbb{A}_{\mathrm{irr}}^+ \text{ dividing } D\}$. For a positive even integer n, write $\mathcal{D}(n) := |\mathcal{D} \cap \mathbb{A}_n^{+,o}|$ and $\mathcal{D}^-(n) := |\{D \in \mathcal{D} \cap \mathbb{A}_n^{+,o} : \mathcal{N}(\epsilon_D) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}\}|$. It can be shown that

$$\mathcal{D}(n) \sim \frac{q^n}{\sqrt{n}}.$$

Let

$$\alpha := \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{+\infty} (1 + 2^{-j})^{-1}.$$

THEOREM 1.5. *Assume that $q \equiv 3 \bmod 4$. For even integers $n \to +\infty$,*

$$(\alpha - o(1))\mathcal{D}(n) \leq \mathcal{D}^-(n) \leq (2/3 + o(1))\mathcal{D}(n).$$

For any positive even integer n and any positive integer h, let

$$S^*(n,h) := \sum_{D \in \mathcal{D} \cap \mathbb{A}_n^{+,o}} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)},$$

$$S^*_{\mathrm{mix}}(n,h) := \sum_{D \in \mathcal{D} \cap \mathbb{A}_n^{+,o}} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)} \cdot 2^{\mathrm{rk}_4(\mathcal{C}l_D)}.$$

In §6, we shall prove the following analogue of [FK10, Theorems 3 and 4]:

THEOREM 1.6. *Assume that $q \equiv 3 \bmod 4$. For any positive integer r and any positive real ϵ,*

$$S^*(n,h) = \prod_{j=0}^{h-1} (2^j + 1) \cdot \mathcal{D}(n) + O_{h,\epsilon}(q^n n^{\epsilon - 2^{-h-1}}),$$

$$S^*_{\mathrm{mix}}(n,h) = (2^{h-1} + 1) \prod_{j=0}^{h-1} (2^j + 1) \cdot \mathcal{D}(n) + O_{h,\epsilon}(q^n n^{\epsilon - 2^{-h-2}}).$$

Theorem 1.5 follows from Theorem 1.6 as in the classical case. We have an exact sequence

$$1 \to F_D \to \mathcal{C}_D \to \mathcal{C}l_D \to 1, \tag{1.3}$$

where $|F_D| \le 2$. It is known that $|F_D| = 2$ if and only if $\deg D$ is even and $\mathcal{N}(\epsilon_D) \in \mathbb{F}_q^{*2}$. Thus $\mathcal{C}_D = \mathcal{C}l_D$ if and only if $\mathcal{N}(\epsilon_D) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. By the exact sequence (1.3), we have

$$\mathrm{rk}_{2^h}(\mathcal{C}_D) - 1 \le \mathrm{rk}_{2^h}(\mathcal{C}l_D) \le \mathrm{rk}_{2^h}(\mathcal{C}_D) \quad \text{for all } h \ge 1. \tag{1.4}$$

By genus theory,

$$\mathrm{rk}_2(\mathcal{C}_D) = \omega(D) - 1,$$

where $\omega(D)$ is the number of prime divisors of D. As in the classical case we have the following lemma.

LEMMA 1.7. *Let $D \in \mathbb{A}^{+,o}$ be of even degree with $|F_D| = 2$. Then the following are equivalent:*

(i) $\mathcal{C}_D \cong \mathbb{Z}/2\mathbb{Z} \times \mathcal{C}l_D$.
(ii) *There exists $P \in \mathbb{A}^+_{\mathrm{irr}}$ dividing D of odd degree.*

In this case $\mathcal{C}_D^2 \cong \mathcal{C}l_D^2$.

Therefore $D \in \mathcal{D}$ if and only if $\mathrm{rk}_2(\mathcal{C}_D) = \mathrm{rk}_2(\mathcal{C}l_D)$. For $D \in \mathcal{D}$, $\mathcal{N}(\epsilon_D) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$ if and only if $\mathrm{rk}_{2^h}(\mathcal{C}_D) = \mathrm{rk}_{2^h}(\mathcal{C}l_D)$ for all $h \ge 2$. Thus we have

LEMMA 1.8. *For $D \in \mathcal{D}$ with $\mathrm{rk}_4(\mathcal{C}_D) = 0$, we have $\mathcal{N}(\epsilon_D) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$.*

LEMMA 1.9. *Let $D \in \mathcal{D}$. If $\mathcal{N}(\epsilon_D) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$, then $\mathrm{rk}_4(\mathcal{C}_D) = \mathrm{rk}_4(\mathcal{C}l_D)$.*

For any nonnegative integers a and b, we define

$$\delta(a,b) := \lim_{\substack{n \to +\infty \\ n \text{ even}}} \frac{|\{D \in \mathcal{D} \cap \mathbb{A}_n^{+,0} : \mathrm{rk}_4(\mathcal{C}_D) = a,\ \mathrm{rk}_4(\mathcal{C}l_D) = b\}|}{\mathcal{D}(n)}.$$

By (1.4), we have $\delta(a,b) = 0$ if $0 \le a < b$ or $0 \le b < a - 1$. Following the argument of §2 in [FK10] and using Theorem 1.6, we get

$$\delta(a,b) = \begin{cases} 2^{-a}\alpha_\infty(a) & \text{if } a = b, \\ (1 - 2^{-a})\alpha_\infty(a) & \text{if } a = b + 1, \end{cases} \tag{1.5}$$

where $\alpha_\infty(a) = \alpha \prod_{j=1}^{a} (2^j - 1)^{-1}$. Thus we have

COROLLARY 1.10. *For any nonnegative integer r, as even integers $n \to +\infty$,*

$$|\{D \in \mathcal{D} \cap \mathbb{A}_n^{+,o} : \mathrm{rk}_4(\mathcal{C}_D) = r\}| \sim \alpha_\infty(r) \cdot \mathcal{D}(n),$$
$$|\{D \in \mathcal{D} \cap \mathbb{A}_n^{+,o} : \mathrm{rk}_4(\mathcal{C}l_D) = r\}| \sim 3 \cdot 2^{-r-1}\alpha_\infty(r) \cdot \mathcal{D}(n).$$

Now we follow the argument of [FK10, §1.2] to get Theorem 1.5 from Corollary 1.10 and Lemmas 1.8 and 1.9.

2. 4-ranks of class groups of quadratic function fields. In this section we give some criteria for the 4-ranks of $\mathcal{C}_D$ and $\mathcal{C}l_D$. Throughout this section, we assume that $q \equiv 3 \bmod 4$.

2.1. Case of the narrow ideal class group $\mathcal{C}_D$. For any $a, b \in \mathrm{k}^*$, let $(a|b) \in \{0, 1\}$ be the *Hilbert symbol*, that is, $(a|b) = 1$ if and only if the equation

$$x^2 - ay^2 - bz^2 = 0$$

has a nontrivial solution in k^3.

LEMMA 2.1. *Let $a, b, c \in \mathrm{k}^*$. Then:*

(i) $(a|b) = (b|a)$, $(a|1) = 1$, $(ac^2|b) = (a|b)$, $(a|-a) = 1$, $(a|b) = (a|-ab)$.
(ii) *If $(a|b) = 1$, then $(a|bc) = (a|c)$.*
(iii) *Let $a, b \in \mathbb{A}$ be square-free and $(a, b) = 1$ with $b \in \mathbb{A}^+$. Then $(a|b) = 1$ if and only if a is a square modulo b and b is a square modulo $\tilde{a}$, where $\tilde{a} = \mathrm{sgn}(a)^{-1}a$.*

Proof. (i) and (ii) are easy. (iii) follows from the Hasse–Minkowski principle and the product formula for Hilbert symbols since q is odd. ∎

LEMMA 2.2. *Let $B \in \mathbb{A}^+$ be a divisor of D. Then $(B|\bar{D}) = (B|-\bar{D}/B)$.*

Proof. $(B|-\bar{D}/B) = (B|B\bar{D}/B) = (B|\bar{D})$. ∎

Let $D = P_1 \cdots P_t$, where $P_i \in \mathbb{A}^+_{\mathrm{irr}}$. Let $\mathfrak{p}_i$ be the unique prime ideal of $\mathcal{O}_D$ lying above P_i. For any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_D$, let $[\mathfrak{a}]_+$ denote the image of $\mathfrak{a}$ in $\mathcal{C}_D$.

LEMMA 2.3. *We have $\mathcal{C}_D^G = \langle [\mathfrak{p}_1]_+, \ldots, [\mathfrak{p}_t]_+ \rangle$, where $G = \mathrm{Gal}(\mathrm{k}_D/\mathrm{k})$.*

Proof. Recall that it is assumed that $q \equiv 3 \bmod 4$. Then the result follows immediately from Lemma 2.2 of [BJ]. ∎

Let $\mathfrak{P}$ be the trivial class in $\mathcal{C}_D$ and

$$\mathcal{B} := \{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t} : e_i \in \{0, 1\} \text{ for } 1 \le i \le t\}.$$

LEMMA 2.4.

(i) $2^{\mathrm{rk}_4(\mathcal{C}_D)} = |\{\mathfrak{B}^2 \in \mathcal{C}_D : \mathfrak{B}^4 = \mathfrak{P}\}|$.
(ii) $2^{\mathrm{rk}_4(\mathcal{C}_D)} = \frac{1}{2}|\{\mathfrak{b} \in \mathcal{B} : \mathfrak{a}^2 = (a)\mathfrak{b}$ *for suitable* $\mathfrak{a}$ *and totally positive* $a\}|$.

Now we prove

PROPOSITION 2.5 (First criterion). *We have*

$$2^{\mathrm{rk}_4(\mathcal{C}_D)} = \tfrac{1}{2}|\{B \in \mathbb{A}^{+,o} : B \mid D \text{ and } (B|\bar{D}) = 1\}|.$$

Proof. For a nonzero ideal $\mathfrak{a}$ of k_D let $\mathbf{N}(\mathfrak{a})$ be the monic generator of the ideal $\mathfrak{a}\mathfrak{a}'$, where $\mathfrak{a}'$ is the conjugate of $\mathfrak{a}$. Let $\mathcal{N}$ be the norm map from k_D to k. Then it is easy to see that, for every $a \in \mathrm{k}_D$, we have $\mathbf{N}((a)) = \mathcal{N}(a)$ up to $\mathbb{F}_q^*$.

Let $B \in \mathbb{A}^{+,o}$ be a divisor of D. Suppose first that $(B|\bar{D}) = 1$, that is, $B = \mathcal{N}(b)$ for some $b \in \mathrm{k}_D$. By clearing denominators we can find $a \in \mathrm{k}_D$ such that $\mathcal{N}(a) = BW^2$ with $W \in \mathbb{A}^+$. Thus a or γa is totally positive. Then as in [FK07] we have $(a) = \mathfrak{b}\mathfrak{a}^2$, where $\mathfrak{b}$ is the unique ideal of k_D with $\mathbf{N}(\mathfrak{b}) = B$ and $\mathbf{N}(\mathfrak{a}) = W$.

Now assume that $\mathfrak{a}^2 = (a)\mathfrak{b}$ with $\mathfrak{b} \in \mathcal{B}$ and a totally positive. Let $B = \mathbf{N}(\mathfrak{b})$. Then $\mathbf{N}((a)) = \mathcal{N}(a)$ up to $\mathbb{F}_q^{*2}$, so we may assume $\mathbf{N}((a)) = \mathcal{N}(a)$. Then $\mathcal{N}(a) = \mathbf{N}(\mathfrak{a})^2/\mathbf{N}(\mathfrak{b}) = B \cdot (\mathbf{N}(\mathfrak{a})/B)^2$. ∎

Now we are going to describe the second criterion for $2^{\mathrm{rk}_4(\mathcal{C}_D)}$ when $D \in \mathcal{D}$. Let N be a maximal abelian extension of k_D, unramified at all finite places, whose Galois group $\mathrm{Gal}(\mathrm{N}/\mathrm{k}_D)$ has exponent dividing 4. Write

$$A := \mathrm{Gal}(\mathrm{N}/\mathrm{k}_D) = \mathcal{C}_D/\mathcal{C}_D^4 \cong C(4)^r \times C(2)^s,$$

where $C(m)$ denotes the cyclic group of order m. Then Lemma 11 of [FK10] remains valid in this case too.

We say that $\{D_1, D_2\}$ is a *decomposition* of $D \in \mathbb{A}^{+,o}$ if $D = D_1 D_2$ with $D_1, D_2 \in \mathbb{A}^+$. A decomposition $\{D_1, D_2\}$ of D is said to be *of the second type* if $(D_1|D_2) = 1$, or, equivalently the following conditions hold (cf. Lemma 6 in [FK07], Lemma 13 in [FK10]):

$$\left(\frac{D_1}{P}\right) = 1 \text{ for } P \mid D_2,\ P \in \mathbb{A}^+_{\mathrm{irr}} \quad \text{and} \quad \left(\frac{D_2}{P}\right) = 1 \text{ for } P \mid D_1,\ P \in \mathbb{A}^+_{\mathrm{irr}}.$$

As in §3.2 of [FK10], any $C(4)$-extension K_4 of k_D unramified at finite places corresponds to a decomposition $\{D_1, D_2\}$ of D of the second type, i.e. K_4 is a quadratic extension of $\mathrm{K}_2 = \mathrm{k}(\sqrt{D_1}, \sqrt{D_2})$. For each monic divisor D' of D not contained in $\{1, D_1, D_2, D\}$, the field $\mathrm{K}_4(\sqrt{D'})$ contains a $C(4)$-extension K_4' of k_D unramified at finite places and different from K_4. It is easy to see that K_4 is totally real if and only if K_4' is totally real. Since we get the same K_4' if two D''s only differ by a square in K_2, there are $2^{\omega(D)-2}$ $C(4)$-extensions of k_D unramified at finite places and corresponding to the decomposition $\{D_1, D_2\}$.

Lemma 2.6. *Let $D \in \mathcal{D}$ and $\{D_1, D_2\}$ be a decomposition of D of the second type. Then there exists a nontrivial solution $(x, y, z) \in \mathbb{A}^3$ of*

$$x^2 - D_1 y^2 - D_2 z^2 = 0$$

such that:

(i) *$x^2, D_1 y^2, D_2 z^2$ are pairwise coprime and $x \in \mathbb{A}^+$.*
(ii) $\deg x \geq \max\left\{\deg y + \frac{1}{2}\deg D_1, \deg z + \frac{1}{2}\deg D_2\right\}$.

