Proc. Indian Acad. Sci. (Math. Sci.) Vol. 123, No. 1, February 2013, pp. 1–18.

Divisibility of class numbers of imaginary quadratic function fields by a fixed odd number

PRADIPTO BANERJEE[1] and SRINIVAS KOTYADA[2]

[1]Indian Statistical Institute, Stat-Math Unit, 203 Barrackpore Trunk Road, Kolkata 700 108, India
[2]Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India
E-mail: pradipto.banerjee7@gmail.com; srini@imsc.res.in

MS received 23 August 2011; revised 24 January 2012

Abstract. In this paper we find a new lower bound on the number of imaginary quadratic extensions of the function field $\mathbb{F}_q(x)$ whose class groups have elements of a fixed odd order. More precisely, for q, a power of an odd prime, and g a fixed odd positive integer ≥ 3, we show that for every $\epsilon > 0$, there are $\gg q^{L(\frac{1}{2}+\frac{3}{2(g+1)}-\epsilon)}$ polynomials $f \in \mathbb{F}_q[x]$ with $\deg f = L$, for which the class group of the quadratic extension $\mathbb{F}_q(x, \sqrt{f})$ has an element of order g. This sharpens the previous lower bound $q^{L(\frac{1}{2}+\frac{1}{g})}$ of Ram Murty. Our result is a function field analogue which is similar to a result of Soundararajan for number fields.

Keywords. Divisibility; class numbers; quadratic extensions; function fields.

1. Introduction

For a square-free integer D, let $\mathrm{Cl}(-D)$ denote the ideal class group of $\mathbb{Q}(\sqrt{-D})$, and let $h(-D) = \#\mathrm{Cl}(-D)$ denote the class number. In his 1801 *Disquisitiones Arithmeticae*, Gauss put forward the problem of finding all positive square-free D such that $h(-D)$ is some fixed number C. Heegner [15], Baker [5] and Stark [25] solved Gauss's problem completely for $C = 1$. Subsequently, Baker [6] and Stark [26] provided solutions to the case $C = 2$. Recently, Watkins [27] extended the range of the complete solutions to Gauss's problem for $C \leq 100$.

A related problem of interest is to determine the existence of g-torsion subgroups of $\mathrm{Cl}(-D)$ for positive integers g. Gauss studied the case $g = 2$. Davenport and Heilbronn [10] proved that the proportion of D with $3 \nmid h(-D)$ is at least $1/2$. For any g the infinitude of such fields was established by Nagell [21], Honda [17], Ankeny and Chowla [3], Hartung [16], Yamamoto [30] and Weinberger [28].

For a positive integer g, let $N_g(X)$ denote the number of positive square-free $D \leq X$ such that $g|h(-D)$. Gauss's genus theory (see [7]) demonstrates that $2|h(-D)$ whenever D is a product of at least two odd prime numbers. This, in particular, implies that $N_2(X) \sim$

$6X/\pi^2$. In general, it is believed that $N_g(X) \sim C_g X$ for some positive constant C_g. For odd primes g, Cohen and Lenstra [8] conjectured that

$$C_g = \frac{6}{\pi^2}\left(1 - \prod_{i=1}^{\infty}\left(1 - \frac{1}{g^i}\right)\right).$$

Ankeny and Chowla [3] were among the first to achieve an estimate for $N_g(X)$ for $g \geq 3$. Although they did not explicitly point this out, their method shows that for $g \geq 3$, $N_g(X) \gg X^{1/2}$. Recently, Murty [20] improved this lower bound to $N_g(X) \gg X^{\frac{1}{2}+\frac{1}{g}}$, which was subsequently sharpened by Soundararajan [24] who showed

$$N_g(X) \gg \begin{cases} X^{\frac{1}{2}+\frac{2}{g}-\epsilon}, & \text{if } g \equiv 0 \text{ (mod4)} \\ X^{\frac{1}{2}+\frac{3}{g+2}-\epsilon}, & \text{if } g \equiv 2 \text{ (mod4)}. \end{cases}$$

For q, a power of an odd prime, we define $k := \mathbb{F}_q(x)$ to be the function field over the finite field $\mathbb{F}_q$ and $\mathcal{A} := \mathbb{F}_q[x]$, its ring of integers. For a square-free $f \in \mathcal{A}$, we will denote the quadratic field extension $k(\sqrt{f})$ by K, and its ring of integers $\mathcal{A}[\sqrt{f}]$ by $\mathcal{B}$. The function field analogue of the class number divisibility problem was initiated by Artin [4]. Friesen [13] constructed infinitely many polynomials $f \in \mathcal{A}$ of even degree such that the class groups for K have an element of order g where g is not divisible by q. In [19], Murty and Cardon proved that for $q \geq 5$ there are $\gg q^{L(\frac{1}{2}+\frac{1}{g})}$ polynomials $f \in \mathcal{A}$ with $\deg(f) \leq L$ such that the class groups for the quadratic extensions K have an element of order g, which is analogous to the result $N_g(X) \gg X^{\frac{1}{2}+\frac{1}{g}}$ of Murty [20]. Further, the lower bound of Murty and Cardon was extended by Pacelli [22] to $q^{L(\frac{1}{l}+\frac{1}{g})}$ for cyclic extensions $\mathbb{F}_q(x, \sqrt[l]{f})$ of $\mathbb{F}_q(x)$ where l is a prime dividing $q-1$. In [9], Chakraborty and Mukhopadhyay have shown that there are $\gg q^{L/2g}$ monic polynomials $f \in \mathcal{A}$ of even degree with $\deg(f) \leq L$ such that the ideal class group of the (real) quadratic extensions K have an element of order g. This is a function field analogue of Murty's result [20] $N_g(X) \gg X^{1/2g}$ for real quadratic number fields.

The case when $\deg f$ is odd is analogous to the case of an imaginary quadratic number field in which the prime at infinity ramifies and the unit group has rank 0. Recently, Merberg [18] used a function field analogue to the diophantine method of Soundararajan [24] for finding imaginary quadratic function fields whose class groups have elements of a given order. He further proved that if either $c = 4$, or c is any odd prime distinct from the characteristic, then there are infinitely many such fields whose class numbers are not divisible by c. Wong [29] gives a lower bound on the number of such pairwise distinct quadratic extensions whose class numbers are not divisible by c, in the case when c is an odd prime distinct from the characteristic. Precisely, he shows that if $L \geq 5$, then for any odd prime $c \nmid q$, there are at least $(\ln L)/(\ln 5) + 1$ pairwise coprime $D \in \mathbb{F}_q[x]$ which are square-free and of odd degree $\leq L$, such that c does not divide the class number of the imaginary quadratic fields $\mathbb{F}_q(x)(\sqrt{D})/\mathbb{F}_q(x)$.

