TAIWANESE JOURNAL OF MATHEMATICS
Vol. 25, No. 1, pp. 23–43, February 2021
DOI: 10.11650/tjm/200602

Variation of a Theme of Landau–Shanks in Positive Characteristic

Chih-Yun Chuang, Yen-Liang Kuan* and Wei-Chen Yao

Abstract. Let $\mathbf{A} := \mathbb{F}_q[t]$ be a polynomial ring over a finite field $\mathbb{F}_q$ of odd characteristic and let $D \in \mathbf{A}$ be a square-free polynomial. Denote by $\mathbf{N}_D(n,q)$ the number of polynomials f in $\mathbf{A}$ of degree n which may be represented in the form $u \cdot f = A^2 - DB^2$ for some $A, B \in \mathbf{A}$ and $u \in \mathbb{F}_q^\times$, and by $\mathbf{B}_{\mathcal{D}}(n,q)$ the number of polynomials in $\mathbf{A}$ of degree n which can be represented by a primitive quadratic form of a given discriminant $\mathcal{D} \in \mathbf{A}$, not necessary square-free. If the class number of the maximal order of $\mathbb{F}_q(t, \sqrt{D})$ is one, then we give very precise asymptotic formulas for $\mathbf{N}_D(n,q)$. Moreover, we also give very precise asymptotic formulas for $\mathbf{B}_{\mathcal{D}}(n,q)$.

1. Introduction

Let $B(x)$ denote the number of positive integers $m \le x$ which may be represented in the form $m = u^2 + v^2$, where u and v are integers. Landau [8] proved that

$$B(x) \sim \mathcal{K} \frac{x}{\sqrt{\log x}}$$

where $\mathcal{K} = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} (1 - p^{-2})^{-1/2}$ is the Landau–Ramanujan constant. Landau's result was improved by Shanks [13] who gave an asymptotic formula for $B(x)$:

$$B(x) = \mathcal{K} \frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log^{3/2} x} \right).$$

A similar problem for positive integers represented as the form $u^2 + dv^2$ where $d \neq -k^2$ and u, v are positive integers was considered by several mathematicians [14]. For integer $d \neq -k^2$, let $B_d(x)$ be the number of positive integers $m \le x$ which may be represented of the form $m = u^2 + dv^2$,

$$B_d(x) \sim \frac{b_d}{(\log x)^{1/2}}$$

for some constant b_d, but b_d is not easy to calculate in general.

A variation of the problem of integers represented by a sum of squares is integers represented by a binary quadratic form. Let $d \le -3$ be a negative integer and let $\mathbf{B}(x)$

Received March 5, 2020; Accepted June 16, 2020.
Communicated by Yu-Ru Liu.
2010 *Mathematics Subject Classification.* 11N37, 11E12, 11T55.
Key words and phrases. binary quadratic forms, polynomials over finite fields.
*Corresponding author.

denote the number of positive integers $m \leq x$ which are prime to d and which can be represented by positive, primitive, binary quadratic forms of a given negative discriminant d. James [7] used Pall's result [10] to prove that

$$\mathbf{B}(x) = b\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{\log x}\right),$$

where b is the positive constant given by

$$b = \frac{1}{\sqrt{\pi}} \prod_{p:\left(\frac{d}{p}\right)=-1} (1-p^{-2})^{-1/2} \prod_{p|d} (1-p^{-1})^{1/2} \left(\sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n}\right)^{1/2}.$$

Here $\left(\frac{d}{n}\right)$ is the Kronecker symbol. Moreover, Pall [11] deduced a similar result of James without the restriction that m is prime to d.

In this paper, we study analogues of Landau–Shanks' and James–Pall's theorems for polynomial rings. For convenience, we will fix the following notations in this paper:

$$\begin{aligned}
\mathbf{A} &= \mathbb{F}_q[t], \text{ the polynomial ring over the finite field } \mathbb{F}_q \text{ of odd characteristic,}\\
k &= \mathbb{F}_q(t), \text{ the fraction field of } \mathbf{A},\\
\mathbf{A}^+ &= \text{the set of monic polynomials in } \mathbf{A},\\
\mathbf{A}_n^+ &= \text{the set of monic polynomials of degree } n \text{ in } \mathbf{A},\\
\mathbf{P}^+ &= \text{the set of all monic irreducible polynomials in } \mathbf{A}.
\end{aligned}$$

Let D be a square-free polynomial in $\mathbf{A}$. Put $K = k(\sqrt{D})$ and $O_K = \mathbf{A} + \mathbf{A}\sqrt{D}$. For $f \in \mathbf{A}^+$, we define the characteristic function

$$\mathbf{n}_{D,q}(f) := \begin{cases} 1 & \text{if } u \cdot f = A^2 - DB^2 \text{ for some } A, B \in \mathbf{A} \text{ and } u \in \mathbb{F}_q^\times, \\ 0 & \text{otherwise} \end{cases}$$

and the counting function

$$\mathbf{N}_D(n,q) := \sum_{f \in \mathbf{A}_n^+} \mathbf{n}_{D,q}(f).$$

There are several cases that u can be removed. First of all, if $\deg D$ is odd and the leading coefficient of $-D$ is a square in $\mathbb{F}_q^\times$. Secondly, O_K is real quadratic and has narrow class number one. For the cases $D = -1$ and $D = -t$, a polynomial analogue of Landau–Shanks' problem has been studied by Bary-Soroker, Smilansky, Wolf [1] and Gorodetsky [5]. We generalize their results to square-free polynomials $D \in \mathbf{A}$ and prove an analogue of Landau–Shanks' theorem as follows.

Theorem 1.1. *Assume that the class number of O_K is 1. We have, for any real number $0 < \delta < 1/2$,*

$$\mathbf{N}_D(n,q) = \widehat{a}_{D,q}(1)\binom{n-1/2}{n}q^n + O\left(\frac{q^{n-1/2+\delta}}{n^{3/2}}\right) \quad \text{as } n \to \infty,$$

where

$$\widehat{a}_{D,q}(s) = \sqrt{L\big(s,\big(\tfrac{D}{\cdot}\big)\big)} \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=-1}} (1-\mathbf{q}_P^{-2s})^{-1/2} \cdot \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=0}} (1-\mathbf{q}_P^{-s})^{-1/2}.$$

Here $\mathbf{q}_P := q^{\deg P}$ and $L\big(s,\big(\frac{D}{\cdot}\big)\big)$ is the Dirichlet L-function corresponding to the quadratic character $\big(\frac{D}{\cdot}\big)$.

In order to satisfy the condition that the class number of O_K is one, we only state the asymptotic formula in Theorem 1.1 for fix q. If we add some specific conditions to D, then we can rewrite the asymptotic formula in more general limit.

Theorem 1.2. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic and let $D \in \mathbb{F}_{q_0}[t]$. Then, for any real number $0 < \delta < 1/2$,*

$$\mathbf{N}_D(n,q) = \widehat{a}_{D,q}(1)\binom{n-1/2}{n}q^n + O\left(\frac{q^{n-1/2+\delta}}{n^{3/2}}\right) \quad \text{as } q^n \to \infty,$$

where $\widehat{a}_{D,q}(s)$ is defined as in Theorem 1.1 and q varies through powers of q_0 under the condition that D is square-free in $\mathbb{F}_q[t]$ and the class number of the maximal order of $\mathbb{F}_q(t,\sqrt{D})$ is one.

Remark 1.3. (a) There are only finitely many D for which O_K is imaginary quadratic of class number one, and conjecturally there are infinitely many D for which O_K is real quadratic of class number one. For more references, we refer the readers to [4, 15].

(b) If $D \in \mathbb{Z}[t]$ such that $\mathbb{F}_q[t,\sqrt{D}]$ has class number one for infinitely many q, we have the asymptotic formula for $\mathbf{N}_D(n,q)$ in the most general limit $q^n \to \infty$ without the condition q is a power of some fix q_0.

(c) When $D = -t$, the Dirichlet L-function $L\big(s,\big(\frac{D}{\cdot}\big)\big) = 1$ is a constant function. Then the main term coefficient $\widehat{a}_{D,q}(1)$ of $\mathbf{N}_D(n,q)$ is equal to

$$(1-q^{-1})^{-1/2} \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=-1}} (1-q^{-2\deg P})^{-1/2}$$

which is the same as Gorodetsky's result [5, Theorem 1.1].

The condition of class number one in Theorems 1.1 and 1.2 cannot be removed since the product formula (Corollary 3.3) of $\mathbf{n}_{D,q}$ is not correct. We will illustrate it in Example 3.4.

For the case of class number of O_K greater than one or D is not square-free, we investigate Landau–Shanks' problem for binary quadratic forms over polynomial rings. This is an analogue of results of James and Pall for the integer case. Instead of counting the number of solutions of representation by binary quadratic forms as Pall did, we use a different approach which use composition and other properties of binary quadratic forms. Hence we generalize their result for both definite and indefinite binary quadratic forms over polynomial rings.