Proof. (i) is clear. Suppose that $\deg x < \deg y + \frac{1}{2}\deg D_1$. Since $x^2 = D_1 y^2 + D_2 z^2$, we have $\deg y + \frac{1}{2}\deg D_1 = \deg z + \frac{1}{2}\deg D_2$ and $\mathrm{sgn}(y)^2 + \mathrm{sgn}(z)^2 = 0$, which cannot happen for $q \equiv 3 \bmod 4$. Thus (ii) follows. ∎

Let $D \in \mathcal{D}$ and $\{D_1, D_2\}$ be a nontrivial decomposition of D of the second type. Let $\alpha := x + y\sqrt{D_1}$, where (x, y, z) is the solution as in Lemma 2.6 and y is chosen so that $\deg(x + y\sqrt{D_1}) = \deg x$. We may assume α is totally positive by multiplying it by some element $a \in \mathbb{F}_q^*$. Let $\mathrm{K}_2 := \mathrm{k}(\sqrt{D_1}, \sqrt{D_2})$ and $\mathrm{K}_4 := \mathrm{K}_2(\sqrt{\alpha})$. Then K_4 is a $C(4)$-extension of k_D unramified at finite places and corresponding to $\{D_1, D_2\}$.

Now one can follow §3.2 of [FK10] to get the following proposition.

PROPOSITION 2.7 (Second criterion). *Let $D \in \mathcal{D}$. Then*

$$2^{\mathrm{rk}_4(\mathcal{C}_D)} = |\{\{D_1, D_2\} : \{D_1, D_2\} \textit{ is a decomposition of } D \textit{ of the second type}\}|.$$

2.2. Case of the ordinary ideal class group $\mathcal{C}l_D$. For any $A \in \mathbb{A}$ and $P \in \mathbb{A}^+_{\mathrm{irr}}$, we define

$$[A, P]_4 := \begin{cases} 1 & \text{if } \left(\frac{A}{P}\right) = 1 \text{ and } A \text{ is a fourth power modulo } P, \\ -1 & \text{if } \left(\frac{A}{P}\right) = 1 \text{ and } A \text{ is not a fourth power modulo } P, \\ 0 & \text{otherwise.} \end{cases}$$

For $B = P_1 \cdots P_s \in \mathbb{A}^+$, we define

$$[A, B]_4 := [A, P_1]_4 \cdots [A, P_s]_4.$$

LEMMA 2.8. *Let $D \in \mathcal{D}$ and $\{D_1, D_2\}$ be a decomposition of the second type. Let (x, y, z) be a solution of $x^2 - D_1y^2 - D_2z^2 = 0$ as in Lemma 2.6. Then:*

(i) $\left(\frac{z}{D_1}\right) = \left(\frac{y}{D_2}\right) = 1$.
(ii) $\left(\frac{x}{D_1}\right) = [D_2, D_1]_4$ *and* $\left(\frac{x}{D_2}\right) = [D_1, D_2]_4$.
(iii) $\left(\frac{D}{x}\right) = \left(\frac{D_1D_2}{x}\right) = \left(\frac{-1}{x}\right)$.

Proof. Straightforward. ∎

PROPOSITION 2.9. *Let $D \in \mathcal{D}$ and $\{D_1, D_2\}$ be a nontrivial decomposition of D of the second type. Then the corresponding unramified $C(4)$-extensions are totally real if and only if $[D_1, D_2]_4 = [D_2, D_1]_4$.*

Proof. Let $\mathrm{K}_4 = \mathrm{K}_2(\sqrt{\alpha})$ be the $C(4)$-extension of k_D defined in §2.1. It is sufficient to show that K_4 is totally real if and only if $[D_1, D_2]_4 = [D_2, D_1]_4$. We can easily see that K_4 is a totally real extension of k if and only if $\deg x$ is even, and by using Lemma 2.8, $[D_1, D_2]_4[D_2, D_1]_4 = (-1)^{\deg x}$. Hence we get the result. ∎

Now using Lemma 11 and the remark before Theorem 5 of [FK10], we get the following criterion:

PROPOSITION 2.10. *Let $D \in \mathcal{D}$. Then $2^{\mathrm{rk}_4(\mathcal{C}l_D)}$ is given by*

$$\tfrac{1}{2}|\{(A,B) \in (\mathbb{A}^{+,o})^2 : D = AB,\ [A,B]_4 = [B,A]_4 = 1 \text{ or } -1\}|.$$

Let $\mathbb{B} := \mathbb{F}_{q^2}[T]$ and $\mathrm{k}' := \mathbb{F}_{q^2}(T)$. Let $\beta = \sqrt{-1} \in \mathbb{B}$. Then $\mathbb{B} = \mathbb{A}[\beta]$. We use $\bar{v}$ to denote the conjugate of $v \in \mathrm{k}'$ over k. Since $q^2 \equiv 1 \bmod 4$, the quartic residue symbol $(-)_4$ can be defined on $\mathbb{B}$.

LEMMA 2.11. *Let $P \in \mathbb{A}^+_{\mathrm{irr}}$ be of even degree, decomposed as $P = \pi\bar{\pi}$ with $\pi \in \mathbb{B}^+_{\mathrm{irr}}$ and $A \in \mathbb{A}$. Then:*

(i) $\left(\frac{A}{\pi}\right)_4^2 = \left(\frac{A}{P}\right)$.
(ii) *A is a 4th power modulo P if and only if $\left(\frac{A}{\pi}\right)_4 = 1$.*
(iii) *A is a square but not a 4th power modulo P if and only if $\left(\frac{A}{\pi}\right)_4 = -1$.*
(iv) $[A,P]_4 = \frac{1}{2}\left(1 + \left(\frac{A}{P}\right)\right)\left(\frac{A}{\pi}\right)_4$.

Proof. This follows from the fact that $\mathbb{B}/(\pi) = \mathbb{A}/(P)$ and the definitions. ∎

A prime $\pi = A + \beta B \in \mathbb{B}^+_{\mathrm{irr}}$ is called *privileged* if $\mathrm{sgn}(B) \in \mathbb{F}_q^{*2}$ and the degree of $\mathcal{N}(\pi) = P \in \mathbb{A}^+_{\mathrm{irr}}$ is even, where $\mathcal{N}$ is the norm map from k' to k. An element of $\mathbb{B}^+$ is called *privileged* if it is a product of privileged irreducible elements. It is clear from the definition that every $D \in \mathcal{D}$ can be written uniquely as $D = \mathfrak{d}\bar{\mathfrak{d}}$ with $\mathfrak{d}$ privileged. Such a factorization is called a *privileged factorization*.

Using Lemma 2.11(iv) and Proposition 2.10, we get

PROPOSITION 2.12. *For any $D \in \mathcal{D}$,*

$$2^{\mathrm{rk}_4(\mathcal{C}l_D)} = \frac{2^{\mathrm{rk}_4(\mathcal{C}_D)}}{2} + \frac{1}{4 \cdot 2^{\omega(D)}} \sum_{D=AB} \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_4^2 \prod_{P|A}\left(1+\left(\frac{B}{P}\right)\right)\prod_{P|B}\left(1+\left(\frac{A}{P}\right)\right),$$

where $A, B \in \mathbb{A}^+$ and $A = \mathfrak{a}\bar{\mathfrak{a}}, B = \mathfrak{b}\bar{\mathfrak{b}}$ are privileged factorizations.

COROLLARY 2.13. *For any $D \in \mathcal{D}$,*

$$2^{\mathrm{rk}_4(\mathcal{C}l_D)} = \frac{2^{\mathrm{rk}_4(\mathcal{C}_D)}}{2} + \frac{1}{4 \cdot 2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \left(\frac{\mathfrak{d}_0\bar{\mathfrak{d}}_1}{\mathfrak{d}_2\bar{\mathfrak{d}}_3}\right)_4^2, \tag{2.1}$$

where $D_0, D_1, D_2, D_3 \in \mathbb{A}^+$ and $D_0 = \mathfrak{d}_0\bar{\mathfrak{d}}_0, D_1 = \mathfrak{d}_1\bar{\mathfrak{d}}_1, D_2 = \mathfrak{d}_2\bar{\mathfrak{d}}_2$ and $D_3 = \mathfrak{d}_3\bar{\mathfrak{d}}_3$ are privileged factorizations.

3. Character sums in $\mathbb{A} = \mathbb{F}_q[T]$. The results in this section hold true for any odd q. We do not assume $q \equiv 3 \bmod 4$. Let λ be an additive character of conductor $F \in \mathbb{A}$ of degree f. Then λ is completely determined

by the additive characters $\lambda^{(i)} : \mathbb{F}_q \to \mathbb{C}^*$ for $0 \le i \le f-1$, given by $\lambda^{(i)}(\alpha) = \lambda(\alpha T^i)$. Let $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ be the trace map of $\mathbb{F}_q$ into $\mathbb{F}_p$. Since the bilinear form $\langle \alpha, \beta \rangle := \zeta_p^{\mathrm{Tr}(\alpha\beta)}$ is nondegenerate, each additive character $\lambda^{(i)}$ is completely determined by $\lambda_i \in \mathbb{F}_q$ such that $\lambda^{(i)}(\alpha) = \zeta_p^{\mathrm{Tr}(\alpha\lambda_i)}$, where ζ_p is a fixed primitive pth root of unity in $\mathbb{C}$. Therefore we say that an additive character λ modulo F is *determined by* $(\lambda_0, \dots, \lambda_{f-1}) \in \mathbb{F}_q^f$ if

$$\lambda\Big(\sum_{i=0}^{f-1} \alpha_i T^i\Big) = \prod_{i=0}^{f-1} \zeta_p^{\mathrm{Tr}(\alpha_i \lambda_i)}.$$

We associate an $f \times f$ matrix Λ to each additive character λ modulo F as follows. For $M \in \mathbb{A}$, write M_F for the polynomial of degree $< \deg F$ which is congruent to M modulo F. Let $c_{F,i}(M)$ be the coefficient of T^i in M_F and $\mathbf{c}_F(M) = (c_{F,0}(M), \dots, c_{F,f-1}(M))$. Write $F = T^f - b_{f-1}T^{f-1} - \cdots - b_1 T - b_0$. For $i \ge 0$, write

$$T^{f-1+i} \equiv \sum_{a=0}^{f-1} \epsilon_{i,a} T^a \bmod F.$$

Then we have the recursive formula

$$\epsilon_{i+1,j} = \epsilon_{i,j-1} + b_j \epsilon_{i,f-1},$$

where $\epsilon_{i,j} = 0$ for $j < 0$, $\epsilon_{0,j} = 0$ for $j < f-1$, $\epsilon_{0,f-1} = 1$ and $\epsilon_{1,j} = b_j$. Define

$$\lambda_{i,j} = \lambda_{i+j} \quad \text{if } j < f-i,$$
$$\lambda_{i,f-i+a} = \sum_{j=0}^{f-1} \epsilon_{a,j} \lambda_j \quad \text{for } 0 \le a < i.$$

Let Λ be the $f \times f$ matrix with entries $\lambda_{i,j}$. Then we can easily see that

$$\lambda(AX) = \zeta_p^{\mathrm{Tr}(\sum_{a=0}^{f-1} c_{F,a}(AX)\lambda_a)} = \zeta_p^{\mathrm{Tr}(\mathbf{c}_F(A)\Lambda \mathbf{c}_F(X)^t)}. \tag{3.1}$$

Note that Λ is symmetric, since $\lambda(AX) = \lambda(XA)$. In fact, $\lambda_{i,j} = \lambda_{a,b}$ whenever $i + j = a + b$. It is not difficult to see that an additive character λ is primitive if and only if the associated matrix Λ is nonsingular.

For a primitive multiplicative character χ and an additive character λ of conductor F, we define the *Gauss sum* $\tau(\chi, \lambda)$ by

$$\tau(\chi, \lambda) := \sum_{M \bmod F} \chi(M)\lambda(M).$$

For an additive character λ and $N \in \mathbb{A}$, let λ_N be the character defined by $\lambda_N(A) = \lambda(NA)$. As in Lemmas 4.7 and 4.8 of [Wa97], we have the following lemmas.

LEMMA 3.1. *Let χ be a primitive multiplicative character and λ an additive character modulo F of degree f. Then*

$$\chi(N)\tau(\overline{\chi},\lambda) = \sum_{M \bmod F} \overline{\chi}(M)\lambda(MN) = \tau(\overline{\chi},\lambda_N),$$

$$\lambda(A) = \frac{1}{\phi(F)} \sum_{\chi \bmod F} \overline{\chi}(A)\tau(\chi,\lambda),$$

where $\phi(F) = |(\mathbb{A}/F\mathbb{A})^*|$.

LEMMA 3.2. *Let χ be a primitive multiplicative character and λ an additive character modulo F of degree f. Then*

$$|\tau(\chi,\lambda)| = \begin{cases} q^{f/2} & \text{if } \lambda \text{ is primitive,} \\ 0 & \text{if } \lambda \text{ is not primitive.} \end{cases}$$

COROLLARY 3.3. *Let χ be a primitive multiplicative character and λ an additive character modulo F of degree f. Then*

$$\chi(N) = \frac{\tau(\chi,A)}{q^f} \sum_{M \bmod F} \overline{\chi}(M)\lambda(-MN) = \frac{\tau(\chi,\lambda)\tau(\overline{\chi},\overline{\lambda}_N)}{q^f}.$$

For an integer $r \geq 0$ and $X \in \mathbb{A}$, define

$$\alpha_r(\lambda, X) := \sum_{N \in \mathbb{A}_r^+} \lambda(-NX).$$

Note that $\alpha_r(\lambda, X) = 0$ for $r \geq f$, unless $X \not\equiv 0 \bmod F$.