Friedman and Washington [12] have studied the Cohen–Lenstra conjecture in the function field case, and Yu [31] has established the Cohen–Lenstra conjecture when the characteristic p of $\mathbb{F}_q$ tends to infinity for fixed discriminantal degree. For recent developments in this direction, the reader may refer to [1], [2] and [11]. In the present work, we follow the classical approach and obtain a lower bound on the number of imaginary quadratic function fields whose class groups have an element of order g for any odd $g \geq 3$. Specifically, we prove the following:

Theorem 1. *Let $g \geq 3$ be a fixed positive odd integer. Let q be a power of an odd prime. For odd L, let $N_g(L)$ denote the number of square-free polynomials $f \in \mathbb{F}_q[x]$ with $\deg f \leq L$ such that the class group of the quadratic extension $\mathbb{F}_q(x, \sqrt{f})$ contain an element of order g. Then, for sufficiently large L we have*

$$N_g(L) \gg q^{L(\frac{1}{2}+\frac{3}{2(g+1)}-\epsilon)}.$$

We will work with polynomials f with $\deg f = L$. This, however does not affect the statement of our result. We will use ideas from [24] to achieve our result. From our construction of the quadratic extensions of $\mathbb{F}_q(x)$ it will become evident that the case when $g \equiv 0 \pmod 4$ cannot be handled by our method. However, we remark that by a straightforward group theoretic argument and Theorem 1, a new lower bound when $g \equiv 2 \pmod 4$ can be achieved if one can first settle the function field analogue of Gauss's genus theory.

For basic function field related concepts, we refer the reader to [23]. We will denote by $\mathbb{F}_q^\times$ the multiplicative group of non-zero elements in $\mathbb{F}_q$. For an integer U, we let $\pi(U)$ count the number of irreducible monic polynomials of degree U. For a $f \in \mathcal{A}$, define the norm $|f|$ of f as $|f| := q^{\deg f}$, and let $\operatorname{sgn}(f)$ denote the leading coefficient of f. Let the Möbius function $\mu(f)$ be 0 if f is not square-free, and $(-1)^t$ if f is constant times a product of t distinct irreducible monic polynomials in $\mathcal{A}$. We will let $d(f)$ denote the number of distinct monic divisors of f (including $f/\operatorname{sgn} f$). We further define the Euler function $\phi(f)$ to be the order of the unit group $(\mathcal{A}/f\mathcal{A})^\times$ of the ring $\mathcal{A}/f\mathcal{A}$. It can be verified that

$$\phi(f) = |f| \prod_{p|f} \left(1 - \frac{1}{|p|}\right),$$

where the product is taken over irreducible monic polynomials. For a, b in $\mathcal{A}$, the symbol (a, b) will denote the greatest common monic divisor of a and b, and $\left(\frac{a}{b}\right)$ denotes the Jacobi symbol whenever relevant. For functions F and G, we will use the notation $F \asymp G$ whenever $F \gg\ll G$. Finally, we would like to point out to the reader that the ϵ's appearing at different places are different.

We prove our result by first giving a criteria for the existence of elements of order g in $\mathrm{Cl}(f)$, the class group of K. This will be achieved in § 2. In order to obtain the lower bound in the theorem, we need to count the number of square-free f meeting the divisibility criteria. We will do this in § 3. Sections 4 and 5 provide the technical details needed in § 3. The last section contains the conclusion of the proof.

2. A divisibility criteria for the class number of $\mathbb{F}_q(x, \sqrt{f})$

For an element $c + d\sqrt{f}$ in $\mathcal{B} = A[\sqrt{f}]$, with c, d in $\mathcal{A}$, define the norm $N(c + d\sqrt{f})$ of $c + d\sqrt{f}$ as

$$N(c + d\sqrt{f}) = (c + d\sqrt{f})(c - d\sqrt{f}) = c^2 - d^2 f \in \mathcal{A}.$$

For an ideal $\mathfrak{v}$ in $\mathcal{B}$, we consider the ideal $\mathfrak{u}$ in $\mathcal{A}$ generated by the set $\{N(a) : a \in \mathfrak{v}\}$. Since $\mathcal{A}$ is a principal ideal domain, the ideal $\mathfrak{u}$ is principal, say $\mathfrak{u} = (a)$, where $a \in \mathcal{A}$. We define the norm $N(\mathfrak{v})$ of the ideal $\mathfrak{v}$ to be $N(\mathfrak{v}) := |a| = q^{\deg a}$, where $|\cdot|$ is the usual norm of an element in $\mathcal{A}$ as defined earlier. We note that for a principal ideal $(c + d\sqrt{f})$ in $\mathcal{B}$, $N((c + d\sqrt{f})) = |N(c + d\sqrt{f})| = |c^2 - d^2 f| = q^{\deg(c^2 - d^2 f)}$.

In the following proposition, we construct quadratic extensions of k whose class groups contain an element of order g.

PROPOSITION 1

Let $g \geq 3$ be an odd integer. Let $f \in \mathcal{A}$ be a square-free polynomial of odd degree. If there exist nonzero $m, n, t \in \mathcal{A}$ such that $t^2 f = n^2 - m^g$ with $(m, n) = 1$ and $\deg m^g > \max\{\deg n^2, \deg t^4\}$, *then the class group for K has an element of order g.*

Proof. Suppose m, n and t exist as in the lemma. Rewriting $t^2 f = n^2 - m^g$ as $m^g = n^2 - t^2 f$, we see that the ideal $(m)^g$ factors in $\mathcal{B}$ as

$$(m)^g = (n + t\sqrt{f})(n - t\sqrt{f}).$$

We note that any common divisor $\mathfrak{d}$ of the ideals $(n + t\sqrt{f})$ and $(n - t\sqrt{f})$ contains $2n$. As 2 is a unit in $\mathcal{A}$, we deduce that $n \in \mathfrak{d}$. On the other hand, $\mathfrak{d}$ also contains m^g, but $(m^g, n) = 1$. Thus $\mathfrak{d} = \mathcal{B}$, that is the ideals $(n + t\sqrt{f})$ and $(n - t\sqrt{f})$ are co-prime in $\mathcal{B}$. Thus there exist ideals $\mathfrak{a}$ and $\mathfrak{a}'$ in $\mathcal{B}$ such that $(n + t\sqrt{f}) = \mathfrak{a}^g$ and $(n - t\sqrt{f}) = \mathfrak{a}'^g$.