For $\mathcal{D} \in \mathbf{A}$ and $m \in \mathbf{A}^+$, let $\mathbf{b}_{\mathcal{D},q}\colon \mathbf{A}^+ \to \mathbb{R}$ be the characteristic function defined by

$$\mathbf{b}_{\mathcal{D},q}(m) = \begin{cases} 1 & \text{if } m \text{ is represented by a primitive quadratic form of discriminant } \mathcal{D}, \\ 0 & \text{otherwise} \end{cases}$$

and define the counting function

$$\mathbf{B}_{\mathcal{D}}(n,q) := \sum_{f \in \mathbf{A}_n^+} \mathbf{b}_{\mathcal{D},q}(f).$$

Note that, when $\mathcal{D}$ is perfect square in $\mathbf{A}$, $\mathbf{b}_{\mathcal{D},q}(m) = 1$ for all m prime to $\mathcal{D}$. Then we have a trivial estimate

$$\mathbf{B}_{\mathcal{D}}(n,q) = O(q^n) \quad \text{as } n \to \infty.$$

So we now only consider that $\mathcal{D}$ is not perfect square in $\mathbf{A}$. In order to simplify the notation, we use the following definition. For $P \in \mathbf{P}^+$ with $P^2 \mid D$, we write $\mathcal{D} = P^{2k_P}\mathcal{D}'$ where $k_P \geq 1$ and $P^2 \nmid \mathcal{D}'$. The following theorem is an analogue of James–Pall's results with the discriminant $\mathcal{D}$ in odd characteristics.

Theorem 1.4. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic and $\mathcal{D} \in \mathbb{F}_{q_0}[t]$. For any real number $0 < \delta < 1/2$, we have*

$$\mathbf{B}_{\mathcal{D}}(n,q) = \widehat{a}_{\mathcal{D},q}(1)\binom{n-1/2}{n} q^n + O\left(\frac{q^{n-1/2+\delta}}{n^{3/2}}\right) \quad \text{as } q^n \to \infty,$$

where q varies through power of q_0 under the condition that $\mathcal{D}$ is not perfect square in $\mathbb{F}_q[t]$ and

$$\widehat{a}_{\mathcal{D},q}(s) := \sqrt{L\big(s, \left(\tfrac{\mathcal{D}}{\cdot}\right)\big)} \prod_{\substack{P \in \mathbf{P}^+ \\ \left(\frac{\mathcal{D}}{P}\right) = -1}} (1 - \mathbf{q}_P^{-2s})^{-1/2} \cdot \prod_{\substack{P \in \mathbf{P}^+ \\ P \| \mathcal{D}}} (1 - \mathbf{q}_P^{-s})^{-1/2} \cdot S(s).$$

Here

$$S(s) = \prod_{\substack{P \in \mathbf{P}^+ \\ P^2 \mid \mathcal{D}}} (1 - \mathbf{q}_P^{-s})^{1/2}\big(1 + \mathbf{q}_P^{-2s} + \cdots + \mathbf{q}_P^{(-2k_P+2)s} + \mathbf{q}_P^{-2k_P s}\Lambda(s)\big)$$

and

$$\Lambda(s) = \begin{cases} (1-\mathbf{q}_P^{-s})^{-1} & \text{if } \left(\frac{\mathcal{D}'}{P}\right) = 0 \text{ or } 1, \\ (1-\mathbf{q}_P^{-2s})^{-1} & \text{otherwise.} \end{cases}$$

We will prove Theorems 1.1 and 1.2 in Section 3 and prove Theorem 1.4 in Section 4. Darboux used contour integration to prove the following analytic theorem [6, Theorem 11.10b].

Theorem 1.5. *Let $a(x) = \sum a_k x^k$ and $b(x) = (1-x/\beta)^{-c} = \sum b_k x^k$ ($c \in \mathbb{C} \setminus \mathbb{Z}$) be two power series with radii of convergence $\alpha > \beta \geq 0$, respectively. Fix integers $n > m \geq 0$. Let f_n be the n-th coefficient of $f(x) = a(x)b(x)$. Then, as n goes to ∞,*

$$f_n = b_n \left(a(\beta) + \sum_{k=1}^{m} \frac{\binom{k-c}{k}}{\binom{n+c-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta) + O_{a,b,m}\left(\frac{1}{n^{m+1}}\right)\right).$$

Using Theorem 1.5, we can get asymptotic formulas, as n tends to ∞, in all theorems of this paper. In [5], Gorodetsky refine Theorem 1.5 to Theorem 1.6 and use Theorem 1.6 deduce the asymptotic formula as q^n tends to ∞ for $D = -t$.

Theorem 1.6. [5, Theorem 3.3] *Let $a(x) = \exp\left(\sum_{k\geq 1} \widetilde{a}_k x^k\right) = \sum a_k x^k$ and $b(x) = (1-x/\beta)^{-c_1} = \sum b_k x^k$ ($c_1 \in (0,1)$) be two power series, with radii of convergence at least α and exactly β, respectively. Assume that $\alpha > \beta > 0$. Assume that*

$$r = \frac{\beta}{\alpha} \leq \frac{1}{\sqrt{2}}. \tag{1.1}$$

Assume further that there is a positive number c_2 such that

$$\left|\widetilde{a}_k\right| \leq \frac{c_2}{\alpha^k}. \tag{1.2}$$

Fix an integer $m \geq 0$. For an integer $n > m$, write the n-th coefficient f_n of $f(x) = a(x)b(x)$ as

$$f_n = b_n \left(a(\beta) + \sum_{k=1}^{m} \frac{\binom{k-c}{k}}{\binom{n+c-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta) + E\right).$$

Then

$$|E| \ll_{m,c_1,c_2} \left(\frac{r}{n}\right)^{m+1}.$$

For general D, it is difficult to fulfil the assumption (1.2). We derive the same result without the assumptions (1.1) and (1.2) in Section 2.

2. Preliminaries on analytic theorem

For $\alpha \in \mathbb{R}$ and $R > 0$, denote by $D(\alpha, R)$ the unit disk with radius R and its center at α. Set $\partial D(\alpha, R)$ the boundary of $D(\alpha, R)$ and $M_a(\alpha, R) := \max_{x \in \partial D(\alpha,R)} |a(x)|$. Let $x^c := e^{c \ln x}$ for $c \in (0,1)$, analytic branch of $\ln x$ fixed with $0 < \mathrm{Arg}(x) < 2\pi$. We will prove

Theorem 2.1. *Let $a(x) = \sum a_k x^k$ and $b(x) = (1 - x/\beta)^{-c} = \sum b_k x^k$ $(c \in (0,1))$ be two power series, with radii of convergence at least α and exactly β, respectively. Assume that $\alpha > \beta > 0$. Fix an integer $m \geq 0$. For an integer $n > m$, write the n-th coefficient f_n of $f(x) = a(x)b(x)$ as*

$$f_n = b_n \left(a(\beta) + \sum_{k=1}^{m} \frac{\binom{k-c}{k}}{\binom{n+c-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta) + E \right).$$

Then

$$|E| < \frac{\beta^{n+c} \sin(c\pi)}{\pi \cdot R^c \cdot n \cdot (\beta + R)^n \cdot \left|\binom{-c}{n}\right|} + \sum_{k=1}^{m} \frac{\beta^k \cdot \sin(c\pi)}{\pi} \cdot \frac{\left(1 + \frac{R}{\beta}\right)^{-(n-k+c)}}{(n-k+c) \cdot \left|\binom{-c}{n}\right|}$$
$$+ \frac{M_a(\beta, \widetilde{R})}{\pi \cdot \widetilde{R}^m \cdot \left(\widetilde{R} - R\right)} \cdot \frac{\binom{m+1-c}{m+1}}{\binom{n+c-1}{m+1}} \cdot \beta^{m+1} + \frac{\beta^n \cdot M_a(0, \beta + R)}{\left(\frac{R+\beta}{\beta} - 1\right)^c \cdot (\beta + R)^n \cdot \left|\binom{-c}{n}\right|},$$

where R and $\widetilde{R}$ are real numbers satisfying $\alpha - \beta > \widetilde{R} > R > 0$.

Choose $0 < \theta < \pi/2$ and $0 < R < \alpha - \beta$. Fix $r, \epsilon > 0$ such that $r < \min\{R, \beta/2\}$ and $\epsilon < \beta/2$. Let $C_0 := \{u \in \mathbb{C} : |u| = \epsilon\}$ be a small circle oriented clockwise. Consider the keyhole contour starting from a small clockwise oriented circle C_r about β of radius r, extending to a line segment $\gamma_1 = \{\beta + x \exp(i\theta) \mid x \in [r, R]\}$, close to and above the branch cut, then continued to the circle C_R counterclockwise oriented around the origin of radius $\sqrt{2\beta R \cos(\theta) + \beta^2 + R^2}$, returning to a line segment $\gamma_2 = \{\beta + x \exp\left(i(2\pi - \theta)\right) \mid x \in [r, R]\}$, close to and below the branch cut in the negative sense, finally returning to the original small circle C_r as in Figure 2.1.