LEMMA 3.4. *Let the notation be as before and write*

$$\boldsymbol{\Lambda}\mathbf{c}_F(X) = (D_0(X), D_1(X), \ldots, D_{f-1}(X)).$$

Then, for $r < f$,

$$\alpha_r(\lambda, X) = \begin{cases} q^r \zeta_p^{\mathrm{Tr}(D_r(X))} & \text{if } D_0(X) = \cdots = D_{r-1}(X) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. From (3.1) we can easily see that

$$\alpha_r(\lambda, X) = \zeta_p^{\mathrm{Tr}(D_r(X))} \prod_{i=0}^{r-1} \Big(\sum_{a_i \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(a_i D_i(X))} \Big)$$

and the result follows. ∎

Now we will prove an analogue of the Pólya inequality [Ap76, Theorem 8.21], which will be used to prove Proposition 3.6.

LEMMA 3.5. *Let χ be a primitive multiplicative character modulo F of degree f. Then*

$$\Big| \sum_{N \in \mathbb{A}_r^+} \chi(N) \Big| \leq q^{f/2}.$$

Proof. Note that $\sum_{N\in\mathbb{A}_r^+}\chi(N)=0$ for $r\ge f$. We therefore assume that $r<f$. Let λ be a primitive additive character modulo F. By Lemma 3.2 and Corollary 3.3 we have, for any subset $\mathcal{Z}$ of $\mathbb{A}$,

$$q^{f/2}\Big|\sum_{N\in\mathcal{Z}}\chi(N)\Big|=\Big|\sum_{N\in\mathcal{Z}}\sum_{M \bmod F}\overline{\chi}(M)\lambda(-MN)\Big|\le\sum_{M \bmod F}\Big|\sum_{N\in\mathcal{Z}}\lambda(-MN)\Big|.$$

Let $\mathcal{Z}=\mathbb{A}_r^+$. Then $|\sum_{N\in\mathcal{Z}}\lambda(-MN)|=|\alpha_r(\lambda,M)|$ equals q^r if and only if M satisfies $D_i(M)=0$ for $0\le i\le r-1$, and 0 otherwise. Thus $\mathbf{c}_F(M)=(c_0(M),\dots,c_{f-1}(M))$ satisfies r linearly independent relations, and so there are q^{f-r} possible M's with $|\alpha_r(\lambda,M)|=q^r$, which completes the proof. ∎

Let μ be the Möbius function on $\mathbb{A}$, i.e., for any $N\in\mathbb{A}$, $\mu(N)=(-1)^{\omega(N)}$ if N is square-free and $\mu(N)=0$ otherwise. For $M=\beta\prod_i P_i^{e_i}$ with $P_i\in\mathbb{A}^+_{\mathrm{irr}}$ and $\beta\in\mathbb{F}_q^*$, define the *Jacobi symbol* by

$$\left(\frac{N}{M}\right):=\prod_i\left(\frac{N}{P_i}\right)^{e_i}\quad\text{and}\quad\left(\frac{N}{1}\right):=1,$$

where $\left(\frac{N}{P}\right)$ is the Legendre symbol. We prove the following analogue of [FK07, Lemma 15].

Proposition 3.6. *Let a_M and b_N be complex numbers of modulus less than 1 for $M,N\in\mathbb{A}^+$. Then*

$$\Big|\sum_{M\in\mathbb{A}_m^+}\sum_{N\in\mathbb{A}_n^+}a_Mb_N\mu^2(M)\mu^2(N)\left(\frac{N}{M}\right)\Big|\ll q^{m+n}(q^{-m/4}+q^{-n/4}).$$

Proof. Let

$$\Delta=\Big|\sum_{M\in\mathbb{A}_m^+}\sum_{N\in\mathbb{A}_n^+}a_Mb_N\mu^2(M)\mu^2(N)\left(\frac{N}{M}\right)\Big|.$$

Then using the Cauchy–Schwarz inequality, we have

$$\begin{aligned}\Delta^2&\le\sum_{M\in\mathbb{A}_m^+}1\sum_{M\in\mathbb{A}_m^+}\Big|\sum_{N\in\mathbb{A}_n^+}a_Mb_N\mu^2(M)\mu^2(N)\left(\frac{N}{M}\right)\Big|^2\\&\le q^m\sum_{M\in\mathbb{A}_m^+}\mu^2(M)\Big|\sum_{N\in\mathbb{A}_n^+}b_N\mu^2(N)\left(\frac{N}{M}\right)\Big|^2\\&=q^m\sum_{M\in\mathbb{A}_m^+}\mu^2(M)\Big|\sum_{N_1\in\mathbb{A}_n^+}\sum_{N_2\in\mathbb{A}_n^+}b_{N_1}b_{N_2}\mu^2(N_1)\mu^2(N_2)\left(\frac{N_1N_2}{M}\right)\Big|\\&=q^m\Big|\sum_{N_1\in\mathbb{A}_n^+}\sum_{N_2\in\mathbb{A}_n^+}b_{N_1}b_{N_2}\mu^2(N_1)\mu^2(N_2)\sum_{M\in\mathbb{A}_m^+}\mu^2(M)\left(\frac{N_1N_2}{M}\right)\Big|.\end{aligned}$$

Thus,

$$\begin{aligned}\Delta^4 &\le q^{2m}\Big|\sum_{N_1\in\mathbb{A}_n^+}\sum_{N_2\in\mathbb{A}_n^+} b_{N_1}b_{N_2}\mu^2(N_1)\mu^2(N_2)\sum_{M\in\mathbb{A}_m^+}\mu^2(M)\Big(\frac{N_1N_2}{M}\Big)\Big|^2\\ &\le q^{2m}\sum_{N_1\in\mathbb{A}_n^+}\sum_{N_2\in\mathbb{A}_n^+}1\sum_{N\in\mathbb{A}_{2n}^+}2\Big(\sum_{M\in\mathbb{A}_m^+}\mu^2(M)\Big(\frac{N}{M}\Big)\Big)^2\\ &\le 2q^{2(m+n)}\sum_{M_1\in\mathbb{A}_m^+}\mu^2(M_1)\sum_{M_2\in\mathbb{A}_m^+}\mu^2(M_2)\sum_{N\in\mathbb{A}_{2n}^+}\Big(\frac{N}{M_1M_2}\Big).\end{aligned}$$

If $M_1 = M_2$, then

$$\sum_{N\in\mathbb{A}_{2n}^+}\Big(\frac{N}{M_1M_2}\Big) = q^{2n}.$$

From Lemma 3.5, for $M_1 \neq M_2$, we have

$$\sum_{N\in\mathbb{A}_{2n}^+}\Big(\frac{N}{M_1M_2}\Big) \le q^m.$$

Therefore,

$$\Delta^4 \le 2q^{2m+2n}(q^mq^{2n} + (q^{2m} - q^m)q^m) \ll q^{5m+2n} + q^{3m+4n}.$$

Hence

$$\Delta \ll q^{m+n}(q^{(m-2n)/4} + q^{-m/4}).$$

Now by interchanging M and N, we get

$$\Delta \ll q^{m+n}(q^{(n-2m)/4} + q^{-n/4}).$$

It is easy to see that

$$\min\{q^{(m-2n)/4} + q^{-m/4}, q^{(n-2m)/4} + q^{-n/4}\} \le q^{-m/4} + q^{-n/4}.$$

Hence we get the result. ∎

We remark that since Proposition 3.6 holds for any q, we do not need any analogue of Proposition 9 of [FK10].

We quote the following estimate of character sums for later use.

Proposition 3.7 ([Hs98, Theorem 2.1]). *Let χ be a nontrivial character modulo M. Then*

$$\Big|\sum_{P\in\mathbb{A}_{\mathrm{irr},n}^+}\chi(P)\Big| \le (\deg M + 1)\frac{q^{n/2}}{n}.$$

Corollary 3.8. *For any positive real number ϵ,*

$$\Big|\sum_{P\in\mathbb{A}_{\mathrm{irr},n}^+}\chi(P)\Big| \ll_\epsilon q^{2n/3}n^{-\epsilon}.$$

4. A Brun–Titchmarsh theorem for multiplicative functions over $\mathbb{A}$. Again q is an arbitrary power of an odd prime. In this section A, B, C (resp. L, M, N) usually denote polynomials (resp. monic polynomials) in $\mathbb{A} = \mathbb{F}_q[T]$, and P, Q denote monic irreducible polynomials in $\mathbb{A}$ unless otherwise stated.

LEMMA 4.1. *For $q \geq 3$,*

$$\sum_{\deg P \leq m} \frac{1}{\deg P} \leq \frac{q^{m+1}}{m^2}.$$

Proof. It is known [Ro02, Proposition 2.1] that the number of monic irreducible polynomials of degree n is less than q^n/n for $n > 1$ and equal to q for $n = 1$. Thus we have

$$\sum_{\deg P \leq m} \frac{1}{\deg P} \leq \sum_{n=1}^{m} \frac{q^n}{n^2}.$$

It suffices to show that

$$\sum_{n=1}^{m} \frac{q^n}{n^2} \leq \frac{q^{m+1}}{m^2}.$$

This is trivially true for $m = 1, 2$. Now use induction on m to get the result. ∎

Let $p(N) := \max\{\deg P : P \in \mathbb{A}^+_{\rm irr},\ P \mid N\}$ and $q(N) := \min\{\deg P : P \in \mathbb{A}^+_{\rm irr},\ P \mid N\}$. For any integers $m, n \geq 1$, let

$$\Psi(n, m) := \sum_{\substack{\deg N = n \\ p(N) \leq m}} 1.$$

LEMMA 4.2. *For all sufficiently large n,*

$$\Psi(n, \log_q n) \leq q^{(q+1)n/\log_q n}.$$

Proof. For any $\delta > 0$, we have

$$\begin{aligned}
\Psi(n, m) = q^{n\delta} \sum_{\substack{\deg N = n \\ p(N) \leq m}} \frac{1}{q^{\delta \deg N}} &\leq q^{n\delta} \prod_{\deg P \leq m} \left(1 + \frac{1}{q^{\delta \deg P}} + \frac{1}{q^{2\delta \deg P}} + \cdots\right) \\
&= q^{n\delta} \prod_{\deg P \leq m} \left(1 + \frac{1}{q^{\delta \deg P} - 1}\right) \\
&\leq \exp\left(n\delta \log q + \frac{1}{\delta} \sum_{\deg P \leq m} \frac{1}{\deg P} \log q\right) \\
&= q^{n\delta + \frac{1}{\delta} \sum_{\deg P \leq m} \frac{1}{\deg P}} \\
&\leq q^{n\delta + \frac{q^{m+1}}{\delta m^2}} \qquad \text{(by Lemma 4.1).}
\end{aligned}$$

Now take $m = \log_q n$ and $\delta = 1/\log_q n$ to get the result. ∎

Let $\mathcal{P}$ be an infinite subset of $\mathbb{A}_{\mathrm{irr}}^{+}$. For each integer $m \geq 1$, we let

$$\mathcal{P}(m) := \prod_{\substack{P \in \mathcal{P} \\ \deg P \leq m}} P.$$

We have the following analogue of [HR74, Theorem 3.4].

PROPOSITION 4.3. *Suppose that* $(L, P) = 1$ *for any* $P \in \mathcal{P}$. *Then for any* $m \geq 2$,

$$|\{N : \deg N = n, N \equiv A \bmod L \text{ and } (N, \mathcal{P}(m)) = 1\}| \leq \frac{1}{\prod_{\deg P \leq m, P \notin \mathcal{P}} (1 - q^{-\deg P})} \frac{q^n}{m q^{\deg L}} + \Sigma,$$

where $\Sigma < q^{2m}$.

Let

$$\Phi(n, m; L, A) := \sum_{\substack{\deg N = n \\ N \equiv A \bmod L \\ q(N) \geq m}} 1.$$

LEMMA 4.4. *Suppose that* $(A, L) = 1$ *with* $\deg L < n$ *and* $m \geq 1$. *Then*

$$\Phi(n, m; L, A) \leq \frac{q^n}{\phi(L) m} + q^{2m},$$

where $\phi(L)$ *is the number of polynomials of degree* $< \deg L$ *prime to* L.

Proof. This follows from Proposition 4.3 by taking $\mathcal{P} = \{P \in \mathbb{A}_{\mathrm{irr}}^{+} : P \nmid L\}$. ∎

Consider the class $\mathcal{M}$ of functions f on $\mathbb{A}$ which are nonnegative multiplicative and satisfy the following two conditions:

(i) There exists a positive constant A_1 such that

$$f(P^{\ell}) \leq A_1^{\ell} \quad \text{for all } P \in \mathbb{A}_{\mathrm{irr}}^{+} \text{ and } \ell \geq 1.$$

(ii) For every $\epsilon > 0$, there exists a positive constant $A_2 = A_2(\epsilon)$ such that

$$f(N) \leq A_2 |N|^{\epsilon} \quad \text{for all } N \in \mathbb{A}.$$

One can follow exactly the same method as in [Sh80] to get the following lemmas.

LEMMA 4.5. *Let* $f \in \mathcal{M}$. *Then as* $n \to +\infty$,

$$\sum_{\substack{\deg N \leq n \\ (N, L) = 1}} \frac{f(N)}{q^{\deg N}} \ll \exp\Bigg(\sum_{\substack{\deg P \leq n \\ P \nmid L}} \frac{f(P)}{q^{\deg P}} \Bigg)$$

uniformly in L.

LEMMA 4.6. *Let $f \in \mathcal{M}$. Then as $m \to +\infty$,*

$$\sum_{\substack{\deg N \ge m/2 \\ p(N) \le m/r \\ (N,L)=1}} \frac{f(N)}{q^{\deg N}} \ll \exp\Bigg(\sum_{\substack{\deg P \le m \\ P \nmid L}} \frac{f(P)}{q^{\deg P}} - \frac{r \log r}{10} \Bigg)$$

uniformly in L and r, provided that $1 < r \le m/\log m$.

Proof. Almost the same proof as in [Sh80, Lemma 4] gives

$$\sum_{\substack{\deg N \ge n \\ p(N) \le m' \\ (N,L)=1}} \frac{f(N)}{q^{\deg N}} \ll \exp\Bigg(\sum_{\substack{\deg P \le m \\ P \nmid L}} \frac{f(P)}{q^{\deg P}} - n(\delta - 1)\log q + 2A_1 q^{m'(1-\delta)} \Bigg).$$

Now take $n = m/2, m' = m/r$ and $\delta = 1 - r/(4m \log_r q)$, and the result follows. ∎

THEOREM 4.7. *Let $f \in \mathcal{M}$, $0 < \alpha < 1/2$ and $(A, L) = 1$ with $\deg A < \deg L$. Then as $n \to +\infty$,*

$$\sum_{\substack{\deg N = n \\ N \equiv A \bmod L}} f(N) \ll \frac{q^n}{n\phi(L)} \exp\Bigg(\sum_{\substack{\deg P \le n \\ P \nmid L}} \frac{f(P)}{q^{\deg P}} \Bigg)$$

provided that $\deg L < (1 - \alpha)n$.