We claim that the ideal class of $\mathfrak{a}$ has order g. Assume otherwise that there is a positive integer $r < g$ such that $\mathfrak{a}^r$ is principal, say $\mathfrak{a}^r = (u + v\sqrt{f})$ for some $u, v \in \mathcal{A}$. It is clear that $r|g$. Taking norms we have $N(\mathfrak{a})^r = q^{\deg(u^2 - v^2 f)}$. We also have $(n + t\sqrt{f}) = (u + v\sqrt{f})^{g/r}$. Since $t \neq 0$, it immediately follows that $v \neq 0$. Thus $v^2 f \neq 0$ has odd degree, and since u^2 has even degree, $\deg(u^2 - v^2 f) \geq \deg f$. Therefore $N(\mathfrak{a})^r = q^{\deg(u^2 - v^2 f)} \geq q^{\deg f}$. On the other hand,

$$N(\mathfrak{a})^g = q^{\deg(n^2 - t^2 f)} = q^{\deg m^g} = q^{g \deg m}.$$

Thus $N(\mathfrak{a}) = q^{\deg m}$.

Now from $q^{r \deg m} = N(\mathfrak{a})^r \geq q^{\deg f}$ we see that

$$r \deg m \geq \deg f = \deg\left(\frac{n^2 - m^g}{t^2}\right) = g \deg m - 2 \deg t. \tag{1}$$

The last equality above follows from our assumption that $\deg m^g > \max\{\deg n^2, \deg t^4\}$. Rearranging terms in inequality (1), we have $\deg m \leq \frac{2 \deg t}{g - r}$. But from our assumption that $\deg m^g > \deg t^4$, it now follows that

$$\frac{4 \deg t}{g} < \deg m \leq \frac{2 \deg t}{g - r},$$

giving rise to $\frac{g}{r} < 2$, thereby contradicting the fact that $r|g$ since $g \geq 3$. This proves our claim and hence the proposition. □

3. Counting square-free f

In this section we shall obtain a lower bound on the number of square-free $f \in \mathcal{A}$ meeting the criteria of Proposition 1. The bound obtained in this section will depend on some parameter T to be determined in § 6 (see eq. (22)).

Thus we will be interested in counting the number of square-free polynomials $f \in \mathcal{A}$ satisfying

$$n^2 - m^g = t^2 f, \quad (m, n) = 1 \quad \text{and} \quad \deg m^g > \max\{n^2, t^4\}. \tag{2}$$

Let $\deg m = M$, $\deg n = N$, $\deg t = T$ and $\deg f = L$. In view of Proposition 1, we assume that

$$T < L/2, \quad Mg = 2T + L \quad \text{and} \quad N = T + \frac{L}{2} - 1. \tag{3}$$

From the above choice of M, N and T it follows that

$$Mg > \max\{2N, 4T\},$$

that is $\deg m^g > \max\{n^2, t^4\}$. Thus if f admits a solution to (2), then by Proposition 1, $\mathrm{Cl}(f)$ has an element of order g.

Let $N_g(L, T)$ count the number of square-free f with $\deg f = L$ satisfying (2). For a square-free polynomial $f \in \mathcal{A}$ of degree L, let $\mathcal{R}(f)$ denote the number of solutions in monic m, n and t to (2). If we define the characteristic function $\chi(f)$ as

$$\chi(f) = \begin{cases} 0, & \text{if } \mathcal{R}(f) = 0, \\ 1, & \text{if } \mathcal{R}(f) \neq 0, \end{cases}$$

then we can write $N_g(L, T)$ as

$$N_g(L, T) = \sum_{\deg f = L} \chi(f).$$

By the Cauchy–Schwarz inequality, we have

$$\left(\sum_{\deg f = L} \chi(f)^2 \right) \left(\sum_{\deg f = L} \mathcal{R}(f)^2 \right) \geq \left(\sum_{\deg f = L} \chi(f)\mathcal{R}(f) \right)^2,$$

which can be rewritten as

$$N_g(L, T) \geq \left(\sum_{\deg f = L} \mathcal{R}(f) \right)^2 \left(\sum_{\deg f = L} \mathcal{R}(f)^2 \right)^{-1}. \tag{4}$$

Thus, in order to determine a lower bound on $N_g(L, T)$, we need to establish a lower bound on $(\sum_{\deg f = L} \mathcal{R}(f))^2$ and an upper bound on $\sum_{\deg f = L} \mathcal{R}(f)^2$.

In the next section we will obtain the lower bound on $(\sum_{\deg f = L} \mathcal{R}(f))^2$ by establishing the following lemma.

Lemma 1. $\sum_{\deg f=L} \mathcal{R}(f) \asymp q^{M+N-T}$.

By a counting argument, we will show in § 5 the following lemma.

Lemma 2. $\sum_{\deg f=L} \mathcal{R}(f)(\mathcal{R}(f)-1) \ll q^{\epsilon L+2M+2T}$ *for every* $\epsilon > 0$ *and* $L \gg_\epsilon 0$.

Below we demonstrate how Lemmas 1 and 2 give a lower bound on $N_g(L, T)$. Observe that

$$\sum_{\deg f=L} \mathcal{R}(f)^2 = \sum_{\deg f=L} \mathcal{R}(f)(\mathcal{R}(f)-1) + \sum_{\deg f=L} \mathcal{R}(f) \ll q^{M+N-T} + q^{\epsilon L+2M+2T}.$$

Thus

$$\sum_{\deg f=L} \mathcal{R}(f)^2 \ll q^{\epsilon L+2M+2T} \tag{5}$$

provided

$$M + N - T \leq \epsilon L + 2M + 2T. \tag{6}$$

Therefore, from (4), (5) and Lemma 1 we have

$$N_g(L, T) \gg \frac{q^{2(M+N-T)}}{q^{\epsilon L+2M+2T}} = q^{2N-4T-\epsilon L}.$$

Putting the value of N from (3) we get

$$N_g(L, T) \gg q^{L-2T-2-\epsilon L} \gg q^{L-2T-\epsilon L}. \tag{7}$$

The inequality in (6) and the lower bound in Theorem 1 will be achieved by suitably choosing the parameter T in § 6.