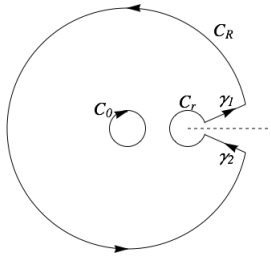

Figure 2.1: A keyhole contour.

Lemma 2.2. *For each $n \in \mathbb{N}$, we have*

$$f_n = \frac{1}{2\pi i} \int_{\gamma_1 + C_R + \gamma_2 + C_r} \frac{f(x)}{x^{n+1}}\, dx.$$

Proof. Since $f(x)/x^{n+1}$ is analytic inside the contour $\gamma_1 + C_R + \gamma_2 + C_r$ except at the point $x = 0$,

$$\int_{C_0 + \gamma_1 + C_R + \gamma_2 + C_r} \frac{f(x)}{x^{n+1}}\, dx = 0.$$

From the power series expansion of $f(x)$ about $x = 0$, we obtain

$$\frac{1}{2\pi i} \int_{C_0} \frac{f(x)}{x^{n+1}}\, dx = -f_n.$$

This completes the proof of the lemma. □

We are now ready to prove Theorem 2.1 by establishing the following

Proposition 2.3. (a) *For each $n \in \mathbb{N}$, we have*

$$\lim_{r \to 0} \frac{1}{2\pi i} \int_{C_r} \frac{f(x)}{x^{n+1}}\, dx = 0.$$

(b) *For each $n \in \mathbb{N}$, we have*

$$\left| \lim_{\theta \to 0} \frac{1}{2\pi i} \int_{C_R} \frac{f(x)}{x^{n+1}}\, dx \right| \leq \frac{M_a(0, \beta + R)}{\left(\frac{R+\beta}{\beta} - 1\right)^c \cdot (\beta + R)^n}.$$

(c) *For each $n \in \mathbb{N}$, we have*

$$\lim_{r \to 0} \frac{1}{2\pi i} \int_{\gamma_1 + \gamma_2} \frac{f(x)}{x^{n+1}}\, dx = b_n \left(a(\beta) + \sum_{k=1}^{m} \frac{\binom{k-c}{k}}{\binom{n+c-1}{k}} \frac{\beta^k}{k!} a^{(k)}(\beta) + \widetilde{E} \right),$$

and

$$\begin{aligned} |\widetilde{E}| < {} & \frac{\beta^{n+c} \sin(c\pi)}{\pi \cdot R^c \cdot n \cdot (\beta + R)^n \cdot \left|\binom{-c}{n}\right|} + \sum_{k=1}^{m} \frac{\beta^k \cdot \sin(c\pi)}{\pi} \cdot \frac{\left(1 + \frac{R}{\beta}\right)^{-(n-k+c)}}{(n-k+c) \cdot \left|\binom{-c}{n}\right|} \\ & + \frac{M_a(\beta, \widetilde{R})}{\pi \cdot \widetilde{R}^m \cdot \left(\widetilde{R} - R\right)} \cdot \frac{\binom{m+1-c}{m+1}}{\binom{n+c-1}{m+1}} \cdot \beta^{m+1}, \end{aligned}$$

where $\widetilde{R}$ is any real number satisfies $\alpha - \beta > \widetilde{R} > R > 0$.

Proof. (a) Let $x = \beta + r\exp(iu)$, where $u \in [\theta, 2\pi - \theta)$. Then we have

$$\begin{aligned} \left| \int_{C_r} \frac{f(x)}{x^{n+1}}\, dx \right| &\leq \int_{\theta}^{2\pi - \theta} \left| \frac{a(\beta + r\exp(iu)) \cdot \beta^c r^{1-c}}{(\beta + r\exp(iu))^{n+1}} \right| du \\ &\leq \frac{2 \cdot \pi \cdot M_a(\beta, r) \cdot \beta^c r^{1-c}}{(\beta - r)^{n+1}} \to 0 \quad \text{as } r \to 0. \end{aligned}$$

(b) Let $x = \left(\sqrt{\beta^2 + 2R\beta\cos(\theta) + R^2}\right) \cdot \exp(iu)$, where $u \in [\theta, 2\pi - \theta)$. We have

$$\begin{aligned}\left|\lim_{\theta\to 0}\int_{C_R} \frac{f(x)}{x^{n+1}}\,dx\right| &\le \int_0^{2\pi}\left|\frac{a((\beta+R)\cdot\exp(iu))\cdot(\beta+R)}{\left(1-\frac{(\beta+R)\cdot\exp(iu)}{\beta}\right)^c((\beta+R)\cdot\exp(iu))^{n+1}}\right| du \\ &\le \frac{2\cdot\pi\cdot M_a(0,\beta+R)}{\left(\frac{R+\beta}{\beta}-1\right)^c\cdot(\beta+R)^n}.\end{aligned}$$

(c) Set $\gamma_1 = \beta + x\exp(i\theta)$, where x goes from r to R and $\gamma_2 = \beta + x\exp\big((2\pi-\theta)i\big)$, where x goes from R to r. As $\theta \to 0$, we have

$$\frac{1}{2\pi i}\int_{\gamma_1+\gamma_2}\frac{f(x)}{x^{n+1}}\,dx = \frac{\beta^c\cdot\sin(c\pi)}{\pi}\cdot\int_r^R \frac{a(\beta+x)}{x^c\cdot(\beta+x)^{n+1}}\,dx.$$

Fix a constant $\widetilde{R}$ with $\alpha - \beta > \widetilde{R} > R$. Since $a(x)$ is holomorphic on the closed disc $D(\beta,\widetilde{R}) \subset D(\beta,\alpha-\beta)$, so the Taylor expansion of $a(x)$ at the point β holds in the form

$$a(x) = \sum_{k=0}^{m}\frac{a^{(k)}(\beta)}{k!}(x-\beta)^k + R_m(x),$$

where the remainder $R_m(x)$ has the following uniform bound

$$|R_m(x)| < \frac{M_a(\beta,\widetilde{R})\cdot|x-\beta|^{m+1}}{\widetilde{R}^m\cdot\big(\widetilde{R}-|x-\beta|\big)}. \tag{2.1}$$

Therefore, we derive

$$\begin{aligned}\int_r^R \frac{a(\beta+x)}{x^c\cdot(\beta+x)^{n+1}}\,dx &= \sum_{k=0}^{m}\frac{a^{(k)}(\beta)}{k!}\int_r^R\frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx + \int_r^R\frac{R_m(\beta+x)}{x^c\cdot(\beta+x)^{n+1}}\,dx \\ &:= I_1 + I_2.\end{aligned}$$

We rewrite the integral in I_1 to be

$$\lim_{r\to 0}\int_r^R\frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx = \int_0^\infty\frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx - \int_R^\infty\frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx.$$

From the property of the beta function, one has

$$\begin{aligned}\int_0^\infty\frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx &= \beta^{k-c-n}\cdot\frac{\Gamma(1+k-c)\Gamma(-k+c+n)}{\Gamma(n+1)} \\ &= \beta^{k-c-n}\cdot\frac{(-1)^n\binom{k-c}{k}\binom{-c}{n}}{\binom{n+c-1}{k}}\cdot\Gamma(1-c)\cdot\Gamma(c).\end{aligned}$$

So we have

$$\begin{aligned}
&\frac{\beta^c \cdot \sin(c\pi)}{\pi} \cdot \lim_{r\to 0}\left(\sum_{k=0}^{m} \frac{a^{(k)}(\beta)}{k!}\int_r^R \frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx\right)\\
&= \frac{\beta^{-n}\cdot \sin(c\pi)}{\pi}\cdot\left[\sum_{k=0}^{m}\frac{a^{(k)}(\beta)\beta^k}{k!}\frac{(-1)^n\binom{k-c}{k}\binom{-c}{n}}{\binom{n+c-1}{k}}\cdot\Gamma(1-c)\cdot\Gamma(c)\right]\\
&\quad -\frac{\beta^c\cdot\sin(c\pi)}{\pi}\cdot\left[\sum_{k=0}^{m}\int_R^\infty \frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx\right].
\end{aligned}$$