Proof. Let $z = \frac{\alpha}{10} n$. Equip $\mathbb{A}^+_{\mathrm{irr}}$ with a total order "$<$" satisfying $P < Q$ if $\deg P < \deg Q$. Let $\mathcal{Z} = \mathcal{Z}(n, A, L) := \{N \in \mathbb{A}^+_n : N \equiv A \bmod L\}$. For each $N \in \mathcal{Z}$, we express N in the form

$$N = P_1^{s_1} \cdots P_j^{s_j} P_{j+1}^{s_{j+1}} \cdots P_\ell^{s_\ell} = B_N D_N,$$

where $P_i < P_j$ for $i < j$ and $B_N = P_1^{s_1} \cdots P_j^{s_j}$ is chosen so that

$$\deg B_N \le z < \deg(B_N P_{j+1}^{s_{j+1}}).$$

We divide $\mathcal{Z}$ into the following four subsets $\mathcal{Z}_i$, $1 \le i \le 4$:

$$\begin{aligned}
\mathcal{Z}_1 &= \{N \in \mathcal{Z} : q(D_N) > z/2\}, \\
\mathcal{Z}_2 &= \{N \in \mathcal{Z} : q(D_N) \le z/2 \text{ and } \deg B_N \le z/2\}, \\
\mathcal{Z}_3 &= \{N \in \mathcal{Z} : q(D_N) \le \log n \text{ and } \deg B_N > z/2\}, \\
\mathcal{Z}_4 &= \{N \in \mathcal{Z} : \log n < q(D_N) \le z/2 \text{ and } \deg B_N > z/2\}.
\end{aligned}$$

First for $\mathcal{Z}_1$, one can easily show that

$$\sum_{N \in \mathcal{Z}_1} f(N) \ll \sum_{\substack{\deg B \le z \\ (B,L)=1}} f(B) \Phi(n - \deg B, z/2; L, A).$$

Then

$$\begin{aligned}\sum_{N\in\mathcal{Z}_1} f(N) &\ll \sum_{\substack{\deg B\le z\\(B,L)=1}} f(B)\left(\frac{2q^{n-\deg B}}{z\phi(L)}+q^z\right) \quad \text{(by Lemma 4.4)}\\ &\le \left(\frac{2q^n}{z\phi(L)}+q^{2z}\right)\sum_{\substack{\deg B\le z\\(B,L)=1}}\frac{f(B)}{q^{\deg B}}\\ &\le \left(\frac{2q^n}{z\phi(L)}+q^{2z}\right)\exp\left(\sum_{\deg P\le z}\frac{f(P)}{q^{\deg P}}\right) \quad \text{(by Lemma 4.5).}\end{aligned}$$

To each $N\in\mathcal{Z}_2$, there correspond P and s such that $P^s \,\|\, N, \deg P\le z/2$ and $s\deg P > z/2$. Let s_P be the least positive integer s satisfying $s\deg P > z/2$, so that $s_P\ge 2$, and so

$$s_P \deg P \ge \max\{2\deg P, z/2\}.$$

Thus,

$$\sum_{\deg P\le z/2}\frac{1}{q^{s_P\deg P}} \le \sum_{\deg P\le z/4} q^{-z/2} + \sum_{z/4<\deg P\le z/2}\frac{1}{q^{2\deg P}} \ll q^{-z/4}.$$

It follows that

$$\sum_{N\in\mathcal{Z}_2} 1 \ll \frac{q^n}{q^{\deg L}}q^{-z/4}+q^{z/2}.$$

For $N\in\mathcal{Z}_3$, there exists B such that $B\,|\,N$, $z/2<\deg B\le z$ and $p(B)\le \log n$. Then

$$\begin{aligned}\sum_{N\in\mathcal{Z}_3} 1 &\le \sum_{\substack{z/2<\deg B\le z\\ p(B)\le\log n}}\sum_{\substack{\deg N=n\\ N\equiv A \bmod L\\ N\equiv 0 \bmod B}} 1\\ &= \sum_{\substack{z/2<\deg B\le z\\ p(B)\le\log n}}\left(\frac{q^n}{q^{\deg L}q^{\deg B}}+O(1)\right)\\ &\le \frac{q^n}{q^{\deg L}}q^{-z/2}\Psi(z,\log_q n)+O(q^z)\\ &\ll \frac{q^n}{q^{\deg L}}q^{-z/2} \quad \text{(by Lemma 4.2 and } \frac{q+1}{\log_q n}<\frac{1}{4} \text{ for large } n).\end{aligned}$$

Since $f\in\mathcal{M}$, we have $f(N)\ll (q^{\deg N})^{\alpha/80}\le q^{z/8}$, so that

$$\sum_{N\in\mathcal{Z}_2\cup\mathcal{Z}_3} f(N) \ll \frac{q^n}{q^{\deg L}}q^{-z/8}.$$

Lastly,

$$\sum_{N\in\mathcal{Z}_4} f(N) \le \sum_{z/2<\deg B\le z} \sum_{\substack{\deg N=n\\ N\equiv A \bmod L\\ B_N=B,\, q(D_N)\ge p(B)\\ \log n<q(D_N)\le z/2}} f(D_N).$$

Put $r_0 = [z/\log n]$, so that $z/(r_0+1) < \log n$. Let $2 \le r \le r_0$. Consider those N for which $z/(r+1) < q(D_N) \le z/r$. For such N, we have $p(B_N) = p(B) \le q(D_N) < z/r$, and

$$\omega(D_N) \le \frac{n}{q(D_N)} \le \frac{(r+1)n}{z} < \frac{10(r+1)}{\alpha} < \frac{20r}{\alpha},$$

so that $f(D_N) \le A_1^{\omega(D_N)} \le A_5^r$, where $A_5 = A_1^{20/\alpha}$. Then

$$\sum_{N\in\mathcal{Z}_4} f(N) \le \sum_{2\le r\le r_0} A_5^r \sum_{\substack{z/2<\deg B\le z\\ p(B)<z/r\\ (B,L)=1}} f(B)\Phi\Big(n-\deg B, \frac{z}{r+1}; L, A'\Big),$$

where $A' \equiv A\overline{B}$ and $B\overline{B} \equiv 1 \bmod L$. Applying Lemma 4.4, we have

$$\begin{aligned}\sum_{N\in\mathcal{Z}_4} f(N) &\le \Big(\frac{q^n}{z\phi(L)} + q^{2z}\Big) \sum_{2\le r\le r_0} (r+1)A_5^r \sum_{\substack{z/2<\deg B\le z\\ p(B)<z/r\\ (B,L)=1}} \frac{f(B)}{q^{\deg B}}\\ &\ll \Big(\frac{q^n}{z\phi(L)} + q^{2z}\Big)\\ &\quad\times \exp\Big(\sum_{\substack{\deg P\le z\\ P\nmid L}} \frac{f(P)}{q^{\deg P}}\Big) \sum_{2\le r\le r_0} rA_5^r \exp\Big(-\frac{r}{10}\log r\Big)\\ &\ll \Big(\frac{q^n}{z\phi(L)} + q^{2z}\Big) \exp\Big(\sum_{\substack{\deg P\le z\\ P\nmid L}} \frac{f(P)}{q^{\deg P}}\Big).\end{aligned}$$

Now $\deg L < (1-\alpha)n$ implies

$$q^{2z} < \frac{q^{\deg L}}{\phi(L)} q^{3z} z < \frac{q^{n(1-\alpha+3\alpha/10)}}{\phi(L)z} < \frac{q^n}{\phi(L)z}.$$

Therefore

$$\sum_{N\in\mathcal{Z}_1} f(N) + \sum_{N\in\mathcal{Z}_4} f(N) \ll \frac{q^n}{\phi(L)z} \exp\Big(\sum_{\substack{\deg P\le z\\ P\nmid L}} \frac{f(P)}{q^{\deg P}}\Big). \ \blacksquare$$

COROLLARY 4.8. *Let γ be a positive real number. Then*

$$\sum_{\substack{N\in\mathcal{D}\\ \deg N=n}} \gamma^{\omega(N)} \ll_\gamma q^n n^{\gamma/2-1}.$$

Proof. Since

$$\sum_{\deg P=n} \frac{1}{q^{\deg P}} \ll \frac{1}{n},$$

we have

$$\sum_{\substack{\deg P\le n\\ \deg P \text{ even}}} \frac{1}{q^{\deg P}} \ll \frac{\log n}{2}.$$

Applying Theorem 4.7 to $f(N)=\gamma^{\omega(N)}$ and summing over all A with $(A,L)=1$ and $\deg A<\deg L$, we get the result. ∎

5. Proof of Theorem 1.1. In this section, we assume that $q\equiv 3 \bmod 4$. We are going to study the sum

$$S(n,h)=\sum_{D\in\mathbb{A}_n^{+,o}} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)}$$

for a positive integer h and for positive even (odd) integers $n\to+\infty$. We can closely follow the arguments of [FK07, §5] (resp. [FK07, §6]) if n is odd (resp. even).

The following lemma can be easily deduced from Lemma 2.1(iii), Lemma 2.2 and Proposition 2.5.

LEMMA 5.1. *For any $D\in\mathbb{A}_n^{+,o}$,*

$$2^{\mathrm{rk}_4(\mathcal{C}_D)}=\tfrac{1}{2}|\{(A,B)\in(\mathbb{A}^+)^2 : D=AB,\ (-1)^{1+\deg D}A \text{ is a square modulo } B \text{ and } B \text{ is a square modulo } A\}|.$$

Then as in [FK07, §5, §6], we also have

LEMMA 5.2. *Let $D\in\mathbb{A}_n^{+,o}$. Then if n is odd,*

$$2^{\mathrm{rk}_4(\mathcal{C}_D)}=\frac{1}{2^{1+\omega(D)}}\sum_{D=D_0D_1D_2D_3}\left(\frac{D_2}{D_0}\right)\left(\frac{D_1}{D_3}\right)\left(\frac{D_0}{D_3}\right)\left(\frac{D_3}{D_0}\right),$$

and if n is even,

$$2^{\mathrm{rk}_4(\mathcal{C}_D)}=\frac{1}{2^{1+\omega(D)}}\sum_{D=D_0D_1D_2D_3}\left(\frac{-1}{D_3}\right)\left(\frac{D_2}{D_0}\right)\left(\frac{D_1}{D_3}\right)\left(\frac{D_0}{D_3}\right)\left(\frac{D_3}{D_0}\right),$$

where $D_i\in\mathbb{A}^{+,o}$ for $0\le i\le 3$.

We replace the indices $0,1,2,3$ by their expansions in base 2: $00,01,10,11$, viewed as elements of $\mathbb{F}_2^2$. For $\mathbf{u}=(u_1,u_2)$ and $\mathbf{v}=(v_1,v_2)\in\mathbb{F}_2^2$, write $\Phi_1(\mathbf{u},\mathbf{v}):=(u_1+v_1)(u_1+v_2)$ and $\lambda_1(\mathbf{u}):=u_1u_2$. Then as in [FK07, §5, §6], we have

$$2^{\mathrm{rk}_4(\mathcal{C}_D)} = \frac{1}{2^{1+\omega(D)}} \sum_{D=D_{00}D_{01}D_{10}D_{11}} \Bigg(\prod_{\mathbf{u}\in\mathbb{F}_2^2}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_1(\mathbf{u})}\Bigg)^{1+\deg D} \prod_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^4}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_1(\mathbf{u},\mathbf{v})}. \tag{5.1}$$

Here all $D_{\mathbf{u}}$ are in $\mathbb{A}^{+,o}$.

To solve the h-fold equation

$$D=\prod_{\mathbf{u}^{(1)}\in\mathbb{F}_2^2} D^{(1)}_{\mathbf{u}^{(1)}} = \cdots = \prod_{\mathbf{u}^{(h)}\in\mathbb{F}_2^2} D^{(h)}_{\mathbf{u}^{(h)}}, \tag{5.2}$$

we let

$$D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}} := \gcd(D^{(1)}_{\mathbf{u}^{(1)}},\dots,D^{(h)}_{\mathbf{u}^{(h)}}).$$

Then this parametrizes the solutions of (5.2) as

$$D^{(i)}_{\mathbf{u}^{(i)}} = \prod_{\substack{1\le j\le h\\ j\ne i}} \prod_{\mathbf{u}^{(j)}\in\mathbb{F}_2^2} D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(i)},\dots,\mathbf{u}^{(h)}}$$

with $\prod_{1\le j\le h}\prod_{\mathbf{u}^{(j)}\in\mathbb{F}_2^2} D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}} = D$. Raising (5.1) to the hth power with these changes of variables, we get

$$\begin{aligned} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)} &= \frac{1}{2^{h(1+\omega(D))}} \\ &\times \sum_{D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}}} \Bigg\{\prod_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}}\Big(\frac{-1}{D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}}}\Big)^{\lambda_1(\mathbf{u}^{(1)})+\cdots+\lambda_1(\mathbf{u}^{(h)})}\Bigg\}^{1+\deg D} \\ &\times \prod_{\substack{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}\\ \mathbf{v}^{(1)},\dots,\mathbf{v}^{(h)}}} \Big(\frac{D_{\mathbf{u}^{(1)},\dots,\mathbf{u}^{(h)}}}{D_{\mathbf{v}^{(1)},\dots,\mathbf{v}^{(h)}}}\Big)^{\Phi_1(\mathbf{u}^{(1)},\mathbf{v}^{(1)})+\cdots+\Phi_1(\mathbf{u}^{(h)},\mathbf{v}^{(h)})}. \end{aligned} \tag{5.3}$$