4. Proof of Lemma 1

Let $(m, n, t) \in \mathcal{A}^3$ be a tuple of pairwise relatively prime monic polynomials with $\deg m = M$, $\deg n = N$ and $\deg t = T$ satisfying $n^2 \equiv m^g (\mathrm{mod}\ t^2)$, and M, N and T are as in (3). We define sets $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$ of such tuples $(m, n, t) \in \mathcal{A}^3$ as follows:

$$\mathcal{S}_1 = \left\{(m, n, t) : p^2 \nmid \frac{n^2 - m^g}{t^2} \text{ for all monic primes } p \text{ with } \deg\ p \leq \log L\right\},$$

$$\mathcal{S}_2 = \left\{(m, n, t) : p^2 \,\Big|\, \frac{n^2 - m^g}{t^2} \text{ for some monic primes } p \text{ with } \log L < \deg\ p \leq Q\right\}$$

and

$$\mathcal{S}_3 = \left\{(m, n, t) : p^2 \,\Big|\, \frac{n^2 - m^g}{t^2} \text{ for some monic primes } p \text{ with } Q < \deg p\right\}.$$

Here logarithms are taken to the base q, and Q is some real parameter to be described below.

Let $N_i = |\mathcal{S}_i|$ for $i = 1, 2, 3$. Note that $N_g(L, T) \geq N_1 - N_2 - N_3$. Thus in order to obtain a lower bound on $N_g(L, T)$, we would want N_1 to be large compared to $N_2 + N_3$. In other words, the sum we desire is $N_1 + O(N_2 + N_3)$. We shall show below that by optimally choosing $Q := (L - T + 2\log L)/3$, one obtains

$$N_1 \asymp q^{M+N-T} + o(q^{M+\frac{L}{3}+\frac{2T}{3}}),$$
$$N_2 \ll q^{M+N-T}/L + o(q^{M+\frac{L}{3}+\frac{2T}{3}})$$

and

$$N_3 = o(q^{M+\frac{L}{3}+\frac{2T}{3}}),$$

where q is fixed in the above $o(\cdot)$ notation. Observe that for $L > 4T + 6$, it follows from (3) that $M + N - T \geq M + (L/3) + (2T/3)$, and hence $N_1 \asymp q^{M+N-T}$, and N_2, N_3 are small. The choice of T as in eq. (22), and by taking $L > 2(g + 1)$, it is ensured that $L > 4T + 6$. Thus it follows that

$$\sum_{\deg f = L} R(f) \asymp q^{M+N-T}.$$

Estimation of N_1. For a fixed monic m and t with $\deg m = M$ and $\deg t = T$, we count the number of monic polynomials n with $\deg n = N$ such that $n^2 \equiv m^g (\bmod\ t^2)$, and p^2 does not divide $\frac{n^2-m^g}{t^2}$ for all irreducible monic p with $\deg p \leq \log L$.

Let $\rho_m(l)$ denote the number of solutions (mod l) to the congruence $n^2 \equiv m^g (\bmod\ l)$. It is worth noting that $\rho_m(l)$ is a multiplicative function of l, and if $p \nmid m$ is irreducible, then for $\alpha \geq 1$ one has

$$\rho_m(p^\alpha) = \rho_m(p) = 1 + \left(\frac{m^g}{p}\right) = 1 + \left(\frac{m}{p}\right), \tag{8}$$

as g is odd.

Set $P = \prod_{\deg p \leq \log L} p$, where the product is taken over all irreducible monic polynomials p. Thus, the sum $\sum_{l^2|(f,P^2)} \mu(l) = 1$ or 0 depending on whether $p^2 \nmid f$ for all p with $\deg p \leq \log L$ or not. Here l is assumed to be monic. Thus in order to estimate N_1, the sum over n (with m and t fixed), what we seek is

$$\sum_{\substack{\deg n = N \\ n^2 \equiv m^g (\bmod\ t^2) \\ (n,m)=1}} \sum_{l^2 | \left(\frac{n^2-m^g}{t^2}, P^2\right)} \mu(l) = \sum_{\substack{l | P \\ (l,m)=1}} \mu(l) \sum_{\substack{\deg n = N \\ n^2 \equiv m^g (\bmod\ l^2 t^2)}} 1. \tag{9}$$

If $N \geq \deg l^2 t^2$, then for fixed l we have

$$\sum_{\substack{\deg n = N \\ n^2 \equiv m^g (\bmod\ l^2 t^2)}} 1 = \frac{q^N}{|l^2 t^2|} \rho_m(l^2 t^2) = \frac{q^{N-2T} \rho_m(l^2 t^2)}{|l^2|},$$

while if $N \leq \deg l^2 t^2$ then

$$\sum_{\substack{\deg n = N \\ n^2 \equiv m^g (\bmod\ l^2 t^2)}} 1 \leq \rho_m(l^2 t^2).$$

Thus the sum in (9) is

$$\begin{aligned}
&\sum_{\substack{\deg n=N\\ n^2\equiv m^g \pmod{t^2}\\ (n,m)=1}} \sum_{l^2|\left(\frac{n^2-m^g}{t^2},P^2\right)} \mu(l)\\
&\quad = \sum_{\substack{l|P\\(l,m)=1}} \mu(l)\frac{q^N}{|l^2t^2|}\rho_m(l^2t^2) + O\left(\sum_{\substack{l|P\\(l,m)=1}} \rho_m(l^2t^2)\right)\\
&\quad = q^{N-2T}\rho_m(t^2) \sum_{\substack{l|P\\(l,m)=1}} \frac{\mu(l)}{|l|^2}\rho_m(l/(l,t)) + O\left(\sum_{\substack{l|P\\(l,m)=1}} \rho_m(l^2t^2)\right),
\end{aligned}$$

which can be written as

$$q^{N-2T}\rho_m(t^2) \prod_{\substack{p|P\\ p\text{-monic}\\ (p,m)=1}} \left(1-\frac{\rho_m\big(p/(p,t)\big)}{|p|^2}\right) + O\left(\sum_{\substack{l|P\\(l,m)=1}} \rho_m(l^2t^2)\right), \tag{10}$$

where the product is taken over irreducible monic polynomials p.