Note that $b_n = (-1)^n\cdot\beta^{-n}\cdot\binom{-c}{n}$ and $\Gamma(1-c)\Gamma(c) = \pi/\sin(c\pi)$. Combining these equalities and the estimate

$$\int_R^\infty \frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx < \begin{cases} \int_R^\infty \frac{1}{(\beta+x)^{n+1-k+c}}\,dx = \frac{(\beta+R)^{-(n-k+c)}}{n-k+c} & \text{if } k>0,\\ \frac{1}{R^c\cdot n\cdot(\beta+R)^n} & \text{if } k=0,\end{cases}$$

we obtain

$$\begin{aligned}
&\frac{\beta^c\cdot\sin(c\pi)}{\pi}\cdot\lim_{r\to 0}\left(\sum_{k=0}^{m}\frac{a^{(k)}(\beta)}{k!}\int_r^R\frac{x^{k-c}}{(\beta+x)^{n+1}}\,dx\right)\\
&= b_n\left(a(\beta)+\sum_{k=1}^{m}\frac{\binom{k-c}{k}}{\binom{n+c-1}{k}}\frac{\beta^k}{k!}a^{(k)}(\beta)+E_1\right),
\end{aligned}$$

where

$$|E_1| < \frac{\beta^{n+c}\sin(c\pi)}{\pi\cdot R^c\cdot n\cdot(\beta+R)^n\cdot\left|\binom{-c}{n}\right|} + \sum_{k=1}^{m}\frac{\beta^k\cdot\sin(c\pi)}{\pi}\cdot\frac{\left(1+\frac{R}{\beta}\right)^{-(n-k+c)}}{(n-k+c)\cdot\left|\binom{-c}{n}\right|}. \tag{2.2}$$

Applying the bound of $R_m(x)$ in (2.1) to I_2, we obtain

$$\begin{aligned}
|I_2| &= \left|\int_r^R \frac{R_m(\beta+x)}{x^c\cdot(\beta+x)^{n+1}}\,dx\right| < \frac{M_a(\beta,\widetilde{R})}{\widetilde{R}^m\cdot(\widetilde{R}-R)}\cdot\int_0^\infty\frac{x^{m+1-c}}{(\beta+x)^{n+1}}\,dx\\
&= \frac{M_a(\beta,\widetilde{R})}{\widetilde{R}^m\cdot(\widetilde{R}-R)}\cdot\beta^{1+m-c-n}\frac{\Gamma(2+m-c)\Gamma(-1-m+c+n)}{\Gamma(n+1)}\\
&= \frac{M_a(\beta,\widetilde{R})}{\widetilde{R}^m\cdot(\widetilde{R}-R)}\cdot\beta^{1+m-c-n}\frac{(-1)^n\binom{m+1-c}{m+1}\binom{-c}{n}}{\binom{n+c-1}{m+1}}\cdot\Gamma(1-c)\cdot\Gamma(c),
\end{aligned}$$

which implies that

$$\left|b_n^{-1}\cdot\frac{\beta^c\cdot\sin(c\pi)}{\pi}\cdot I_2\right| = \frac{M_a(\beta,\widetilde{R})}{\pi\cdot\widetilde{R}^m\cdot(\widetilde{R}-R)}\cdot\frac{\binom{m+1-c}{m+1}}{\binom{n+c-1}{m+1}}\cdot\beta^{m+1}. \tag{2.3}$$

Combining (2.2) and (2.3), this completes the proof. □

We now put $x := q^{-s}$ in Theorem 2.1 for $s \in \mathbb{C}$ and write $\alpha = q^{-\alpha_0}$ and $\beta = q^{-\beta_0}$ with $\alpha > \beta > 0$. Fix a constant $\delta > 0$ such that $\beta_0 - \alpha_0 > \delta > 0$. Set $R = q^{-\alpha_0-\delta} - q^{-\beta_0}$ and $\widetilde{R} = q^{-\alpha_0-\delta/2} - q^{-\beta_0}$. Since $a(x) = \sum a_k x^k$ is a power series with radius of convergence at least $\alpha < 1$, given any $\epsilon > 0$, there exists a constant $C_{a,\epsilon}$ such that $|a_n| \le C_{a,\epsilon} \cdot |\alpha|^{(-1-\epsilon)n}$ for all $n \ge 0$. Take $\epsilon = \delta/(4\alpha_0)$, we have

$$M_a(\beta, \widetilde{R}) < M_a(0, \beta + \widetilde{R}) \le \frac{C_{a,\delta,1}}{1 - q^{-(\delta/2-\delta/4)}} \quad \text{and} \quad M_a(0, \beta + R) \le \frac{C_{a,\delta,2}}{1 - q^{-(\delta-\delta/4)}},$$

where $C_{a,\delta,1}$ and $C_{a,\delta,2}$ are constants which depend on a and δ. Then we can rewrite Theorem 2.1 as follows:

Theorem 2.4. *Let $\widehat{a}(s) = \sum a_k q^{-sk}$ and $\widehat{b}(s) = (1 - q^{\beta_0 - s})^{-c} = \sum b_k q^{-sk}$ $(c \in (0,1))$ be two power series of variable q^{-s}, with radii of convergence at least $q^{-\alpha_0}$ and exactly $q^{-\beta_0}$, respectively. Assume that $\beta_0 > \alpha_0 > 0$. Fix an integer $m \ge 0$. For an integer $n > m$, write the n-th coefficient f_n of variable q^{-s} for $f(s) = \widehat{a}(s)\widehat{b}(s)$ as*

$$f_n = b_n \left(\widehat{a}(\beta_0) + \sum_{k=1}^{m} \frac{\binom{k-c}{k}}{\binom{n+c-1}{k}} \frac{q^{-\beta_0 k}}{k!} \frac{d^k \widehat{a}}{(dq^{-s})^k}(\beta_0) + E \right).$$

Then

$$\begin{aligned} |E| < {} & \frac{\sin(c\pi) \cdot q^{(\alpha_0-\beta_0+\delta)(n+c)}}{\pi \cdot (1 - q^{(\alpha_0-\beta_0+\delta)c}) \cdot \left|\binom{-c}{n}\right|} \\ & + \frac{\sin(c\pi) \cdot q^{(\alpha_0-\beta_0+\delta)(n+c)}}{\pi \cdot \left|\binom{-c}{n}\right|} \left(\sum_{k=1}^{m} \frac{1}{(n-k+c)} \cdot q^{-k(\alpha_0-\beta_0+\delta)} \right) \\ & + \frac{C_{\widehat{a},\delta,1} \cdot q^{(\alpha_0-\beta_0+\delta/2)(m+1)}}{(1 - q^{-\delta/4})(1 - q^{\alpha_0-\beta_0+\delta})^m} \cdot \frac{\binom{m+1-c}{m+1}}{\binom{n+c-1}{m+1}} + \frac{C_{\widehat{a},\delta,2} \cdot q^{(\alpha_0-\beta_0+\delta)(n+c)}}{(1 - q^{-\frac{3}{4}\delta}) \cdot (1 - q^{\alpha_0-\beta_0+\delta})^c \cdot \left|\binom{-c}{n}\right|}, \end{aligned}$$

where δ is any real number satisfying $\beta_0 - \alpha_0 > \delta > 0$ and $C_{\widehat{a},\delta,1}$, $C_{\widehat{a},\delta,2}$ are constants which depend on $\widehat{a}$ and δ.

Remark 2.5. Notice that

$$\frac{C_{\widehat{a},\delta,1} \cdot q^{(\alpha_0-\beta_0+\delta/2)(m+1)}}{(1 - q^{-\delta/4})(1 - q^{\alpha_0-\beta_0+\delta})^m} \cdot \frac{\binom{m+1-c}{m+1}}{\binom{n+c-1}{m+1}} = O\left(\frac{q^{(\alpha_0-\beta_0+\delta/2)(m+1)}}{n^{(m+1)}} \right) \quad \text{as } q^n \to \infty$$

and the other terms are dominated by $O\big(n^{(1-c)} q^{(\alpha_0-\beta_0+\delta)(n+c)}\big)$ since one has $1/\binom{-c}{n} = O(n^{1-c})$.

Corollary 2.6. *Let $\widehat{a}(s) = \sum a_k q^{-sk}$ and $\widehat{b}(s) = (1 - q^{\beta_0 - s})^{-c} = \sum b_k q^{-sk}$ $(c \in (0,1))$ be two power series of variable q^{-s} with radii of convergence at least $q^{-\alpha_0}$ and exactly $q^{-\beta_0}$,*

respectively. Assume that $\beta_0 > \alpha_0 > 0$. *Fix an integer* $m \geq 0$ *and write* $f(s) = \widehat{a}(s)\widehat{b}(s) = \sum f_k q^{-sk}$. *Then we have*

$$f_n = b_n \left(\widehat{a}(\beta_0) + \sum_{k=1}^{m} \frac{\binom{k-c}{k}}{\binom{n+c-1}{k}} \frac{q^{-\beta_0 k}}{k!} \frac{d^k \widehat{a}}{(dq^{-s})^k}(\beta_0) + O\left(\frac{q^{(\alpha_0-\beta_0+\delta/2)(m+1)}}{n^{(m+1)}} \right) \right) \quad \text{as } n \to \infty,$$

where δ *is any real number satisfying* $\beta_0 - \alpha_0 > \delta > 0$.