Summing (5.3) over all $D\in\mathbb{A}_n^{+,o}$, we get

$$S(n,h) = 2^{-h}\sum_{(D_{\mathbf{u}})\in\mathfrak{D}(n,h)} \Big(\prod_{\mathbf{u}} 2^{-h\omega(D_{\mathbf{u}})}\Big)\Bigg(\prod_{\mathbf{u}}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_h(\mathbf{u})}\Bigg)^{1+n}\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_h(\mathbf{u},\mathbf{v})}, \tag{5.4}$$

where $\mathfrak{D}(n,h)$ is the set of 4^h-tuples $(D_{\mathbf{u}})$ of coprime square-free monic polynomials with $\mathbf{u} = (\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(h)}) \in \mathbb{F}_2^{2h}$ satisfying $\sum \deg D_{\mathbf{u}} = n$, and where

$$\lambda_h(\mathbf{u}) := \lambda_1(\mathbf{u}^{(1)}) + \cdots + \lambda_1(\mathbf{u}^{(h)}),$$
$$\Phi_h(\mathbf{u},\mathbf{v}) := \Phi_1(\mathbf{u}^{(1)},\mathbf{v}^{(1)}) + \cdots + \Phi_1(\mathbf{u}^{(h)},\mathbf{v}^{(h)}).$$

For any positive integers m and ℓ, let $p(m,\ell)$ denote the number of all square-free monic polynomials of degree m with ℓ irreducible factors. Then it is known (cf. [BJ, §1]) that

$$p(m,\ell) = \frac{q^m(\log m)^{\ell-1}}{(\ell-1)!m} + O\bigg(\frac{q^m(\log m)^{\ell-2}}{m}\bigg).$$

It is not hard to show that there exists a constant b_0 such that for any positive integers m and ℓ, we have

$$p(m,\ell) \le b_0 \frac{q^m}{m} \frac{(\log m + b_0)^\ell}{\ell!}. \tag{5.5}$$

Let

$$\Omega := e4^h(\log n + b_0).$$

Let $\tau_h(N)$ be the number of ways of writing the monic polynomial N as a product of h monic polynomials. Note that $\tau_h(N) = h^{\omega(N)}$ for $N \in \mathbb{A}^{+,o}$. Let

$$\Sigma_1 := 2^{-h} \sum_{(D_{\mathbf{u}}) \in \mathfrak{D}_1(n,h)} \Big(\prod_{\mathbf{u}} 2^{-h\omega(D_{\mathbf{u}})}\Big)\Big(\prod_{\mathbf{u}} \Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_h(\mathbf{u})}\Big)^{1+n} \prod_{\mathbf{u},\mathbf{v}} \Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_h(\mathbf{u},\mathbf{v})},$$

where $\mathfrak{D}_1(n,h)$ is the subset of $\mathfrak{D}(n,h)$ consisting of those $(D_{\mathbf{u}})$ such that $\omega(D_{\mathbf{u}}) > \Omega$ for some $\mathbf{u} \in \mathbb{F}_2^{2h}$. Write $N = \prod_{\mathbf{u}} D_{\mathbf{u}}$. Then we have

$$\Sigma_1 \ll \sum_{\substack{N \in \mathbb{A}_n^{+,o} \\ \Omega \le \omega(N)}} \tau_{4^h}(N) 2^{-h\omega(N)} = \sum_{\substack{N \in \mathbb{A}_n^{+,o} \\ \Omega \le \omega(N)}} 2^{h\omega(N)}.$$

Using (5.5) and Stirling's formula, we get

$$\Sigma_1 \ll \frac{q^n}{n} \sum_{\Omega \le \ell} \bigg(\frac{2^h(\log n + b_0)}{\ell/e}\bigg)^\ell.$$

Thus, from the choice of Ω, we get

$$\Sigma_1 \ll q^n/n, \tag{5.6}$$

for every $h \ge 1$.

Let $\mathbf{a}=(a_{\mathbf{u}})_{\mathbf{u}\in\mathbb{F}_2^{2h}}$ with $a_{\mathbf{u}}$ nonnegative integers and $\sum_{\mathbf{u}\in\mathbb{F}_2^{2h}} a_{\mathbf{u}}=n$, and $\mathbf{A}$ be the set of all such $\mathbf{a}$'s. For $\mathbf{a}\in\mathbf{A}$, let

$$S(n,h,\mathbf{a}) := 2^{-h}\sum_{(D_{\mathbf{u}})\in\mathfrak{D}(n,h,\mathbf{a})}\Big(\prod_{\mathbf{u}}2^{-h\omega(D_{\mathbf{u}})}\Big) \times\Big(\prod_{\mathbf{u}}\Big(\frac{-1}{D_{\mathbf{u}}}\Big)^{\lambda_h(\mathbf{u})}\Big)^{1+n}\prod_{\mathbf{u},\mathbf{v}}\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_h(\mathbf{u},\mathbf{v})},$$

where $\mathfrak{D}(n,h,\mathbf{a})$ is the subset of $\mathfrak{D}(n,h)$ consisting of $(D_{\mathbf{u}})$ such that $\deg D_{\mathbf{u}}=a_{\mathbf{u}}$ and $\omega(D_{\mathbf{u}})\le\Omega$. Then, by (5.6), we have

$$S(n,h)=\sum_{\mathbf{a}\in\mathbf{A}}S(n,h,\mathbf{a})+O\Big(\frac{q^n}{n}\Big). \tag{5.7}$$

Now we define three families of $\mathbf{a}$'s whose contributions to the right hand side of (5.7) are negligible. We introduce two numbers

$$n^*:=4(1+4^h)\log_q n \quad\text{and}\quad n^{**}:=n^{\eta(h)},$$

where $\eta(h)$ will be defined later. The first family $\mathbf{A}_1$ is the subset of $\mathbf{A}$ consisting of $(a_{\mathbf{u}})$ satisfying the condition:

(5.8) at most 2^h-1 of the $a_{\mathbf{u}}$'s are larger than n^{**}.

Lemma 5.3. *For any positive real γ,*

$$\sum_{N\in\mathbb{A}_n^{+,o}}\gamma^{\omega(N)}\ll q^n n^{\gamma-1}.$$

Proof. The left hand side is

$$\sum_{h=1}^{n}p(n,h)\gamma^h\ll\sum_{h=1}^{\infty}\frac{q^n}{n}\,\frac{(\gamma\log n)^h}{h!}=\frac{q^n}{n}\exp(\gamma\log n)=q^n n^{\gamma-1}.\ \blacksquare$$

Proposition 5.4. *We have*

$$\sum_{\mathbf{a}\in\mathbf{A}_1}|S(n,h,\mathbf{a})|\ll q^n n^{8^h\eta(h)-2^{-h}}. \tag{5.9}$$

Proof. First note that

$$\sum_{\mathbf{a}\in\mathbf{A}_1}|S(n,h,\mathbf{a})| \le\sum_{0\le r\le 2^h-1}\ \sum_{m\le(n^{**})^{4^h-r}}\ \sum_{M\in\mathbb{A}_m^{+,o}}\tau_{4^h-r}(M)2^{-h\omega(M)}\sum_{N\in\mathbb{A}_{n-m}^{+,o}}\tau_r(N)2^{-h\omega(N)}.$$

Now by Lemma 5.3,

$$\sum_{N\in\mathbb{A}_{n-m}^{+,o}}\tau_r(N)2^{-h\omega(N)}=\sum_{N\in\mathbb{A}_{n-m}^{+,o}}(r2^{-h})^{\omega(N)}\ll q^{n-m}n^{r2^{-h}-1}. \tag{5.10}$$

Thus

$$\begin{aligned}\sum_{\mathbf{a}\in\mathbf{A}_1}|S(n,h,\mathbf{a})| &\ll \sum_{0\le r\le 2^h-1}\sum_{m\le(n^{**})^{4^h-r}}\sum_{M\in\mathbb{A}_m^{+,o}} 2^{h\omega(M)}q^{n-m}n^{r2^{-h}-1}\\ &\ll q^n\sum_{0\le r\le 2^h-1} n^{r2^{-h}-1}\sum_{m\le(n^{**})^{4^h}}\frac{1}{q^m}\sum_{M\in\mathbb{A}_m^{+,o}}2^{h\omega(M)}\\ &\ll q^n\sum_{0\le r\le 2^h-1} n^{r2^{-h}-1}\sum_{m\le(n^{**})^{4^h}} m^{2^h-1}.\end{aligned}$$

Since

$$\sum_{0\le r\le 2^h-1} n^{r2^{-h}-1}\ll n^{-2^{-h}} \quad\text{and}\quad \sum_{m\le(n^{**})^{4^h}} m^{2^h-1}\ll (n^{**})^{8^h},$$

we have

$$\sum_{\mathbf{a}\in\mathbf{A}_1}|S(n,h,\mathbf{a})|\ll q^n n^{8^h\eta(h)-2^{-h}}. \ \blacksquare$$

Taking $\eta(h)=8^{-h}\epsilon$ for a small positive real ϵ, we see that the sum over $\mathbf{A}_1$ is negligible.

We say that $D_{\mathbf{u}}$ and $D_{\mathbf{v}}$ (or $\mathbf{u}$ and $\mathbf{v}$) are *linked* if

$$\Phi_h(\mathbf{u},\mathbf{v})+\Phi_h(\mathbf{v},\mathbf{u})=1.$$

The second family $\mathbf{A}_2$ is the subset of $\mathbf{A}$ consisting of $(a_{\mathbf{u}})$'s such that $a_{\mathbf{u}},a_{\mathbf{v}}\ge n^*$ for some linked indices $\mathbf{u}$ and $\mathbf{v}$. Following the idea of [FK07, p. 476] with Proposition 3.6, we can show that, for $\mathbf{a}\in\mathbf{A}_2$,

$$|S(n,h,\mathbf{a})|\ll q^{n-n^*/4}.$$

Since there are $O(n^{4^h})$ possible $\mathbf{a}$'s, we have

$$\sum_{\mathbf{a}\in\mathbf{A}_2}|S(n,h,\mathbf{a})|\ll q^n/n. \tag{5.11}$$

The third family $\mathbf{A}_3$ is the subset of $\mathbf{A}$ consisting of $(a_{\mathbf{u}})\notin\mathbf{A}_2$ such that $1\le a_{\mathbf{v}}<n^*$ and $n^{**}\le a_{\mathbf{u}}$ for some linked indices $\mathbf{u}$ and $\mathbf{v}$. Let $\mathbf{a}\in\mathbf{A}_3$. Then as in [FK07, §5.3] one can show that

$$|S(n,h,\mathbf{a})|\ll \sum_{(D_{\mathbf{w}})_{\mathbf{w}\ne\mathbf{u},\mathbf{v}}}\sum_{D_{\mathbf{v}}}\sum_{1\le\ell\le\Omega}\frac{1}{2^{h\ell}}\Big|\sum_{\omega(D_{\mathbf{u}})=\ell}\mu^2\Big(\prod_{\mathbf{w}}D_{\mathbf{w}}\Big)\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)\Big|.$$

The inner sum satisfies, writing $D_{\mathbf{u}}=P_1\cdots P_\ell$ with $\deg P_i\le\deg P_{i+1}$,

$$\begin{aligned}\Big|\sum_{\omega(D_{\mathbf{u}})=\ell}\mu^2\Big(\prod_{\mathbf{w}}D_{\mathbf{w}}\Big)\Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)\Big| &\le \sum_{P_1,\cdots,P_{\ell-1}}\Big|\sum_{P_\ell}\mu^2\Big(P_1\cdots P_\ell\prod_{\mathbf{w}\ne\mathbf{u}}D_{\mathbf{w}}\Big)\Big(\frac{P_\ell}{D_{\mathbf{v}}}\Big)\Big|\\ &\ll_c q^{a_{\mathbf{u}}-\frac{1}{3}\deg P_\ell}(n^{**})^{-c}\ll_c q^{a_{\mathbf{u}}-\frac{n^{**}}{3\ell}}n^{-c\eta(h)},\end{aligned}$$

for any positive real number c (by Corollary 3.8). Hence

$$|S(n,h,\mathbf{a})| \ll q^n n^{-c\eta(h)}. \tag{5.12}$$

Summing over $\mathbf{a} \in \mathbf{A}_3$ in (5.12), we get

$$\sum_{\mathbf{a}\in\mathbf{A}_3} |S(n,h,\mathbf{a})| \ll q^n n^{4^h - c\eta(h)} \ll q^n/n, \tag{5.13}$$

by taking c large.

Let $\mathbf{A}_4 := \mathbf{A} \setminus (\mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3)$. Then it can be deduced from (5.7), (5.9), (5.12) and (5.13) that

$$S(n,h) = \sum_{\mathbf{a}\in\mathbf{A}_4} S(n,h,\mathbf{a}) + O(q^n n^{8^h\eta(h)-2^{-h}}). \tag{5.14}$$

The family $\mathbf{A}_4$ is characterized by the following conditions (cf. [FK07, Propositions 2 and 3]); for any $\mathbf{a} \in \mathbf{A}_4$,

- $\mathcal{U} = \{\mathbf{u} : a_{\mathbf{u}} > n^{**}\}$ *is a maximal subset of unlinked indices,*
- $a_{\mathbf{u}} = 0$ *for* $\mathbf{u} \notin \mathcal{U}$.

Let $\mathcal{U}$ be any subset of 2^h unlinked indices in $\mathbb{F}_2^{2h}$, that is, $\mathcal{U}$ is a maximal subset of unlinked indices (cf. [FK07, Lemma 18]). An element $\mathbf{a} \in \mathbf{A}$ is said to be *admissible* for $\mathcal{U}$, written $\mathbf{a} \in \mathbf{A}(\mathcal{U})$, if

(i) $a_{\mathbf{u}} > n^{**}$ if and only if $\mathbf{u} \in \mathcal{U}$,
(ii) $a_{\mathbf{u}} = 0$ if and only if $\mathbf{u} \notin \mathcal{U}$.