We trivially see that

$$\prod_{\substack{p|P\\ p\text{-monic}\\ (p,m)=1}} \left(1-\frac{\rho_m\big(p/(p,t)\big)}{|p|^2}\right) < 1.$$

Also, it can be seen from $\rho_m(p/(p,t)) = 1 + \left(\frac{m}{p}\right) \leq 2$ that

$$\begin{aligned}
\prod_{\substack{p|P\\ p\text{-monic}\\ (p,m)=1}} \left(1-\frac{\rho_m(p/(p,t))}{|p|^2}\right) &\geq \prod_{\substack{\text{all } p\\ p\text{-monic}}} \left(1-\frac{2}{|p|^2}\right)\\
&= \prod_{\substack{\text{all } p\\ p\text{-monic}}} \left(1-\frac{1}{|p|^2}\right)^2\left(1+\frac{1}{|p|^2(|p|^2-2)}\right)^{-1}.
\end{aligned}$$

Now, for $x > 2$ we have

$$\left(1+\frac{1}{x(x-2)}\right) = \frac{(x-1)^2}{x(x-2)} \leq \frac{x^2}{x(x-1)} = \left(1-\frac{1}{x}\right)^{-1}.$$

Since $|p| > 2$, we have

$$\prod_{\substack{p|P\\ p\text{-monic}\\ (p,m)=1}} \left(1-\frac{\rho_m(p/(p,t))}{|p|^2}\right) \geq \prod_{\substack{\text{all } p\\ \text{p-monic}}} \left(1-\frac{1}{|p|^2}\right)^3 = \zeta_{\mathcal{A}}(2)^{-3} = \left(1-\frac{1}{q}\right)^3.$$

We have used $\zeta_{\mathcal{A}}(s) = \frac{1}{1-q^{1-s}}$ above. This may easily be derived by looking at the series expansion of $\zeta_{\mathcal{A}}(s)$ (see [23]). Therefore the main term in (10) is $\asymp q^{N-2T}\rho_m(t^2)$. For the error term in (10), we first note from (8) that

$$\rho_m(l^2t^2) = \rho_m(lt) = \prod_{p|lt} \rho_m(p) = \prod_{p|lt}\left(1 + \left(\frac{m}{p}\right)\right) \le \prod_{p|lt} 2 \le d(lt).$$

As l^2t^2 divides $n^2 - m^g$, we have from (3) that

$$2\deg l + 2\deg t \le Mg = L + 2T = L + 2\deg t.$$

Therefore $\deg l \le L/2$. Also from (3) we have $\deg t = T < L/2$. Hence $\deg lt \le L$.

For a polynomial $r(x) \in \mathcal{A}$ with $\deg r \le X$, it is an easy exercise to show that $d(r) = O(q^{\epsilon X})$, where the O-constant depends on ϵ only (see pages 260–262 of [14] for the classical divisor function). Therefore,

$$\rho_m(l^2t^2) \le d(lt) = O(q^{\epsilon L}). \tag{11}$$

Thus the error term in (10) is $O(d(P)q^{\epsilon L})$. Now,

$$d(P) = 2^{\pi(1)+\pi(2)+\cdots+\pi(\log L)} \le 2^{q+\frac{q^2}{2}+\cdots+\frac{q^{\log L}}{\log L}} \ll 2^{\frac{L}{\log L}},$$

for all sufficiently large L. Here we have used that $\pi(U) \le q^U/U$ for all $U \in \mathbb{N}$ (see Proposition 2.1 of [23]). Thus the error term in (10) is $O(q^{\epsilon L})$. Therefore, the sum in (9) is

$$\asymp q^{N-2T}\rho_m(t^2) + O(q^{\epsilon L}).$$

Now, summing over all monic m with $\deg m = M$, and monic t with $\deg t = T$ we have

$$N_1 \asymp q^{N-2T} \sum_{\substack{\deg m=M \\ \deg t=T}} \rho_m(t^2) + O(q^{\epsilon L+M+T}). \tag{12}$$

We now show that the error term in (12) is $o(q^{M+\frac{L}{3}+\frac{2T}{3}})$. We choose $0 < \delta < \frac{1}{2}$ so that $q^{L/2} = o(q^{L(1-\delta)})$. Since we have $T < L/2$ from (3), hence $q^T < q^{L/2} = o(q^{L(1-\delta)})$.

Taking $\epsilon = \frac{\delta}{3}$, we have $q^{T/3} = o(q^{L/3}q^{-\epsilon L})$, that is $q^{\epsilon L} = o(q^{L/3}q^{-T/3})$.

Thus from (12) we have

$$N_1 \asymp q^{N-2T} \sum_{\substack{\deg m=M \\ \deg t=T}} \rho_m(t^2) + o(q^{M+\frac{L}{3}+\frac{2T}{3}}). \tag{13}$$

We next show that

$$\sum_{\substack{\deg m=M \\ \deg t=T}} \rho_m(t^2) \asymp q^{M+T}.$$

In order to prove this result we will need a couple of lemmas. The following lemma is an easy exercise (see Ex. 12, page 20 of [23]).

Lemma 3. *For an integer $U \ge 2$, we have*

$$\sum_{\substack{y\text{-monic} \\ \deg y=U}} \mu(y) = 0.$$

The next lemma is based upon Lemma 17.10, Proposition 17.11 and Proposition 17.12 of [23] which we state without proof as follows.

Lemma 4. *Suppose* $b \notin \mathbb{F}_q^\times$ *is not a square in* $\mathcal{A}$, *and let* $\deg b = B$. *Then*

(i) *for* $D \geq B$,

$$\sum_{\substack{a\text{-monic} \\ \deg a = D}} \left(\frac{b}{a}\right) = 0.$$

(ii) *For* $1 \leq D \leq B - 1$,

$$\sum_{\substack{b\text{-monic} \\ \deg b = B}} \sum_{\substack{a\text{-monic} \\ \deg a = D}} \left(\frac{b}{a}\right) = (q-1)\Phi(D/2, M),$$

where

$$\Phi(D/2, M) = \begin{cases} \left(1 - \frac{1}{q}\right) q^{M + D/2}, & \text{if } D \equiv 0 \pmod 2, \\ 0, & \text{if } D \equiv 1 \pmod 2. \end{cases}$$

We are now ready to estimate the average value of $\rho_m(t^2)$.