3. Landau–Shanks' problem

In this section, we will use Theorem 2.4 to prove Theorems 1.1 and 1.2. We now prove some properties as follows:

Lemma 3.1. *Assume the class number of* O_K *is* 1. *Let* $P \in \mathbf{P}^+$. *Then the quadratic symbol* $\left(\frac{D}{P}\right) \in \{0, 1\}$ *if and only if there exist* $u \in \mathbb{F}_q^\times$ *and* $x, y \in \mathbf{A}$ *such that* $u \cdot P = x^2 - Dy^2$.

Proof. If $\left(\frac{D}{P}\right) = 0$, then $P \mid D$ which implies that P is ramified in O_K/A. So there exists a prime ideal $\wp$ in O_K such that $PO_K = \wp^2$. Since the class number of O_K is 1, there exist $x, y \in A$ such that the ideal $\wp$ generated by $x + y\sqrt{D}$ in O_K. By [12, Proposition 7.8], the ideal generated by P in A is equal to the ideal generated by $N_{K/k}(x + y\sqrt{D}) = x^2 - Dy^2$ in A. Hence there exists $u \in \mathbb{F}_q^\times$ such that $u \cdot P = x^2 - Dy^2$. For the case $\left(\frac{D}{P}\right) = 1$, then P splits in O_K which means $PO_K = \wp_1\wp_2$ for two distinct prime ideals $\wp_1$, $\wp_2$ in O_K. Similarly, there exist $x, y \in A$ such that the ideal $\wp_1$ generated by $x + y\sqrt{D}$ in O_K, and there exists $u \in \mathbb{F}_q^\times$ such that $u \cdot P = x^2 - Dy^2$.

Conversely, we may assume $P \nmid D$. Since $u \cdot P = x^2 - Dy^2$ for some $u \in \mathbb{F}_q^\times$ and $x, y \in \mathbf{A}$, $x^2 \equiv Dy^2 \pmod{P}$ which implies $\left(\frac{D}{P}\right) = 1$. □

Proposition 3.2. *Assume the class number of* O_K *is* 1. *For any* $f \in \mathbf{A}$, *write* $f = mn^2$ *where* $m, n \in \mathbf{A}$ *and* m *is square-free. Then we have* $\left(\frac{D}{P}\right) \in \{0, 1\}$ *for all* $P \in \mathbf{P}^+$ *and* $P \mid m$ *if and only if there exist* $u \in \mathbb{F}_q^\times$ *and* $x, y \in \mathbf{A}$ *such that* $u \cdot f = x^2 - Dy^2$.

Proof. Assume that $f = mn^2$ and $\left(\frac{D}{P}\right) \in \{0, 1\}$ for all $P \mid m$. Since

$$(x_1 - Dy_1^2)(x_2 - Dy_2^2) = (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2$$

and n^2 is represented by $n^2 - D \cdot 0^2$, then there exists $u \in \mathbb{F}_q^\times$ such that $u \cdot f = x^2 - Dy^2$ for some $x, y \in \mathbf{A}$ by Lemma 3.1.

Conversely, assume that $u \cdot f = x^2 - Dy^2$ for some $u \in \mathbb{F}_q^\times$ and $x, y \in \mathbf{A}$, and there exists $P \mid m$ such that $\left(\frac{D}{P}\right) = -1$. Since $m \mid (x^2 - Dy^2)$, $x^2 \equiv Dy^2 \pmod{P}$. This contradicts to $\left(\frac{D}{P}\right) = -1$. □

Let $\mathbf{n}_{D,q}\colon \mathbf{A}^+ \to \mathbb{R}$ be the characteristic function defined by

$$\mathbf{n}_{D,q}(f) := \begin{cases} 1 & \text{if } u \cdot f = A^2 - DB^2 \text{ for some } A, B \in \mathbf{A} \text{ and } u \in \mathbb{F}_q^\times, \\ 0 & \text{otherwise.} \end{cases}$$

It is clearly that $\mathbf{n}_{D,q}(f^2) = 1$ for all $f \in \mathbf{A}^+$.

Corollary 3.3. *Assume the class number of O_K is 1. Then $\mathbf{n}_{D,q}(fg) = \mathbf{n}_{D,q}(f) \cdot \mathbf{n}_{D,q}(g)$ for all $f, g \in \mathbf{A}^+$ with $\gcd(f, g) = 1$.*

Proof. Assume $\mathbf{n}_{D,q}(fg) = 1$ and write $f = m_1 n_1^2$, $g = m_2 n_2^2$ where $m_1, m_2, n_1, n_2 \in \mathbf{A}^+$ and m_1, m_2 are square-free. Since $\gcd(f, g) = 1$, $m_1 m_2$ is also square-free. By Proposition 3.2, we have $\left(\frac{D}{P}\right) \in \{0, 1\}$ for all irreducible polynomials P dividing $m_1 m_2$. Thus $\left(\frac{D}{P}\right) \in \{0, 1\}$ for all irreducible polynomials P dividing m_1, which implies that $\mathbf{n}_{D,q}(f) = 1$. Similarly, we also have $\mathbf{n}_{D,q}(g) = 1$.

On the other hand, if $\mathbf{n}_{D,q}(fg) = 0$, then there exists an irreducible polynomial $P \mid m_1 m_2$ such that $\left(\frac{D}{P}\right) = -1$ by Proposition 3.2. We may assume $P \mid m_1$. Since $\left(\frac{D}{P}\right) = -1$ for some P dividing m_1, we have $\mathbf{n}_{D,q}(f) = 0$. This completes the proof. □

The corollary fails if the class number of O_K is not one. We will illustrate it in the following example.

Example 3.4. Let $q = 3$ and $D = t^3 + t^2 + 2 \in A$, then the class number of O_K is 3. Put $f = t^2 + t + 2$ and $g = t^2 + 2t + 2$. It is easy to calculate that $\mathbf{n}_{D,q}(f) = \mathbf{n}_{D,q}(g) = 0$ and $\mathbf{n}_{D,q}(fg) = 1$.

Now, we are ready to prove Theorems 1.1 and 1.2. Define the counting function

$$\mathbf{N}_D(n, q) := \sum_{f \in \mathbf{A}_n^+} \mathbf{n}_{D,q}(f)$$

for $n \in \mathbb{Z}_{\geq 0}$. Consider the generating function of $\mathbf{N}_D(n, q)$:

$$F_D(s) = \sum_{n=0}^{\infty} \mathbf{N}_D(n, q) q^{-ns}.$$

Since $\mathbf{n}_{D,q}(f)$ is multiplicative, we have

$$\begin{aligned} F_{D,q}(s) &= \sum_{f \in \mathbf{A}^+} \mathbf{n}_{D,q}(f) q^{-\deg(f)s} = \prod_{P \in \mathbf{P}^+} \sum_{j=1}^{\infty} \frac{\mathbf{n}_{D,q}(P^j)}{(q^{\deg(P)s})^j} \\ &= \prod_{\substack{P \in \mathbf{P}^+ \\ \left(\frac{D}{P}\right) \in \{0,1\}}} (1 - q^{-\deg Ps})^{-1} \cdot \prod_{\substack{P \in \mathbf{P}^+ \\ \left(\frac{D}{P}\right) = -1}} (1 - q^{-2\deg Ps})^{-1} \end{aligned}$$

by Proposition 3.2.

For simplicity, we denote $q^{\deg P}$ by $\mathbf{q}_P$. We now recall some basic facts about zeta function of $\mathbf{A}$ and Dirichlet L-function corresponding to the quadratic character $\left(\frac{D}{\cdot}\right)$. The zeta function $\zeta_{\mathbf{A}}(s)$ of $\mathbf{A}$ is defined by

$$\zeta_{\mathbf{A}}(s) := \prod_{P\in\mathbf{P}^+} (1-\mathbf{q}_P^{-s})^{-1} \quad \text{for } \mathrm{Re}(s)>1.$$

Note that $\zeta_{\mathbf{A}}(s) = (1-q^{1-s})^{-1}$. On the other hand, Dirichlet L-function corresponding to $\left(\frac{D}{\cdot}\right)$ is defined by

$$\begin{aligned} L\big(s,\left(\tfrac{D}{\cdot}\right)\big) &:= \prod_{P\in\mathbf{P}^+} \left(1-\left(\frac{D}{P}\right)\mathbf{q}_P^{-s}\right)^{-1} \quad \text{for } s\in\mathbb{C} \\ &= \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=1}} (1-\mathbf{q}_P^{-s})^{-1} \cdot \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=-1}} (1+\mathbf{q}_P^{-s})^{-1}. \end{aligned}$$

It is well-known that $L\big(s,\left(\frac{D}{\cdot}\right)\big)$ is a polynomial in q^{-s} of degree at most $\deg(D)-1$ [12, Proposition 4.3]. It is not difficult to check that

$$F_{D,q}(s) = \sqrt{\zeta_{\mathbf{A}}(s)}\cdot\sqrt{L\big(s,\left(\tfrac{D}{\cdot}\right)\big)} \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=-1}} (1-\mathbf{q}_P^{-2s})^{-1/2} \cdot \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=0}} (1-\mathbf{q}_P^{-s})^{-1/2}.$$