For $\mathbf{a} \in \mathbf{A}(\mathcal{U})$, since we assumed $q \equiv 3 \bmod 4$ and by the quadratic reciprocity law, we have

$$S(n,h,\mathbf{a}) = 2^{-h} \sum_{(D_{\mathbf{u}})\in\mathfrak{D}(n,h,\mathbf{a})} \Big(\prod_{\mathbf{u}\in\mathcal{U}} 2^{-h\omega(D_{\mathbf{u}})}\Big) \times \Big(\prod_{\mathbf{u}\in\mathcal{U}} (-1)^{a_{\mathbf{u}}\lambda_h(\mathbf{u})}\Big)^{1+n} \prod_{\mathbf{u},\mathbf{v}\in\mathcal{U}} (-1)^{a_{\mathbf{u}}a_{\mathbf{v}}\Phi_h(\mathbf{u},\mathbf{v})}.$$

Since $\mathbf{A}_4$ is the disjoint union of the $\mathbf{A}(\mathcal{U})$'s, where $\mathcal{U}$ runs over all maximal subsets of unlinked indices, we have

$$\sum_{\mathbf{a}\in\mathbf{A}_4} S(n,h,\mathbf{a}) = \sum_{\mathcal{U}} \sum_{\mathbf{a}\in\mathbf{A}(\mathcal{U})} S(n,h,\mathbf{a}).$$

Let $\mathbf{H}(\mathcal{U})$ be the set of all $\mathbf{h} = (h_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}$ with $h_{\mathbf{u}} \in \{0,1\}$ and $\sum_{u\in\mathcal{U}} h_{\mathbf{u}} \equiv n \bmod 2$. For $\mathbf{h} \in \mathbf{H}(\mathcal{U})$ we write $\mathbf{a} \sim_{\mathcal{U}} \mathbf{h}$ if $\mathbf{a} \in \mathbf{A}(\mathcal{U})$ and $a_{\mathbf{u}} \equiv h_{\mathbf{u}} \bmod 2$ for all $\mathbf{u} \in \mathcal{U}$. Then

$$\sum_{\mathbf{a}\in\mathbf{A}(\mathcal{U})} S(n,h,\mathbf{a}) = \sum_{\mathbf{h}\in\mathbf{H}(\mathcal{U})} S(n,\mathcal{U},\mathbf{h}),$$

where

$$S(n,\mathcal{U},\mathbf{h}) = \sum_{\mathbf{a}\sim_{\mathcal{U}}\mathbf{h}} S(n,h,\mathbf{a}).$$

Let $\mathfrak{D}(n,\mathcal{U},\mathbf{h})$ be the set of 2^h-tuples $(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}$ of coprime square-free monic polynomials such that $\sum_{\mathbf{u}\in\mathcal{U}} \deg D_{\mathbf{u}} = n$ and $\deg D_{\mathbf{u}} \equiv h_{\mathbf{u}} \bmod 2$, $\omega(D_{\mathbf{u}}) \le \Omega$ for all $\mathbf{u}\in\mathcal{U}$. Then

$$S(n,\mathcal{U},\mathbf{h}) = 2^{-h}\beta(\mathbf{h}) \sum_{(D_{\mathbf{u}})\in\mathfrak{D}(n,\mathcal{U},\mathbf{h})} \prod_{\mathbf{u}\in\mathcal{U}} 2^{-h\omega(D_{\mathbf{u}})},$$

where

$$\beta(\mathbf{h}) = \Big(\prod_{\mathbf{u}\in\mathcal{U}} (-1)^{h_{\mathbf{u}}\lambda_h(\mathbf{u})}\Big)^{1+n} \prod_{\mathbf{u},\mathbf{v}\in\mathcal{U}} (-1)^{h_{\mathbf{u}}h_{\mathbf{v}}\Phi_h(\mathbf{u},\mathbf{v})}.$$

LEMMA 5.5. *Let m be a positive integer and $h_1,h_2 \in \{0,1\}$ with $h_1+h_2 \equiv m \bmod 2$. Then, for any $A\in\mathbb{A}$,*

$$\sum_{\substack{\deg D_i\equiv h_i \bmod 2\\ \deg D_1+\deg D_2=m\\ \omega(D_1D_2)=\ell}} \mu^2(AD_1D_2)2^{-h\ell} = \frac{1}{2} \sum_{\substack{\deg D_1+\deg D_2=m\\ \omega(D_1D_2)=\ell}} \mu^2(AD_1D_2)2^{-h\ell} + O\Big(\frac{q^m}{m}\frac{(\log m/2^h)^{\ell-1}}{(\ell-1)!}\Big) + O\Big(\frac{q^m(\log m/2^h)^{\ell-2}}{(\ell-2)!m}\Big),$$

where the sums are over monic polynomials.

Proof. Assume first that $A=1$. When m is odd, the result follows without error term by just changing the order. Now assume that m is even. Let $p_2(m,\ell)$ be the number of all monic square-free polynomials of degree m with ℓ irreducible factors all of whose degrees are even. It is known that

$$p_2(m,\ell) = \frac{q^m(\log m)^{\ell-1}}{(\ell-1)!2^{\ell-1}m} + O\Big(\frac{q^m(\log m)^{\ell-2}}{m}\Big).$$

Then, for $h_1=h_2=1$,

$$\sum_{\substack{\deg D_i\equiv h_i \bmod 2\\ \deg D_1+\deg D_2=m\\ \omega(D_1D_2)=\ell}} \mu^2(D_1D_2) = (p(m,\ell)-p_2(m,\ell))2^{\ell-1},$$

and for $h_1=h_2=0$,

$$\sum_{\substack{\deg D_i\equiv h_i \bmod 2\\ \deg D_1+\deg D_2=m\\ \omega(D_1D_2)=\ell}} \mu^2(D_1D_2) = (p(m,\ell)-p_2(m,\ell))2^{\ell-1} + p_2(m,\ell)2^{\ell}.$$

Now since

$$\sum_{\substack{\deg D_1+\deg D_2=m\\ \omega(D_1D_2)=\ell}} \mu^2(D_1D_2) = p(m,\ell)2^\ell,$$

we get the result when $A=1$.

When $\deg A \geq 1$, it is clear that the number of square-free monic polynomials of degree m with ℓ irreducible factors, which are not relatively prime to A, is

$$O(p(m-1,\ell-1)) = O\Big(\frac{q^{m-1}(\log(m-1))^{\ell-2}}{(\ell-2)!(m-1)}\Big).$$

Thus the result follows in this case too. ∎

Corollary 5.6. *Let m be a positive integer and $h_1, h_2 \in \{0,1\}$ with $h_1+h_2 \equiv m \bmod 2$. Then, for any $A \in \mathbb{A}$,*

$$\sum_{\substack{\deg D_i \equiv h_i \bmod 2\\ \deg D_1+\deg D_2=m}} \mu^2(AD_1D_2)2^{-h\omega(D_1D_2)}$$
$$= \frac{1}{2}\sum_{\deg D_1+\deg D_2=m} \mu^2(AD_1D_2)2^{-h\ell} + O\Big(\frac{q^m}{m^{1-2^{-h}}}\Big),$$

where the sums are over monic polynomials.

Proof. The result follows from Lemma 5.5 by summing over ℓ and the fact that

$$\sum_{\ell=1}^{\infty} \frac{(2^{-h}\log m)^{\ell-1}}{(\ell-1)!} = m^{2^{-h}} + O(1). \ ∎$$

Lemma 5.7. *For $0<\alpha<1$,*

$$\sum_{d\leq n} \frac{1}{d^\alpha (n-d)^\alpha} \ll n^{1-2\alpha}.$$

Proof. This follows from the inequality

$$\Big(\frac{1}{d}+\frac{1}{n-d}\Big)^\alpha \leq \Big(\frac{1}{d}\Big)^\alpha + \Big(\frac{1}{n-d}\Big)^\alpha \quad \text{for } 0<\alpha<1. \ ∎$$

Proposition 5.8. *For any $\mathbf{h} \in \mathbf{H}(\mathcal{U})$ we have, for $h=1$,*

$$S(n,\mathcal{U},\mathbf{h}) = \frac{\beta(\mathbf{h})}{2^{2^h-1+h}} \sum_{\substack{(D_\mathbf{u})_{\mathbf{u}\in\mathcal{U}}\\ \sum \deg D_\mathbf{u}=n}} \mu^2\Big(\prod_{\mathbf{u}} D_\mathbf{u}\Big)\prod_{\mathbf{u}} 2^{-h\omega(D_\mathbf{u})} + O\Big(\frac{q^n}{n^{1-2^{-h}}}\Big),$$

and, for $h>1$,

$$S(n,\mathcal{U},\mathbf{h}) = \frac{\beta(\mathbf{h})}{2^{2^h-1+h}} \sum_{\substack{(D_\mathbf{u})_{\mathbf{u}\in\mathcal{U}}\\ \sum \deg D_\mathbf{u}=n}} \mu^2\Big(\prod_{\mathbf{u}} D_\mathbf{u}\Big)\prod_{\mathbf{u}} 2^{-h\omega(D_\mathbf{u})} + O\Big(\frac{q^n}{n^{1-2^{1-h}}}\Big).$$

Proof. We only prove the case when n is odd. The case when n is even is very similar and we leave it to the reader. For $h = 1$, the result follows from Corollary 5.6, since n is odd. Now assume that $h > 1$. By similar computations to those leading to (5.6), we can write

$$S(n,\mathcal{U},\mathbf{h}) = 2^{-h}\beta(\mathbf{h}) \sum_{\substack{(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}\\ \sum \deg D_{\mathbf{u}}=n\\ \deg D_{\mathbf{u}}\equiv h_{\mathbf{u}} \bmod 2}} \mu^2\Big(\prod_{\mathbf{u}\in\mathcal{U}} D_{\mathbf{u}}\Big) \prod_{\mathbf{u}\in\mathcal{U}} 2^{-h\omega(D_{\mathbf{u}})} + O\Big(\frac{q^n}{n}\Big).$$

Write $\mathcal{U} = \{1, 2, \dots, 2^h\}$ for simplicity. Write $D_i' = D_{i+1}\cdots D_{2^h}$, $d_i = \deg D_i$ and $d_i' = \deg D_i'$ to simplify the notation. By Lemma 5.5, we have

$$\begin{aligned}
&\sum_{\substack{D_1,D_1'\\ d_1+d_1'=n}} \mu^2(D_1D_1')2^{-h\omega(D_1)-h\omega(D_1')}\\
&= 2\sum_{D_1,d_1\equiv h_1 \bmod 2}\ \sum_{D_1',d_1'=n-d_1} \mu^2(D_1D_1')2^{-h\omega(D_1)-h\omega(D_1')}\\
&= 4\sum_{D_1,d_1\equiv h_1 \bmod 2}\ \sum_{D_2,d_2\equiv h_2 \bmod 2}\ \sum_{D_2',d_2'=n-d_1-d_2} \mu^2(D_1D_2D_2')2^{-h\omega(D_1)-h\omega(D_2)-h\omega(D_2')}\\
&\quad + \sum_{D_1} 2^{-h\omega(D_1)} O\Big(\frac{q^{n-d_1}}{(n-d_1)^{1-2^{-h}}}\Big).
\end{aligned}$$

Now

$$\begin{aligned}
\sum_{D_1} 2^{-h\omega(D_1)} O\Big(\frac{q^{n-d_1}}{(n-d_1)^{1-2^{-h}}}\Big) &= \sum_{d_1}\sum_{\ell} p(d_1,\ell)2^{-h\omega(D_1)} O\Big(\frac{q^{n-d_1}}{(n-d_1)^{1-2^{-h}}}\Big)\\
&= \sum_{d_1} \frac{q^{d_1}}{d_1^{1-2^{-h}}} + O\Big(\frac{q^{n-d_1}}{(n-d_1)^{1-2^{-h}}}\Big) = O\Big(\frac{q^n}{n^{1-2^{1-h}}}\Big).
\end{aligned}$$

Continuing this process, we get the result. ∎

Now

$$\begin{aligned}
&\sum_{\substack{(D_{\mathbf{u}})_{\mathbf{u}\in\mathcal{U}}\\ \sum \deg D_{\mathbf{u}}=n}} \mu^2\Big(\prod_{\mathbf{u}} D_{\mathbf{u}}\Big)\prod_{\mathbf{u}} 2^{-h\omega(D_{\mathbf{u}})}\\
&\qquad = \sum_{N\in\mathbb{A}_n^+} \mu^2(N)\tau_{2^h}(N)2^{-h\omega(N)} + O\Big(\frac{q^n}{n}\Big)\\
&\qquad\quad + O\Big(\sum_{d\le n^{**}}\ \sum_{\deg D=d} 2^{-h\omega(D)} \sum_{\deg M=n-d} 2^{-h\omega(M)}(2^h-1)^{\omega(M)}\Big)\\
&\qquad = \sum_{N\in\mathbb{A}_n^+} \mu^2(N) + O\Big(\frac{q^n}{n}\Big) + O\Big(\sum_{d\le n^{**}} \frac{q^d}{d^{1-2^{-h}}}\,\frac{q^{n-d}}{(n-d)^{2^{-h}}}\Big)
\end{aligned}$$

$$= \sum_{N\in\mathbb{A}_n^+} \mu^2(N) + O\bigg(\frac{q^n}{n}\bigg) + O\bigg(\sum_{d\le n^{**}} q^n \frac{1}{d^{1-2^{-h}}}\,\frac{1}{(n-n^{**})^{2^{-h}}}\bigg)$$

$$= \sum_{N\in\mathbb{A}_n^+} \mu^2(N) + O\bigg(\frac{q^n}{n}\bigg) + O\bigg(q^n\bigg(\frac{n^{**}}{(n-n^{**})}\bigg)^{2^{-h}}\bigg)$$

$$= \sum_{N\in\mathbb{A}_n^+} \mu^2(N) + O\bigg(\frac{q^n}{n^{(1-\eta(h))2^{-h}}}\bigg) = q^n\bigg(1-\frac{1}{q}\bigg) + O\bigg(\frac{q^n}{n^{(1-\eta(h))2^{-h}}}\bigg).$$

Hence

$$S(n,\mathcal{U},\mathbf{h}) = 2^{1-h-2^h}\beta(\mathbf{h})q^n\bigg(1-\frac{1}{q}\bigg) + O\bigg(\frac{q^n}{n^{(1-\eta(h))2^{-h}}}\bigg). \tag{5.15}$$

Summing over $\mathbf{h}\in\mathbf{H}(\mathcal{U})$ in (5.15), we get

$$\sum_{\mathbf{a}\in\mathbf{A}(\mathcal{U})} S(n,h,\mathbf{a}) = 2^{1-h-2^h}\gamma(\mathcal{U})q^n\bigg(1-\frac{1}{q}\bigg) + O\bigg(\frac{q^n}{n^{(1-\eta(h))2^{-h}}}\bigg), \tag{5.16}$$

where

$$\gamma(\mathcal{U}) = \sum_{(h_{\mathbf{u}})\in\mathbf{H}(\mathcal{U})} \Big(\prod_{\mathbf{u}\in\mathcal{U}} (-1)^{h_{\mathbf{u}}\lambda_h(\mathbf{u})}\Big)^{1+n} \prod_{\mathbf{u},\mathbf{v}\in\mathcal{U}} (-1)^{h_{\mathbf{u}}h_{\mathbf{v}}\Phi_h(\mathbf{u},\mathbf{v})}.$$

Now we sum over all the maximal subsets $\mathcal{U}$ of unlinked indices in (5.16) and choose $\eta(h) = 8^{-h}\epsilon$ to obtain

Proposition 5.9. *For every integer $h\ge 1$ and every positive real ϵ,*

$$S(n,h) = q^n\bigg(1-\frac{1}{q}\bigg)2^{1-h-2^h}\bigg(\sum_{\mathcal{U}}\gamma(\mathcal{U})\bigg) + O(q^n n^{-2^{-h}+\epsilon}),$$

where the sum is over all the maximal subsets $\mathcal{U}$ of unlinked indices.