Lemma 5. *Assume that* m *and* $t \in A$ *are monic and relatively prime. Then we have*

$$\sum_{\deg m = M} \sum_{\deg t = T} \rho_m(t^2) = q^{M+T} + O(q^{M/2+T}).$$

Proof. Since $\rho_m(\cdot)$ is multiplicative and $\rho_m(p^\alpha) = \rho_m(p)$ for any irreducible $p \in \mathcal{A}$ and $\alpha \geq 1$, we have the following product to sum formula for $\rho_m(t^2)$.

$$\rho_m(t^2) = \rho_m(t) = \prod_{p|t} \left(1 + \left(\frac{m}{p}\right)\right) = \sum_{d|t} \mu^2(d) \left(\frac{m}{d}\right).$$

We derive our result by showing that the main contribution in the above sum comes from $d = 1$. For $d = 1$, the sum over t, we are interested in

$$\begin{aligned} \sum_{\substack{\deg t = T \\ (t,m)=1}} 1 &= \sum_{\substack{\deg t = T \\ s|t}} \sum_{s|m} \mu(s) = \sum_{s|m} \mu(s) \sum_{\substack{\deg t = T \\ s|t}} 1 \\ &= \sum_{s|m} \mu(s) \sum_{\substack{l \\ ls = t}} 1 = \sum_{s|m} \mu(s) \sum_{\substack{l \\ \deg l = T - \deg s}} 1 \\ &= \sum_{s|m} \mu(s) q^{T - \deg s} = q^T \prod_{p|m} \left(1 - \frac{1}{q^{\deg p}}\right) \\ &= q^T \frac{\phi(m)}{|m|} = q^{T-M} \phi(m). \end{aligned}$$

Now summing over m, and using Proposition 2.7 of [23] we have

$$q^{T-M} \sum_{\deg m = M} \phi(m) = q^{T-M} \cdot q^{2M}\left(1 - \frac{1}{q}\right).$$

Thus the contribution from $d = 1$ is indeed $\asymp q^{M+T}$.

We next demonstrate that the contribution from $d \neq 1$ is $O(q^{M/2+T})$. The sum we seek to bound is

$$\sum_{\deg m = M} \sum_{\substack{\deg t = T \\ (t,m)=1}} \sum_{\substack{d \mid t \\ d \neq 1}} \mu^2(d)\left(\frac{m}{d}\right).$$

Let us denote $\deg d$ by Z. We split the above sum into $1 \leq Z \leq M$ and $Z \geq M + 1$, where $M = \deg m$. The sum corresponding to $1 \leq Z \leq M$ (after changing the order of summation) is

$$\sum_{\substack{\deg t = T \\ (t,m)=1}} \sum_{\substack{d \mid t \\ Z \leq M}} \mu^2(d) \sum_{\deg m = M} \left(\frac{m}{d}\right).$$

Observe that if d is a square then $\mu^2(d) = 0$, and if d is not a square, then from quadratic reciprocity law we have

$$\left(\frac{m}{d}\right)\left(\frac{d}{m}\right) = (-1)^{\frac{q-1}{2}(\deg m)(\deg d)} \operatorname{sgn}(m)^{\deg d} = (-1)^{\frac{q-1}{2}MZ}.$$

Since $d \neq 1$, Lemma 4 implies that

$$\sum_{\deg m = M} \left(\frac{m}{d}\right) = (-1)^{\frac{q-1}{2}MZ} \sum_{\deg m = M} \left(\frac{d}{m}\right) = 0$$

for $\deg d = Z \leq M$. So the sum over $1 \leq Z \leq M$ is 0.

Consider the sum over $Z \geq M + 1$,

$$\begin{aligned}
&\sum_{\deg m = M} \sum_{\substack{\deg t = T \\ (t,m)=1}} \sum_{\substack{d \mid t \\ M+1 \leq Z \leq T}} \mu^2(d)\left(\frac{m}{d}\right) \\
&\quad = \sum_{\deg m = M} \sum_{M+1 \leq Z \leq T} \sum_{\substack{\deg d = Z \\ (d,m)=1}} \mu^2(d)\left(\frac{m}{d}\right) q^{T-Z} \\
&\quad = q^T \sum_{M+1 \leq Z \leq T} q^{-Z} \sum_{\deg m = M} \sum_{\substack{\deg d = Z \\ (d,m)=1}} \mu^2(d)\left(\frac{m}{d}\right).
\end{aligned}$$

Since $\left(\frac{m}{d}\right) = 0$ when $(d, m) \neq 1$, we can ignore the condition $(d, m) = 1$ in the above summation. Let us denote the inner sum by

$$S := \sum_{\deg m = M} \sum_{\deg d = Z} \mu^2(d)\left(\frac{m}{d}\right).$$

We write $d = l^2 s$. Further without loss of generality, we assume that l and s are monic. Observe that for monic d and m we have by quadratic reciprocity law that

$$\left(\frac{m}{d}\right)\left(\frac{d}{m}\right) = (-1)^{\frac{q-1}{2}(\deg m)(\deg d)} = (-1)^{\frac{q-1}{2}MZ}.$$

Noting that $d = l^2 s$ we have from above that

$$\left(\frac{m}{d}\right)\left(\frac{s}{m}\right) = (-1)^{\frac{q-1}{2}MZ}.$$

Similarly, for monic m and s we have

$$\left(\frac{m}{s}\right)\left(\frac{s}{m}\right) = (-1)^{\frac{q-1}{2}(\deg m)(\deg s)} = (-1)^{\frac{q-1}{2}M(Z-2\deg l)} = (-1)^{\frac{q-1}{2}MZ},$$

since q is odd. Therefore, $\left(\frac{m}{d}\right) = \left(\frac{m}{s}\right)$. Now using $\sum_{l^2|d} \mu(d) = \mu^2(d)$, we have

$$\begin{aligned} S &= \sum_{\deg m=M} \sum_{\deg d=Z} \sum_{l^2|d} \mu(l)\left(\frac{m}{s}\right) \\ &= \sum_{\deg m=M} \sum_{\deg l\leq \frac{Z}{2}} \mu(l) \sum_{\deg s=Z-2\deg l} \left(\frac{m}{s}\right) \end{aligned}$$