Let

$$\widehat{a}_{D,q}(s) := \sqrt{L\big(s,\left(\tfrac{D}{\cdot}\right)\big)} \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=-1}} (1-\mathbf{q}_P^{-2s})^{-1/2} \cdot \prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{D}{P}\right)=0}} (1-\mathbf{q}_P^{-s})^{-1/2}$$

which converges absolutely for $\mathrm{Re}(s)>1/2$ and

$$\widehat{b}_q(s) := \sqrt{\zeta_{\mathbf{A}}(s)} = (1-q^{1-s})^{-1/2}.$$

We now consider $m=0$ in Theorem 2.4 with $F_{D,q}(s) = \widehat{a}_{D,q}(s)\cdot\widehat{b}_q(s)$, $\alpha_0=1/2$, $\beta_0=1$ and $c=1/2$. From Remark 2.5, when $\delta<1/2$, the error terms are dominated by

$$O\left(\frac{q^{-1/2+\delta/2}}{n}\right).$$

Note that if we write $\widehat{b}_q(s) = \sum b_k q^{-sk}$, then $b_n = (-1)^n\binom{-1/2}{n}q^n = \binom{n-1/2}{n}q^n$ for $n\geq 1$. When any $0<\delta<1/2$, one has

$$\begin{aligned} \mathbf{N}_D(n,q) &= \binom{n-1/2}{n} q^n \left(\widehat{a}_{D,q}(1) + O\left(\frac{q^{-1/2+\delta}}{n}\right)\right) \\ &= \widehat{a}_{D,q}(1)\binom{n-1/2}{n} q^n + O\left(\frac{q^{n-1/2+\delta}}{n^{3/2}}\right) \quad \text{as } q^n\to\infty, \end{aligned}$$

where q varies through finite powers of q_0. Here the second equality follows from the fact $\binom{n-1/2}{n} \sim 1/\sqrt{\pi n}$ as $n \to \infty$. This completes the proofs of Theorems 1.1 and 1.2.

4. Binary quadratic forms over $\mathbf{A}$

In this section, we will generalize Landau–Shanks' problem to binary quadratic forms over polynomial rings. A binary quadratic form f is a function in two variables $f(x,y) = Ax^2 + Bxy + Cy^2$ where $A, B, C \in \mathbf{A}$. For simplicity, we denote f by (A, B, C). A quadratic form $f = (A, B, C)$ is called primitive if $\gcd(A, B, C) = 1$. We say that a quadratic forms f and g are equivalent if there exists $\left[\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbf{A})$ such that $g(x,y) = a^{-1} f(\alpha x + \beta y, \gamma x + \delta y)$ where $a = \alpha\delta - \beta\gamma$. Furthermore, if $\left[\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{A})$, we say that f and g are properly equivalent. It is easy to see that the relations are equivalence relations and preserve the discriminant $\mathcal{D} = B^2 - 4AC$.

A polynomial m is represented by a form $f = (A, B, C)$ if there exist $z, w \in \mathbf{A}$ such that

$$m = Az^2 + Bzw + Cw^2.$$

If z and w are relatively prime, we say that m is *properly represented* by $f(z, w)$.

The following proposition is well-known. We omit the proof.

Proposition 4.1. [3, Lemma 2.3] *A form $f(x,y)$ properly represents a polynomial m if and only if $f(x,y)$ is properly equivalent to the form $g(x,y) = mx^2 + nxy + ly^2$ for some $n, l \in \mathbf{A}$.*

We define the composition of binary quadratic forms similar to the definition in integer cases [2, 16].

Definition 4.2. Let $f_1 = (A_1, B_1, C_1)$ and $f_2 = (A_2, B_2, C_2)$ be two binary quadratic forms of the same discriminant $\mathcal{D}$ and let $U, V, W \in \mathbf{A}$ such that

$$UA_1 + VA_2 + W(B_1 + B_2) = S = \gcd(A_1, A_2, B_1 + B_2).$$

We define the composition of f_1 and f_2 by $f_1 \cdot f_2 = (A, B, C)$ where

$$A = \frac{A_1 A_2}{S^2}, \quad B = B_2 + \frac{A_2}{S}[V(B_1 - B_2) - 4WC_2], \quad C = \frac{B^2 - \mathcal{D}}{4A}.$$

Remark 4.3. (a) In last definition, B is unique modulo A (c.f. [3]) satisfying

$$B \equiv B_1 \pmod{A_1/S}, \quad B \equiv B_2 \pmod{A_2/S}, \quad B^2 \equiv \mathcal{D} \pmod{A_1 A_2/S^2}.$$

(b) If f_1 and f_2 are primitive, then $f_1 \cdot f_2$ is also primitive.

Proposition 4.4. *Let $f_1 = (A_1, B_1, C_1)$ and $f_2 = (A_2, B_2, C_2)$ be two quadratic forms with discriminant $\mathcal{D}$. Assume that* $\gcd(A_1, A_2) = 1$. *If m_1 (resp. m_2) is represented by a binary quadratic form f_1 (resp. f_2), then $m_1 m_2$ is represented by $f_1 \cdot f_2$.*

Proof. Assume that $f_1 \cdot f_2 = (A, B, C)$ is defined as in Definition 4.2 and $m_1 = f_1(x, y)$, $m_2 = f_2(z, w)$ for $x, y, z, w \in \mathbf{A}$. By Remark 4.3(a), there are $Q, R \in \mathbf{A}$ such that $B = B_1 + A_1 Q$ and $B = B_2 + A_2 R$. It is easy to see that

$$f_1(x + \tfrac{Q}{2}y, y) f_2(z + \tfrac{R}{2}w, w) = (f_1 \cdot f_2)(xz - Cyw, A_1 xw + A_2 yz + Byw).$$

Hence

$$\begin{aligned} m_1 m_2 &= f_1(x, y) f_2(z, w) \\ &= (f_1 \cdot f_2)\big((x - \tfrac{Q}{2}y)(z - \tfrac{R}{2}w) - Cyw, A_1(x - \tfrac{Q}{2}y)w + A_2 y(z - \tfrac{R}{2}w) + Byw\big). \ \square \end{aligned}$$

If $m = Az^2 + Bzw + Cw^2$ and $a \in \mathbb{F}_q^\times$, then $am = aAz^2 + Bz(aw) + a^{-1}C(aw)^2$ which means that am is represented by $(aA, B, a^{-1}C)$. Hence, we only consider the representation for monic polynomials.

Definition 4.5. Let $\mathbf{b}_{\mathcal{D},q} \colon \mathbf{A}^+ \to \mathbb{R}$ be the characteristic function defined by

$$\mathbf{b}_{\mathcal{D},q}(m) = \begin{cases} 1 & \text{if } m \text{ is represented by a primitive quadratic form of discriminant } \mathcal{D}, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 4.6. (1) Observe that $\mathbf{b}_{\mathcal{D},q}(m^2) = 1$ and $\mathbf{b}_{\mathcal{D},q}(P) = 1$ for a monic irreducible polynomial $P \mid \mathcal{D}$ but $P^2 \nmid \mathcal{D}$ since P is represented by $\big(P, 0, \frac{-\mathcal{D}}{4P}\big)$.

(2) Let $P \in \mathbf{P}^+$. Then $\mathbf{b}_{\mathcal{D},q}(P) = 1$ implies $\mathbf{b}_{\mathcal{D},q}(P^i) = 1$ for all $i \geq 1$.

The following result is a corollary of Proposition 4.4.

Corollary 4.7. *Let $m_1, m_2 \in \mathbf{A}^+$ such that* $\gcd(m_1, m_2) = 1$. *Assume that $\mathbf{b}_{\mathcal{D},q}(m_1) = \mathbf{b}_{\mathcal{D},q}(m_2) = 1$. Then $\mathbf{b}_{\mathcal{D},q}(m_1 m_2) = 1$.*

Proof. Assume that $m \in \mathbf{A}$ such that $m = Ax^2 + Bxy + Cy^2$ for some $x, y \in \mathbf{A}$ and (A, B, C) is a primitive quadratic form of discriminant $\mathcal{D}$. Assume that $\gcd(x, y) = d$ and $x = x'd$, $y = y'd$. Then $m = (Ax'^2 + Bx'y' + Cy'^2)d^2$ and therefore $m' = m/d^2$ can be properly represented by (A, B, C). By Proposition 4.1, (A, B, C) is properly equivalent to the primitive quadratic form (m', n, l) for some $n, l \in \mathbf{A}$. Hence m can be represented by (m', n, l).