If $q\equiv 3 \bmod 4$, the argument of [FK07, §5.6, §6.1] works in our case too:

$$2^{1-h-2^h}\sum_{\mathcal{U}}\gamma(\mathcal{U}) = \begin{cases} \mathcal{N}(h,2) & \text{if } n \text{ is odd,}\\ 2^{-h}(\mathcal{N}(h+1,2)-\mathcal{N}(h,2)) & \text{if } n \text{ is even,}\end{cases}$$

where $\mathcal{N}(h,2)$ is the number of subspaces of $\mathbb{F}_2^h$.

Finally,

$$S(n,h) = \begin{cases} \mathcal{N}(h,2)q^n(1-1/q) + O(q^n n^{-2^{-h}+\epsilon}) & \text{if } n \text{ is odd,}\\ 2^{-h}(\mathcal{N}(h+1,2)-\mathcal{N}(h,2))q^n(1-1/q) + O(q^n n^{-2^{-h}+\epsilon}) & \\ & \text{if } n \text{ is even,}\end{cases}$$

with finishes the proof of Theorem 1.1.

6. Proof of Theorem 1.6. In this section we also assume that $q \equiv 3 \bmod 4$. We are going to study the sums

$$S^*(n,h) := \sum_{D\in\mathcal{D}\cap\mathbb{A}_n^{+,o}} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)},$$
$$S^*_{\mathrm{mix}}(n,h) := \sum_{D\in\mathcal{D}\cap\mathbb{A}_n^{+,o}} 2^{h\,\mathrm{rk}_4(\mathcal{C}_D)}\cdot 2^{\mathrm{rk}_4(\mathcal{C}l_D)}$$

for a positive integer h and for positive even integes $n \to +\infty$.

6.1. For $r,s \in \mathcal{Q} := \{0,1,2,3\}$, we define $\kappa_1(r,s)$ to be 1 if $s = r+2$ and 0 otherwise. For $D \in \mathcal{D}$, from Lemma 5.2 and by using the quadratic reciprocity law, we get

$$2^{\mathrm{rk}_4(\mathcal{C}_D)} = \frac{1}{2^{1+\omega(D)}} \sum_{D=D_0D_1D_2D_3} \prod_{r,s\in\mathcal{Q}} \left(\frac{D_r}{D_s}\right)^{\kappa_1(r,s)}, \tag{6.1}$$

where $D_i \in \mathcal{D}\cup\{1\}$ for $0 \le i \le 3$. Then as in §5, we have

$$2^{h\,\mathrm{rk}_4(\mathcal{C}_D)} = \frac{1}{2^{h(1+\omega(D))}} \sum_{(D_{\mathbf{r}})} \prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_h(\mathbf{r},\mathbf{s})}, \tag{6.2}$$

where $\mathbf{r} = (r_1,\dots,r_h), \mathbf{s} = (s_1,\dots,s_h) \in \mathcal{Q}^h$, $\kappa_h(\mathbf{r},\mathbf{s}) = \kappa_1(r_1,s_1) + \cdots + \kappa_1(r_h,s_h)$ and the sum is over all the 4^h-tuples $(D_{\mathbf{r}})$ of coprime square-free monic polynomials such that $\prod_{\mathbf{r}} D_{\mathbf{r}} = D$. Summing (6.2) over all $D \in \mathcal{D}\cap\mathbb{A}_n^{+,o}$, we get

$$S^*(n,h) = 2^{-h} \sum_{(D_{\mathbf{r}})\in\mathfrak{D}^*(n,h)} \Big(\prod_{\mathbf{r}} 2^{-h\omega(D_{\mathbf{r}})}\Big) \prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_h(\mathbf{r},\mathbf{s})}, \tag{6.3}$$

where $\mathfrak{D}^*(n,h)$ is the set of all the 4^h-tuples $(D_{\mathbf{r}})$ of square-free monic and coprime polynomials such that $D_{\mathbf{r}} \in \mathcal{D}\cup\{1\}$ and $\sum_{\mathbf{r}} \deg D_{\mathbf{r}} = n$. Let $\mathfrak{D}_1^*(n,h)$ be the subset of $\mathfrak{D}^*(n,h)$ consisting of all $(D_{\mathbf{r}})$ such that $\omega(D_{\mathbf{r}}) > \Omega$ for some $\mathbf{r} \in \mathcal{Q}^h$, and

$$\Sigma_1^* := 2^{-h} \sum_{(D_{\mathbf{r}})\in\mathfrak{D}_1^*(n,h)} \Big(\prod_{\mathbf{r}} 2^{-h\omega(D_{\mathbf{r}})}\Big) \prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_h(\mathbf{r},\mathbf{s})}.$$

Then, by the same argument used to obtain (5.6), we get

$$\Sigma_1^* \ll q^n/n. \tag{6.4}$$

We say that $D_{\mathbf{r}}$ and $D_{\mathbf{s}}$ (or $\mathbf{r}$ and $\mathbf{s}$) are *linked* if $\kappa_h(\mathbf{r},\mathbf{s}) + \kappa_h(\mathbf{s},\mathbf{r}) \equiv 1 \bmod 2$. We identify $\mathcal{Q}$ with $\mathbb{F}_2^2$, as in §5. Then $\mathcal{Q}^h$ can be identified with $\mathbb{F}_2^{2h}$, and unlinked indices in $\mathcal{Q}^h$ are just unlinked indices in $\mathbb{F}_2^{2h}$ as in §5 (cf. [FK10, §7.6]). With this identification, $\mathbf{A}$ denotes the set of all

4^h-tuples $(a_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^h}$ of nonnegative integers such that $\sum_{\mathbf{r}} a_{\mathbf{r}} = n$. As in §5, for $\mathbf{a} \in \mathbf{A}$, we define

$$S^*(n,h,\mathbf{a}) := 2^{-h} \sum_{(D_{\mathbf{r}})\in\mathfrak{D}^*(n,h,\mathbf{a})} \Big(\prod_{\mathbf{r}} 2^{-h\omega(D_{\mathbf{r}})}\Big) \prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_h(\mathbf{r},\mathbf{s})}, \tag{6.5}$$

where $\mathfrak{D}^*(n,h,\mathbf{a})$ be the subset of $\mathfrak{D}^*(n,h)$ consisting of all $(D_{\mathbf{r}})$ such that $\deg D_{\mathbf{r}} = a_{\mathbf{r}}$ and $\omega(D_{\mathbf{r}}) \le \Omega$ for all $\mathbf{r} \in \mathcal{Q}^h$. Then, by (6.4), we have

$$S^*(n,h) = \sum_{\mathbf{a}\in\mathbf{A}} S^*(n,h,\mathbf{a}) + O(q^n/n). \tag{6.6}$$

Moreover, by similar computations to those proving (5.9), (5.12) and (5.13), we get the inequalities

$$\sum_{\mathbf{a}\in\mathbf{A}_1} |S^*(n,h,\mathbf{a})| \ll q^n n^{8^h\eta(h)-2^{-h-1}}, \tag{6.7}$$

$$\sum_{\mathbf{a}\in\mathbf{A}_2} |S^*(n,h,\mathbf{a})| \ll q^n/n \quad \text{and} \quad \sum_{\mathbf{a}\in\mathbf{A}_3} |S^*(n,h,\mathbf{a})| \ll q^n/n.$$

For (6.7), we use the inequality (which follows from Corollary 4.8)

$$\sum_{N\in\mathcal{D}\cap\mathbb{A}^{+,o}_{n-m}} \tau_r(N)2^{-h\omega(N)} = \sum_{N\in\mathcal{D}\cap\mathbb{A}^{+,o}_{n-m}} (r2^{-h})^{\omega(N)} \ll q^{n-m} n^{r2^{-h-1}-1}$$

instead of (5.10) in the proof of Proposition 5.4. Then we obtain

$$S^*(n,h) = \sum_{\mathbf{a}\in\mathbf{A}_4} S^*(n,h,\mathbf{a}) + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-1}}). \tag{6.8}$$

Let $\mathcal{U}$ be any maximal subset of unlinked indices. Since $\mathbf{A}_4$ is the disjoint union of the $\mathbf{A}(\mathcal{U})$'s, we can write

$$\sum_{\mathbf{a}\in\mathbf{A}_4} S^*(n,h,\mathbf{a}) = \sum_{\mathcal{U}} \sum_{\mathbf{a}\in\mathbf{A}(\mathcal{U})} S^*(n,h,\mathbf{a}). \tag{6.9}$$

By definition and the quadratic reciprocity law, for $\mathbf{a} \in \mathbf{A}(\mathcal{U})$, we have

$$S^*(n,h,\mathbf{a}) = 2^{-h} \sum_{(D_{\mathbf{r}})\in\mathfrak{D}^*(n,h,\mathbf{a})} \Big(\prod_{\mathbf{r}\in\mathcal{U}} 2^{-h\omega(D_{\mathbf{r}})}\Big). \tag{6.10}$$

For $\mathbf{a} \in \mathbf{A}(\mathcal{U})$, let $\mathfrak{D}^*(n,\mathcal{U},\mathbf{a})$ be the set of all the 2^h-tuples $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{U}}$ of coprime square-free monic polynomials such that $D_{\mathbf{r}} \in \mathcal{D}\cup\{1\}$, $\deg D_{\mathbf{r}} = a_{\mathbf{r}}$ and $\omega(D_{\mathbf{r}}) \le \Omega$ for all $\mathbf{r} \in \mathcal{U}$. Then we can rewrite (6.10) as

$$S^*(n,h,\mathbf{a}) = 2^{-h} \sum_{(D_{\mathbf{r}})\in\mathfrak{D}^*(n,\mathcal{U},\mathbf{a})} \Big(\prod_{\mathbf{r}\in\mathcal{U}} 2^{-h\omega(D_{\mathbf{r}})}\Big).$$

Let $\mathfrak{D}^*(n,\mathcal{U})$ be the set of all the 2^h-tuples $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{U}}$ of coprime square-free monic and coprime polynomials such that $D_{\mathbf{r}} \in \mathcal{D}\cup\{1\}$ and $\sum_{\mathbf{r}} \deg D_{\mathbf{r}} = n$,

and let

$$S^*(n,\mathcal{U}) := 2^{-h} \sum_{(D_{\mathbf{r}})\in\mathfrak{D}^*(n,\mathcal{U})} \Big(\prod_{\mathbf{r}\in\mathcal{U}} 2^{-h\omega(D_{\mathbf{r}})}\Big).$$

Write $D=\prod_{\mathbf{r}} D_{\mathbf{r}}$. Then

$$S^*(n,\mathcal{U}) = 2^{-h} \sum_{D\in\mathcal{D}\cap\mathbb{A}_n^{+,o}} \tau_{2^h}(D)2^{-h\omega(D)} = 2^{-h}\cdot\mathcal{D}(n). \tag{6.11}$$

By the same techniques used to obtain (6.4) and (6.7), we also have

$$S^*(n,\mathcal{U}) = \sum_{\mathbf{a}\in\mathbf{A}^*(\mathcal{U})} S^*(n,h,\mathbf{a}) + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-1}}). \tag{6.12}$$

Now (6.8), (6.9), (6.11) and (6.12) yield

Proposition 6.1. *For every integer $h\ge 1$ and every positive real ϵ,*

$$S^*(n,h) = 2^{-h}\cdot\mathcal{D}(n)\Big(\sum_{\mathcal{U}} 1\Big) + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-1}}), \tag{6.13}$$

where the sum is over all the maximal subsets $\mathcal{U}$ of unlinked indices.

By using the fact that (cf. [FK10, Lemmas 41 and 42])

$$\sum_{\mathcal{U}} 1 = 2^h\cdot\prod_{j=1}^{h-1}(2^j+1),$$

we get

$$S^*(n,h) = \prod_{j=1}^{h-1}(2^j+1)\cdot\mathcal{D}(n) + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-1}}), \tag{6.14}$$

which completes the proof of the first part of Theorem 1.6.