If $\deg l = Z/2$, then $s = 1$. For such l, the corresponding contribution in S is

$$\sum_{\deg m=M} \sum_{\deg l=\frac{Z}{2}} \mu(l).$$

For $Z \geq 2$, the sum $\sum_{\deg l=\frac{Z}{2}} \mu(l)$ is zero by Lemma 3. Since $Z \geq M+1 > 2$, we deduce that the contribution in S corresponding to $s = 1$ is 0. Therefore,

$$\begin{aligned} S &= \sum_{\deg m=M} \sum_{\deg l<\frac{Z}{2}} \mu(l) \sum_{\substack{\deg s=Z-2\deg l \\ s\neq 1}} \left(\frac{m}{s}\right) \\ &= \sum_{\deg l<\frac{Z}{2}} \mu(l) \sum_{\deg m=M} \sum_{\substack{\deg s=Z-2\deg l \\ s\neq 1}} \left(\frac{m}{s}\right), \end{aligned}$$

which is

$$\leq \sum_{\deg l<\frac{Z}{2}} \left| \sum_{\deg m=M} \sum_{\substack{\deg s=Z-2\deg l \\ s\neq 1}} \left(\frac{m}{s}\right) \right|. \tag{14}$$

Observe that since m satisfies equation (2), and since we have assumed that $\deg f$ and g are odd in (2), m cannot be a square in $\mathcal{A}$. Also $\deg m = M > 1$ implies that $m \notin \mathbb{F}_q^\times$. Thus appealing to the first part of Lemma 4 we deduce that if $M \leq Z - 2\deg l$, then

$$\sum_{\substack{\deg s=Z-2\deg l \\ s\neq 1}} \left(\frac{m}{s}\right) = 0,$$

while if $M \geq Z - 2\deg l$, then from the second part of Lemma 4 we have

$$\sum_{\deg m = M} \sum_{\substack{\deg s = Z - 2\deg l \\ s \neq 1}} \left(\frac{m}{s}\right) \leq \left(1 - \frac{1}{q}\right) q^{\frac{Z}{2} - \deg l + M}.$$

Summing over l in (14) we deduce that $S \leq q^{M + \frac{Z}{2}}$. Thus the contribution from $d \neq 1$ is less than

$$q^{M+T} \sum_{Z \geq M+1} q^{-Z/2} = q^{M+T} q^{-\frac{M+1}{2}} \left(1 - \frac{1}{\sqrt{q}}\right)^{-1} = O(q^{M/2+T}).$$

This completes the proof of the lemma. □

As an immediate consequence of Lemma 5, from (13) we have

$$N_1 \asymp q^{M+N-T} + o(q^{M + \frac{L}{3} + \frac{2T}{3}}).$$

Estimation of N_2. In order to estimate N_2, once again, we fix m and t and count the number of n with $\deg n = N$ such that $\frac{n^2 - m^g}{t^2}$ divisible by p^2 for some prime p with $\log L < \deg p \leq Q = \frac{L - T + 2\log L}{3}$. Therefore the sum over n that we seek is

$$\sum_{\log L < \deg p \leq Q} \sum_{\substack{\deg n = N \\ n^2 \equiv m^g \pmod{p^2 t^2}}} 1. \tag{15}$$

Following the same line of argument as in the estimation of N_1 we deduce that the sum in (15) is equal to

$$\sum_{\log L < \deg p \leq Q} \left(\frac{q^N \rho_m(p^2 t^2)}{|p^2 t^2|} + O(\rho_m(p^2 t^2))\right). \tag{16}$$

Since $\rho_m(p/(p,t)) \leq 2$, the main term in (16) is

$$\begin{aligned}
&q^{N-2T} \rho_m(t^2) \sum_{\log L < \deg p \leq Q} \frac{\rho_m(p/(p,t))}{|p|^2} \\
&\leq q^{N-2T} \rho_m(t^2) \sum_{\log L \leq \deg p \leq Q} \frac{2}{|p|^2} = 2q^{N-2T} \rho_m(t^2) \sum_{Y = \log L}^{Q} \sum_{\deg p = Y} \frac{1}{|p|^2} \\
&= 2q^{N-2T} \rho_m(t^2) \sum_{Y = \log L}^{Q} q^{-2Y} \sum_{\deg p = Y} 1 = 2q^{N-2T} \rho_m(t^2) \sum_{Y = \log L}^{Q} q^{-2Y} \pi(Y) \\
&\leq 2q^{N-2T} \rho_m(t^2) \sum_{Y = \log L}^{Q} q^{-2Y} q^Y / Y \\
&\leq \frac{2q^{N-2T} \rho_m(t^2)}{\log L} \sum_{Y = \log L}^{Q} q^{-Y} \leq \frac{2q^{N-2T} \rho_m(t^2)}{q^{\log L} \log L} \left(1 - \frac{1}{q}\right)^{-1} \\
&= \frac{2q^{N-2T} \rho_m(t^2)}{L \log L} \left(1 - \frac{1}{q}\right)^{-1} \ll \frac{q^{N-2T} \rho_m(t^2)}{L}.
\end{aligned}$$

From

$$\rho_m(p^2t^2) = \rho_m(t^2)\rho_m(p^2/(p,t)^2) = \rho_m(t^2)\rho_m(p/(p,t)) \le 2\rho_m(t^2),$$

we deduce that the remainder term in (16) is

$$O\left(\rho_m(t^2) \sum_{\log L < \deg p \le Q} 1\right). \tag{17}$$

Now,

$$\sum_{\log L < \deg p \le Q} 1 \le \sum_{D=\log L}^{Q} \frac{q^D}{D}.$$

It can be easily seen that

$$\sum_{D=\log L}^{Q} \frac{q^D}{D} \ll q^Q/Q.$$

Now,

$$\frac{q^Q}{Q} = \frac{q^{L/3}q^{-T/3}q^{2\log L/3}}{\frac{L}{3} - \frac{T}{3} + \frac{2\log L}{3}} = \frac{3q^{L/3}q^{-T/3}L^{2/3}}{L(1 - \frac{T}{L} + \frac{2\log L}{L})}.$$

In the end we will take T to be a constant (< 1) multiple of L. For such choice of T, we have from above that

$$\frac{q^Q}{Q} \ll q^{L/3}q^{-T/3}L^{-1/3} = o(q^{L/3}q^{-T/3}).$$

Using this estimate in (17) we deduce that the remainder term in (16) is $o(q^{L/3}$ $q^{-T/3}\rho_m(t^2))$.