Assume that $m_1, m_2 \in \mathbf{A}$ with $\gcd(m_1, m_2) = 1$ and m_1, m_2 can be represented by primitive quadratic forms of discriminant $\mathcal{D}$. From about arguments, we may assume that m_i is represented by (m_i', n_i, l_i) where $m_i' \mid m_i$ and $n_i, l_i \in \mathbf{A}$ for $i = 1, 2$. By Proposition 4.4, $m_1 m_2$ can be represented by $(m_1', n_1, l_1) \cdot (m_2', n_2, l_2)$. $\square$

Lemma 4.8. *Let $P \in \mathbf{P}^+$ and $\left(\frac{\mathcal{D}}{P}\right) = 1$. Then $\mathbf{b}_{\mathcal{D},q}(P) = 1$.*

Proof. Since $\left(\frac{\mathcal{D}}{P}\right) = 1$, there is a $B \in \mathbf{A}$ such that $P \mid (B^2 - \mathcal{D})$. Hence $f = \left(P, B, \frac{B^2-\mathcal{D}}{4P}\right)$ is a primitive quadratic form of discriminant $\mathcal{D}$ and P is represented by f. □

Following the idea of James [7] and Pall [10, Section 5], we have the following lemmas.

Lemma 4.9. *Let $m, M \in \mathbf{A}^+$ and let P be any monic irreducible polynomial for which $\left(\frac{\mathcal{D}}{P}\right) = -1$. If $m = P^{2n+1}M$ where $n \in \mathbb{Z}_{\geq 0}$ and $P \nmid M$, then $\mathbf{b}_{\mathcal{D},q}(m) = 0$.*

Proof. Let $f = (A, B, C)$ be a primitive quadratic form of discriminant $\mathcal{D}$. We may assume $P \nmid A$. If $P \mid A$ and $P \nmid C$, then we may replace $f(x, y)$ by $f(-y, x)$ since properly equivalent forms represent the same polynomials. If $P \mid A$, $P \mid C$ and $P \nmid B$, then we replace $f(x, y)$ by $f(x, x + y)$.

Suppose that m is represented by $f = (A, B, C)$ with $P \nmid A$, which means $P^{2n+1}M = Az_0^2 + Bz_0w_0 + Cw_0^2$ for some $z_0, w_0 \in \mathbf{A}$. We shall show that this assumption leads to a contradiction. Multiplying $4A$ on both sides of the equation, we have

$$4AP^{2n+1}M = (2Az_0 + Bw_0)^2 - \mathcal{D}w_0^2$$

which implies

$$(2Az_0 + Bw_0)^2 \equiv \mathcal{D}w_0^2 \pmod{P}.$$

Since $\left(\frac{\mathcal{D}}{P}\right) = -1$, it follows that $P \mid w_0$ and $P \mid (2Az_0 + Bw_0)$ and therefore $P \mid z_0$ since $P \nmid A$. Thus one has

$$P^{2n-1}M = Az_1^2 + Bz_1w_1 + Cw_1^2,$$

where $w_0 = Pw_1$, $z_0 = Pz_1$. Repetition of this arguments leads to the equation

$$PM = Az_n^2 + Bz_nw_n + Cw_n^2$$

for some $z_n, w_n \in \mathbf{A}$. As before we have

$$(2Az_n + Bw_n)^2 \equiv \mathcal{D}w_n^2 \pmod{P},$$

and we find that $P \mid w_n$, $P \mid z_n$ which implies that $P^2 \mid PM$. This contradicts to $P \nmid M$. □

Lemma 4.10. *Let P be an irreducible polynomial such that $P^2 \mid \mathcal{D}$.*

(a) *If $P \nmid n$, then $\mathbf{b}_{\mathcal{D},q}(Pn) = 0$.*

(b) *$\mathbf{b}_{\mathcal{D},q}(P^2m) = 1$ if and only if $\mathbf{b}_{\mathcal{D}/P^2,q}(m) = 1$.*

Proof. (a) Assume that $f = (A, B, C)$ is a primitive quadratic form of discriminant $\mathcal{D}$ and $Pn = Ax^2 + Bxy + Cy^2$ for some $x, y \in \mathbf{A}$. Hence, we have

$$4APn = (2Ax + By)^2 - \mathcal{D}y^2$$

which implies

$$2Ax + By \equiv 0 \pmod{P}.$$

Since f is primitive, we may assume $P \nmid A$. Hence there is an $A' \in \mathbf{A}$ such that $2AA' \equiv 1 \pmod{P}$. There is a $z \in \mathbf{A}$ such that $x = -A'By + Pz$. Hence

$$\begin{aligned} Pn &= A(-A'By + Pz)^2 + B(-A'By + Pz)y + Cy^2 \\ &= AP^2z^2 + BP(-2AA' + 1)zy + (AA'^2B^2 - A'B^2 + C)y^2. \end{aligned}$$

Since $P \mid (-2AA' + 1)$ and $\mathcal{D} = B^2 - 4AC$ is divided by P, it is easy to see that $P \mid (AA'^2B^2 - A'B^2 + C)$. Put $(AA'^2B^2 - A'B^2 + C) = PR$ and $(-2AA' + 1) = PQ$ for some $Q, R \in \mathbf{A}$. We have

$$n = APz^2 + BPQzy + Ry^2.$$

Let $g = (AP, BPQ, R)$. The discriminant of g is $\mathcal{D}$. Since $P^2 \mid \mathcal{D}$ and $P \nmid A$, we have $P \mid R$. Therefore $P \mid n$. This contradicts to assumption.

(b) Following the ideal of (a), if we have P^2m is represented by a primitive quadratic form (A, B, C), then m is represented by a primitive quadratic form $(A, BQ, R/P)$ of discriminant $\mathcal{D}/P^2$. Conversely, if $m = ax^2 + bxy + cy^2$ for some primitive quadratic form (a, b, c) of discriminant $\mathcal{D}/P^2$. Since (a, b, c) is primitive, we may assume that $P \nmid a$. Then $P^2m = a(Px)^2 + bP(Px)y + cP^2y^2$. It is easy to see that (a, bP, cP^2) is primitive and its discriminant equals $\mathcal{D}$. □

Definition 4.11. Let P be an irreducible polynomial, $A \in \mathbf{A}$ and k be a positive integer. We say that $P^k||A$ if $P^k \mid A$ and $P^{k+1} \nmid A$.

From Lemmas 4.9, 4.10 and Remark 4.6, we have the following corollaries.

Corollary 4.12. *Let $P \in \mathbf{P}^+$ and $M \in \mathbf{A}^+$ such that $P \nmid M$.*

(a) *Assume that $P^{2k}||\mathcal{D}$ and $\mathcal{D} = P^{2k}\mathcal{D}'$. If $2i+1 < 2k$ or $\left(\frac{\mathcal{D}'}{P}\right) = -1$, then $\mathbf{b}_{\mathcal{D},q}(P^{2i+1}M) = 0$.*

(b) *Assume that $P^{2k+1}||\mathcal{D}$, then $\mathbf{b}_{\mathcal{D},q}(P^{2i+1}M) = 0$ for all $i < k$.*

Corollary 4.13. *Let $P \in \mathbf{P}^+$ and $k \in \mathbb{Z}_{\geq 0}$.*

(a) *Assume that $P^{2k}||\mathcal{D}$ and $\mathcal{D} = P^{2k}\mathcal{D}'$. If $\left(\frac{\mathcal{D}'}{P}\right) = 1$, then $\mathbf{b}_{\mathcal{D},q}(P^{2i+1}) = 1$ for all $i \geq k$.*

(b) *If* $P^{2k+1}||\mathcal{D}$, *then* $\mathbf{b}_{\mathcal{D},q}(P^{2i+1}) = 1$ *for all* $i \geq k$.

Combining the above results, we have the following proposition.

Proposition 4.14. *For any* $m \in \mathbf{A}^+$, *write* $m = P_1^{2r_1+1} \cdots P_s^{2r_s+1} N^2$ *where* P_i *are distinct and* $P_i \nmid N$ *for all* i. *Then* $\mathbf{b}_{\mathcal{D},q}(m) = 1$ *if and only if* P_i *satisfies one of the following properties for all* $1 \leq i \leq r$:

(i) $P_i \nmid \mathcal{D}$ *and* $\left(\frac{\mathcal{D}}{P_i}\right) = 1$,

(ii) $P_i^{2k_i+1}||\mathcal{D}$ *and* $r_i \geq k_i$,

(iii) $P_i^{2k_i}||\mathcal{D}$, $r_i \geq k_i$ *and* $\left(\frac{\mathcal{D}/P^{2k_i}}{P_i}\right) = 1$.

Theorem 4.15. *If* $\gcd(m, n) = 1$, *then* $\mathbf{b}_{\mathcal{D},q}(mn) = \mathbf{b}_{\mathcal{D},q}(m)\mathbf{b}_{\mathcal{D},q}(n)$.

Proof. By Corollary 4.7, $\mathbf{b}_{\mathcal{D},q}(m) = \mathbf{b}_{\mathcal{D},q}(n) = 1$ implies $\mathbf{b}_{\mathcal{D},q}(mn) = 1$.