6.2. Now we consider the sum $S^*_{\mathrm{mix}}(n,h)$. Let

$$S^\diamond(n,h) := \sum_{D\in\mathcal{D}\cap\mathbb{A}_n^{+,o}} \frac{2^{h\,\mathrm{rk}_4(\mathcal{C}_D)}}{2^{\omega(D)}} \sum_{D=D_0D_1D_2D_3} \left(\frac{\mathfrak{d}_0\bar{\mathfrak{d}}_1}{\mathfrak{d}_2\bar{\mathfrak{d}}_3}\right)_4^2,$$

where $D_i\in\mathcal{D}\cup\{1\}$ and $D_i=\mathfrak{d}_i\bar{\mathfrak{d}}_i$ is a privileged factorization for $0\le i\le 3$. Then it follows from Corollary 2.13 that

$$S^*_{\mathrm{mix}}(n,h) = \tfrac{1}{2}S^*(n,h+1) + \tfrac{1}{4}S^\diamond(n,h). \tag{6.15}$$

The equality (6.2) implies

$$\begin{aligned}\frac{2^{h\,\mathrm{rk}_4(\mathcal{C}_D)}}{2^{\omega(D)}} &\sum_{D=D_0D_1D_2D_3} \left(\frac{\mathfrak{d}_0\bar{\mathfrak{d}}_1}{\mathfrak{d}_2\bar{\mathfrak{d}}_3}\right)_4^2 \\ &= \frac{1}{2^h\cdot 2^{(h+1)\omega(D)}} \sum_{(D_{\mathbf{r}})}\sum_{\mathbf{d}}\prod_{\mathbf{r}}\prod_{\mathbf{s}} \left(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}}\right)^{\kappa_h(\mathbf{r},\mathbf{s})} \left(\frac{\mathfrak{d}_0\bar{\mathfrak{d}}_1}{\mathfrak{d}_2\bar{\mathfrak{d}}_3}\right)_4^2,\end{aligned} \tag{6.16}$$

where the sum is over $(D_{\mathbf{r}})_{\mathbf{r}\in\mathcal{Q}^h}$ and $\mathbf{d}=(D_0,D_1,D_2,D_3)$ such that

$$D=\prod_{\mathbf{r}} D_{\mathbf{r}} = D_0D_1D_2D_3. \tag{6.17}$$

For $i\in\mathcal{Q}$ and $\mathbf{r}\in\mathcal{Q}^h$, let $D_{\mathbf{r},i}:=\gcd(D_{\mathbf{r}},D_i)$. These parametrize the solutions of (6.17) by writing $D_{\mathbf{r}}=\prod_i D_{\mathbf{r},i}$ and $D_i=\prod_{\mathbf{r}} D_{\mathbf{r},i}$ with the conditions

$$\prod_{\mathbf{r}}\prod_{i} D_{\mathbf{r},i}=D.$$

Summing (6.16) over all $D\in\mathcal{D}\cap\mathbb{A}_n^{+,o}$, we get

$$\begin{aligned} S^{\diamond}(n,h) &= 2^{-h}\sum_{(D_{\mathbf{r},i})\in\mathfrak{D}^{\diamond}(n,h)}\Big(\prod_{\mathbf{r},i}2^{-(h+1)\omega(D_{\mathbf{r},i})}\Big)\Big\{\prod_{\mathbf{r},i}\prod_{\mathbf{s},j}\Big(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\Big)^{\kappa_h(\mathbf{r},\mathbf{s})}\Big\}\\ &\quad\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\mathfrak{d}_{\mathbf{r},0}}{\mathfrak{d}_{\mathbf{s},2}}\Big)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\mathfrak{d}_{\mathbf{r},0}}{\overline{\mathfrak{d}}_{\mathbf{s},3}}\Big)_4^2\Big\}\\ &\quad\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\overline{\mathfrak{d}}_{\mathbf{r},1}}{\mathfrak{d}_{\mathbf{s},2}}\Big)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\overline{\mathfrak{d}}_{\mathbf{r},1}}{\overline{\mathfrak{d}}_{\mathbf{s},3}}\Big)_4^2\Big\}, \end{aligned} \tag{6.18}$$

where $\mathfrak{D}^{\diamond}(n,h)$ is the set of 4^{h+1}-tuples $(D_{\mathbf{r},i})$ of coprime square-free monic polynomials such that $D_{\mathbf{r},i}\in\mathcal{D}\cup\{1\}$ and $\sum\deg D_{\mathbf{r},i}=n$, and where $D_{\mathbf{r},i}=\mathfrak{d}_{\mathbf{r},i}\overline{\mathfrak{d}}_{\mathbf{r},i}$ is a privileged factorization.

To bound the number of prime divisors of the summation variables, we replace the constant Ω in §5 by

$$\Omega':=e4^{h+1}(\log n+b_0).$$

Then as in (5.6), the contribution $\Sigma_1^{\diamond}$ of the $(D_{\mathbf{r},i})\in\mathfrak{D}^{\diamond}(n,h)$ such that $\omega(D_{\mathbf{r},i})>\Omega'$ for some $(\mathbf{r},i)$ to the right hand side of (6.18) is $O(q^n/n)$.

Let $\mathbf{A}^{\diamond}$ be the set of all 4^{h+1}-tuples $(a_{\mathbf{r},i})_{(\mathbf{r},i)\in\mathcal{Q}^{h+1}}$ of nonnegative integers such that $\sum_{\mathbf{r},i}a_{\mathbf{r},i}=n$. For $\mathbf{a}\in\mathbf{A}^{\diamond}$, let

$$\begin{aligned} S^{\diamond}(n,h,\mathbf{a}) &:= 2^{-h}\sum_{(D_{\mathbf{r},i})\in\mathfrak{D}^{\diamond}(n,h,\mathbf{a})}\Big(\prod_{\mathbf{r},i}2^{-(h+1)\omega(D_{\mathbf{r},i})}\Big)\Big\{\prod_{\mathbf{r},i}\prod_{\mathbf{s},j}\Big(\frac{D_{\mathbf{r},i}}{D_{\mathbf{s},j}}\Big)^{\kappa_h(\mathbf{r},\mathbf{s})}\Big\}\\ &\quad\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\mathfrak{d}_{\mathbf{r},0}}{\mathfrak{d}_{\mathbf{s},2}}\Big)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\mathfrak{d}_{\mathbf{r},0}}{\overline{\mathfrak{d}}_{\mathbf{s},3}}\Big)_4^2\Big\}\\ &\quad\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\overline{\mathfrak{d}}_{\mathbf{r},1}}{\mathfrak{d}_{\mathbf{s},2}}\Big)_4^2\Big\}\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{\overline{\mathfrak{d}}_{\mathbf{r},1}}{\overline{\mathfrak{d}}_{\mathbf{s},3}}\Big)_4^2\Big\}, \end{aligned} \tag{6.19}$$

where $\mathfrak{D}^\diamond(n,h,\mathbf{a})$ is the subset of $\mathfrak{D}^\diamond(n,h)$ consisting of all $(D_{\mathbf{r},i})$ such that $\deg D_{\mathbf{r},i} = a_{\mathbf{r},i}$ and $\omega(D_{\mathbf{r},i}) \le \Omega'$ for all $(\mathbf{r},i) \in \mathcal{Q}^{h+1}$. Then we have

LEMMA 6.2. *For any integer $h \ge 0$ and any positive ϵ,*

$$S^\diamond(n,h) = \sum_{\mathbf{a}\in\mathbf{A}^\diamond} S^\diamond(n,h,\mathbf{a}) + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-2}}). \tag{6.20}$$

LEMMA 6.3. *We have*

$$\sum_{\mathbf{a}} |S^\diamond(n,h,\mathbf{a})| = O(q^n/n), \tag{6.21}$$

where the sum is over those $\mathbf{a} = (a_{\mathbf{r},i}) \in \mathbf{A}^\diamond$ satisfying

$$\sum_{\mathbf{r}} a_{\mathbf{r},0} + \sum_{\mathbf{r}} a_{\mathbf{r},1} > 0 \quad \textit{and} \quad \sum_{\mathbf{r}} a_{\mathbf{r},2} + \sum_{\mathbf{r}} a_{\mathbf{r},3} > 0.$$

Proof. We can follow the proof of Lemma 46 in [FK10], replacing $(\log X)^{100\cdot 10^k}$ by $4\log_q n$. ∎

By the quartic reciprocity law, Lemmas 6.2, 6.3, and symmetry, we have

$$S^\diamond(n,h) = 2\sum_{\mathbf{a}\in\mathbf{A}_0^\diamond} S^\diamond(n,h,\mathbf{a}) + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-2}}),$$

where $\mathbf{A}_0^\diamond$ is the subset of $\mathbf{A}^\diamond$ consisting of $(a_{\mathbf{r},i})$ such that $a_{\mathbf{r},2} = a_{\mathbf{r},3} = 0$. For $\mathbf{a} \in \mathbf{A}_0^\diamond$, since $D_{\mathbf{r},2} = D_{\mathbf{r},3} = 1$ for all $(D_{\mathbf{r},i}) \in \mathfrak{D}^\diamond(n,h,\mathbf{a})$, we have

$$\begin{aligned} &S^\diamond(n,h,\mathbf{a}) \\ &\quad = 2^{-h}\sum_{D_{\mathbf{r},0}}\sum_{D_{\mathbf{r},1}} \Big(\prod_{\mathbf{r}} 2^{-(h+1)\omega(D_{\mathbf{r},0}D_{\mathbf{r},1})}\Big)\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}D_{\mathbf{r},1}}{D_{\mathbf{s},0}D_{\mathbf{s},1}}\Big)^{\kappa_h(\mathbf{r},\mathbf{s})}\Big\}, \end{aligned}$$

where $D_{\mathbf{r},i} \in \mathcal{D}\cup\{1\}$ are coprime, $\deg D_{\mathbf{r},i} = a_{\mathbf{r},i}$ and $\omega(D_{\mathbf{r},i}) \le \Omega'$ for all $(\mathbf{r},i) \in \mathcal{Q}^h \times \{0,1\}$. Since the error term involved in the condition $\omega(D_{\mathbf{r},i}) > \Omega'$ for some $(\mathbf{r},i)$ is $O(q^n/n)$, we have

$$\begin{aligned} S^\diamond(n,h) = 2^{-(h-1)}&\sum_{D_{\mathbf{r},0}}\sum_{D_{\mathbf{r},1}} \Big(\prod_{\mathbf{r}} 2^{-(h+1)\omega(D_{\mathbf{r},0}D_{\mathbf{r},1})}\Big) \\ &\times\Big\{\prod_{\mathbf{r}}\prod_{\mathbf{s}}\Big(\frac{D_{\mathbf{r},0}D_{\mathbf{r},1}}{D_{\mathbf{s},0}D_{\mathbf{s},1}}\Big)^{\kappa_h(\mathbf{r},\mathbf{s})}\Big\} + O_{h,\epsilon}(q^n n^{\epsilon-2^{-h-2}}), \end{aligned} \tag{6.22}$$

where $D_{\mathbf{r},0}, D_{\mathbf{r},1} \in \mathcal{D}\cup\{1\}$ are coprime and satisfy

$$\sum_{\mathbf{r}} \deg D_{\mathbf{r},0} + \sum_{\mathbf{r}} \deg D_{\mathbf{r},1} = n.$$

Setting $D_{\mathbf{r}} = D_{\mathbf{r},0}D_{\mathbf{r},1}$ (we have $2^{\omega(D_{\mathbf{r}})}$ possibilities), we modify (6.22) into

$$S^{\diamond}(n,h) = 2^{-(h-1)} \sum_{D_{\mathbf{r}}} \Big(\prod_{\mathbf{r}} 2^{-h\omega(D_{\mathbf{r}})} \Big) \Big\{ \prod_{\mathbf{r}} \prod_{\mathbf{s}} \Big(\frac{D_{\mathbf{r}}}{D_{\mathbf{s}}} \Big)^{\kappa_h(\mathbf{r},\mathbf{s})} \Big\} + O_{h,\epsilon}(q^n n^{\epsilon - 2^{-h-2}}),$$

where $D_{\mathbf{r}} \in \mathcal{D} \cup \{1\}$ are coprime and $\sum_{\mathbf{r}} \deg D_{\mathbf{r}} = n$. Then (6.3) implies

$$S^{\diamond}(n,h) = 2S^*(n,h) + O_{h,\epsilon}(q^n n^{\epsilon - 2^{-h-2}}). \tag{6.23}$$

By inserting (6.23) into (6.15), we get

$$S^*_{\mathrm{mix}}(n,h) = \tfrac{1}{2} S^*(n,h+1) + \tfrac{1}{2} S^*(n,h) + O_{h,\epsilon}(q^n n^{\epsilon - 2^{-h-2}}).$$

Therefore, by (6.14) and the equality

$$\frac{1}{2} \prod_{j=0}^{h} (2^j + 1) + \frac{1}{2} \prod_{j=0}^{h-1} (2^j + 1) = (2^{h-1} + 1) \frac{1}{2} \prod_{j=0}^{h-1} (2^j + 1),$$

we have

$$S^*_{\mathrm{mix}}(n,h) = (2^{h-1} + 1) \prod_{j=0}^{h-1} (2^j + 1) \cdot \mathcal{D}(n) + O_{h,\epsilon}(q^n n^{\epsilon - 2^{-h-2}}),$$

which finishes the proof of the second part of Theorem 1.6.

Acknowledgments. The first author is supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0001184).

The second author is supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0005138).

References

[Ap76] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[BJ] S. Bae and H. Jung, *ℓ-ranks of class groups of function fields*, submitted.

[CL84] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields*, in: Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. 1068, Springer, Berlin, 1984, 33–62.

[FK06] E. Fouvry and J. Klüners, *Cohen–Lenstra heuristics of quadratic number fields*, in: F. Hess et al. (eds.), 7th Algorithmic Number Theory Symposium, Lecture Notes in Comput. Sci. 4076, Springer, Berlin, 2006, 40–55.

[FK07] —, —, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. 167 (2007), 455–513.

[FK10] —, —, *On the negative Pell equation*, Ann. of Math. (2) 172 (2010), 2035–2104.

[Ge87] F. Gerth III, *Extension of conjectures of Cohen and Lenstra*, Expo. Math. 5 (1987), 181–184.

[HR74] H. Halberstam and H. E. Richert, *Sieve Methods*, London Math. Soc. Monogr. 4, Academic Press, London, 1974.

[Hs98] C.-N. Hsu, *On certain character sums over* $\mathbb{F}_q[T]$, Proc. Amer. Math. Soc. 126 (1998), 647–652.

[Ro02] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, New York, 2002.

[Sh80] P. Shiu, *A Brun–Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. 313 (1980), 161–170.

[St93] P. Stevenhagen, *The number of real quadratic fields with units of negative norms*, Experiment. Math. 2 (1993), 121–136.

[Wa97] L. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997,

[Wi07] C. Wittmann, *ℓ-Class groups of cyclic function fields of degree ℓ*, Finite Fields Appl. 13 (2007), 327–347.

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

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

Received on 18.3.2010
and in revised form on 6.7.2011 (6335)