Conversely, we assume $\mathbf{b}_{\mathcal{D},q}(m) = 0$. Since $\gcd(m, n) = 1$, we may write $m = P_1^{2r_1+1} \cdots P_s^{2r_s+1} M^2$ and $n = P_{s+1}^{2r_{s+1}+1} \cdots P_u^{2r_u+1} N^2$ where P_i are distinct and $P_i \nmid MN$. The assumption $\mathbf{b}_{\mathcal{D},q}(m) = 0$ implies that there is a P_i does not satisfy any condition of Proposition 4.14. Hence $\mathbf{b}_{\mathcal{D},q}(mn) = 0$ by Proposition 4.14. □

We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4. Define the counting function

$$\mathbf{B}_{\mathcal{D}}(n, q) := \sum_{f \in \mathbf{A}_n^+} \mathbf{b}_{\mathcal{D},q}(f)$$

for $n \in \mathbb{Z}_{\geq 0}$. Consider the generating function of $\mathbf{B}_{\mathcal{D}}(n, q)$:

$$F_{\mathcal{D}}(s) = \sum_{n=0}^{\infty} \mathbf{B}_{\mathcal{D}}(n, q) q^{-ns}.$$

Following Theorem 4.15, we can write $F_{\mathcal{D}}(s)$ as

$$F_{\mathcal{D}}(s) = \sum_{f \in \mathbf{A}^+} \mathbf{b}_{\mathcal{D},q}(f) q^{-\deg(f)s} = \prod_{P \in \mathbf{P}^+} \left(\sum_{i=0}^{\infty} \frac{\mathbf{b}_{\mathcal{D},q}(P^i)}{q^{i \deg(P)s}} \right).$$

From Lemmas 4.8, 4.9, Corollary 4.13 and Proposition 4.14, we have

$$F_{\mathcal{D}}(s) = \prod_{\substack{P \in \mathbf{P}^+ \\ \left(\frac{\mathcal{D}}{P}\right)=1}} (1 - \mathbf{q}_P^{-s})^{-1} \cdot \prod_{\substack{P \in \mathbf{P}^+ \\ \left(\frac{\mathcal{D}}{P}\right)=-1}} (1 - \mathbf{q}_P^{-2s})^{-1} \cdot \prod_{\substack{P \in \mathbf{P}^+ \\ P | \mathcal{D}}} \left(\sum_{i=0}^{\infty} \frac{\mathbf{b}_{\mathcal{D},q}(P^i)}{\mathbf{q}_P^{is}} \right).$$

For $P^2 \mid \mathcal{D}$, we write $\mathcal{D} = P^{2k_P}\mathcal{D}'$ where $k_P \geq 1$ and $P^2 \nmid \mathcal{D}'$. Then we can rewrite the last product of $F_{\mathcal{D}}(s)$ as

$$\prod_{\substack{P\in\mathbf{P}^+\\ P\mid\mathcal{D}}}\left(\sum_{i=0}^{\infty}\frac{\mathbf{b}_{\mathcal{D},q}(P^i)}{\mathbf{q}_P^{-is}}\right)=\prod_{\substack{P\in\mathbf{P}^+\\ P\|\mathcal{D}}}(1-\mathbf{q}_P^{-s})^{-1}\prod_{\substack{P\in\mathbf{P}^+\\ P^2\mid\mathcal{D}}}\big(1+\mathbf{q}_P^{-2s}+\cdots+\mathbf{q}_P^{(-2k_P+2)s}+\mathbf{q}_P^{-2k_Ps}\Lambda(s)\big),$$

where

$$\Lambda(s)=\begin{cases}(1-\mathbf{q}_P^{-s})^{-1} & \text{if } \left(\frac{\mathcal{D}'}{P}\right)=0 \text{ or } 1,\\ (1-\mathbf{q}_P^{-2s})^{-1} & \text{otherwise.}\end{cases}$$

Using the same arguments in Section 3, we have

$$F_{\mathcal{D}}(s)=\sqrt{\zeta_{\mathbf{A}}(s)}\cdot\sqrt{L\big(s,\left(\tfrac{\mathcal{D}}{\cdot}\right)\big)}\prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{\mathcal{D}}{P}\right)=-1}}(1-\mathbf{q}_P^{-2s})^{-1/2}\cdot\prod_{\substack{P\in\mathbf{P}^+\\ P\|\mathcal{D}}}(1-\mathbf{q}_P^{-s})^{-1/2}\cdot S(s),$$

where

$$S(s):=\prod_{\substack{P\in\mathbf{P}^+\\ P^2\mid\mathcal{D}}}(1-\mathbf{q}_P^{-s})^{1/2}\big(1+\mathbf{q}_P^{-2s}+\cdots+\mathbf{q}_P^{(-2k_P+2)s}+\mathbf{q}_P^{-2k_Ps}\Lambda(s)\big).$$

Write $F_{\mathcal{D}}(s)=\widehat{a}_{\mathcal{D},q}(s)\cdot\widehat{b}_q(s)$ where

$$\widehat{a}_{\mathcal{D},q}(s):=\sqrt{L\big(s,\left(\tfrac{\mathcal{D}}{\cdot}\right)\big)}\prod_{\substack{P\in\mathbf{P}^+\\ \left(\frac{\mathcal{D}}{P}\right)=-1}}(1-\mathbf{q}_P^{-2s})^{-1/2}\cdot\prod_{\substack{P\in\mathbf{P}^+\\ P\|\mathcal{D}}}(1-\mathbf{q}_P^{-s})^{-1/2}\cdot S(s)$$

and

$$\widehat{b}_q(s):=\sqrt{\zeta_{\mathbf{A}}(s)}=(1-q^{1-s})^{-1/2}.$$

We now consider $m=0$ in Theorem 2.4 with $F_{\mathcal{D}}(s)=\widehat{a}_{\mathcal{D},q}(s)\cdot\widehat{b}_q(s)$, $\alpha_0=1/2$, $\beta_0=1$ and $c=1/2$. When $m=0$ and any $0<\delta<1/2$, one has

$$\mathbf{B}_{\mathcal{D}}(n,q)=\widehat{a}_{\mathcal{D},q}(1)\binom{n-1/2}{n}q^n+O\left(\frac{q^{n-1/2+\delta}}{n^{3/2}}\right)\quad\text{as } q^n\to\infty,$$

where q varies under the condition that $\mathcal{D}$ is not perfect square in $\mathbb{F}_q[t]$. This completes the proof. □

References

[1] L. Bary-Soroker, Y. Smilansky and A. Wolf, *On the function field analogue of Landau's theorem on sums of squares*, Finite Fields Appl. **39** (2016), 195–215.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993.

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, John Wiley & Sons, New York, 1989.

[4] C. Friesen and P. van Wamelen, *Class numbers of real quadratic function fields*, Acta Arith. **81** (1997), no. 1, 45–55.

[5] O. Gorodetsky, *A polynomial analogue of Landau's theorem and related problems*, Mathematika **63** (2017), no. 2, 622–665.

[6] P. Henrici, *Applied and Computational Complex Analysis 2: Special functions—integral transforms—asymptotics—continued fractions*, A Wiley-Interscience Publication, John Wiley & Sons, New York, 1977.

[7] R. D. James, *The distribution of integers represented by quadratic forms*, Amer. J. Math. **60** (1938), no. 3, 737–744.

[8] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. (3) **13** (1908), 305–312.

[9] W. Leahey, *Sums of squares of polynomials with coefficients in a finite field*, Amer. Math. Monthly **74** (1967), no. 7, 816–819.

[10] G. Pall, *The structure of the number of representations function in a positive binary quadratic form*, Math. Z. **36** (1933), no. 1, 321–343.

[11] ———, *The distribution of integers represented by binary quadratic forms*, Bull. Amer. Math. Soc. **49** (1943), 447–449.

[12] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics **210**, Springer-Verlag, New York, 2002.

[13] D. Shanks, *The second-order term in the asymptotic expansion of $B(x)$*, Math. Comp. **18** (1964), 75–86.

[14] D. Shanks and L. P. Schmid, *Variations on a theorem of Landau I*, Math. Comp. **20** (1966), no. 96, 551–569.

[15] Q. Shen and S. Shi, *Function fields of class number one*, J. Number Theory **154** (2015), 375–379.

[16] A. Stein, *Explicit infrastructure for real quadratic function fields and real hyperelliptic curves*, Glas. Mat. Ser. III **44(64)** (2009), no. 1, 89–126.

Chih-Yun Chuang
AIMS, Taipei City 104, Taiwan
E-mail address: chihyun@am.is

Yen-Liang Kuan
National Center for Theoretical Sciences, Mathematics Division, Taipei City 10617, Taiwan
E-mail address: kuanyenliang@ncts.ntu.edu.tw

Wei-Chen Yao
Department of Mathematics, University of Taipei, Taipei City 10048, Taiwan
E-mail address: yao@utaipei.edu.tw