Therefore the sum over n in (15) is

$$\sum_{\log L < \deg p \le Q} \sum_{\substack{\deg n = N \\ n^2 \equiv m^g (\text{mod } p^2t^2)}} 1 \ll \frac{q^{N-2T}\rho_m(t^2)}{L} + o(q^{L/3}q^{-T/3}\rho_m(t^2)). \tag{18}$$

Summing over all monic m and t in (18) with $\deg m = M$ and $\deg t = T$, and using Lemma 5 we get

$$N_2 \ll \frac{q^{M+N-T}}{L} + o(q^{M+\frac{L}{3}+\frac{2T}{3}}).$$

Estimation of N_3. If (m, n, t) is a tuple counted in N_3, then

$$n^2 - m^g = \beta p^2 t^2, \tag{19}$$

for some monic prime p with $\deg p > Q$ and some $\beta \in \mathcal{A}$. Clearly, $\deg \beta < L - 2Q = (L + 2T - 4\log L)/3$. As m, n and t are monic and pairwise relatively prime, for fixed

m and β with $\deg m = M$, and $\deg \beta < L - 2Q$, the number of monic n and t satisfying (19) is bounded by the number of solutions to the equation

$$m^g = x^2 - \beta y^2 \tag{20}$$

with x and y monic and co-prime. Assuming that such x and y exists, the ideal $(m)^g$ factors in $\mathcal{A}[\sqrt{\beta}]$ as

$$m^g = (x + y\sqrt{\beta})(x - y\sqrt{\beta}).$$

Working similarly as in Proposition 1, it can be seen that any common factor of the ideals $(x + y\sqrt{\beta})$ and $(x - y\sqrt{\beta})$ contains m^g and x. But $(m^g, x) = 1$ as x and y are co-prime, hence any common factor of $(x + y\sqrt{\beta})$ and $(x - y\sqrt{\beta})$ must be the whole ring $\mathcal{A}[\sqrt{\beta}]$. Therefore the ideals $(x + y\sqrt{\beta})$ and $(x - y\sqrt{\beta})$ are co-prime. From unique factorization of ideals of $\mathcal{A}[\sqrt{\beta}]$ we have

$$(x + y\sqrt{\beta}) = \mathfrak{a}^g \quad \text{and} \quad (x - y\sqrt{\beta}) = \bar{\mathfrak{a}}^g,$$

for some ideal $\mathfrak{a}$ and its conjugate $\bar{\mathfrak{a}}$ in $\mathcal{A}[\sqrt{\beta}]$. Thus the number of solutions in x and y to (20) is bounded by the number of factorizations of the ideal (m) into the product $\mathfrak{a}\bar{\mathfrak{a}}$. It can be easily verified that the number of such factorizations of the ideal (m) in $\mathcal{A}[\sqrt{\beta}]$ is $\leq d(m)$. Thus for fixed m and β, the number of choices for n and t satisfying (19) is $\leq d(m)$. From Proposition 2.5 of [23] it follows that $\sum_{\substack{m\text{-monic}\\ \deg m = M}} d(m) = q^M(M+1)$. Therefore N_3 is $\leq$ (number of choices of β)$\Big(\sum_{\substack{m\text{-monic}\\ \deg m = M}} d(m)\Big)$ which is

$$\begin{aligned}
&\leq (1 + q + q^2 + \cdots + q^{L-2Q}) \sum_{\substack{m\text{-monic}\\ \deg m = M}} d(m)\\
&= \frac{(q^{L-2Q+1} - 1)}{q - 1} q^M(M+1)\\
&\leq q^{L-2Q+1} q^M (M+1)\\
&= q \cdot q^{(L+2T-4\log L)/3} q^M (M+1)\\
&= q^{L/3} q^{2T/3} q^M q L^{-4/3} (M+1).
\end{aligned}$$

Noting from (3) that $M < L$, we conclude

$$N_3 \leq q^{L/3} q^{2T/3} q^M q L^{-4/3}(M+1) \leq q^{L/3} q^{2T/3} q^M q L^{-1/3} = o(q^{M + \frac{L}{3} + \frac{2T}{3}}),$$

as desired.

5. Proof of Lemma 2

Let $\mathcal{S}$ denote the set of monic tuples $(m_1, n_1, t_1; m_2, n_2, t_2)$ such that $\dfrac{n_1^2 - m_1^g}{t_1^2} = \dfrac{n_2^2 - m_2^g}{t_2^2}$ with $\deg m_i = M$, $\deg n_i = N$, $\deg t_i = T$; $(m_i, n_i) = (m_i, t_i) = 1$, and $(m_1, n_1, t_1) \neq (m_2, n_2, t_2)$. It can be seen that for a square-free f, if (m_1, n_1, t_1) and

(m_2, n_2, t_2) are solutions to equation (2) of § 3, then $(m_1, n_1, t_1; m_2, n_2, t_2) \in \mathcal{S}$. For a fixed square-free f, the number of such tuples is $\mathcal{R}(f)\big(\mathcal{R}(f)-1\big)$. Thus

$$\sum_{\deg f = L} \mathcal{R}(f)\big(\mathcal{R}(f)-1\big) \le |\mathcal{S}|.$$

For $(m_1, n_1, t_1; m_2, n_2, t_2) \in \mathcal{S}$ we have

$$t_2^2(n_1^2 - m_1^g) = t_1^2(n_2^2 - m_2^g).$$

Rearranging we have

$$(t_1n_2 + t_2n_1)(t_1n_2 - t_2n_1) = t_1^2 m_2^g - t_2^2 m_1^g.$$

Since $\deg(t_1^2 m_2^g - t_2^2 m_1^g) \le Mg + 2T < 3L$, for a fixed m and t, the number of choices for n_1 and n_2 is bounded by $d(t_1^2 m_2^g - t_2^2 m_1^g)$, provided $t_1^2 m_2^g \neq t_2^2 m_1^g$. However, if $t_1^2 m_2^g = t_2^2 m_1^g$, then from $(m_i, t_i) = 1$ and since g is odd, we have $t_1 = t_2$, $m_1 = m_2$, and consequently $n_1 = n_2$, contradicting the fact that $(m_1, n_1, t_1) \neq (m_2, n_2, t_2)$. Now $d(t_1^2 m_2^g - t_2^2 m_1^g) = O(q^{\epsilon L})$.

Thus summing over m_i and t_i for $i = 1, 2$ we have

$$\begin{aligned}\sum_{\deg f = L} \mathcal{R}(f)\big(\mathcal{R}(f)-1\big) &\le \sum_{\deg m_i = M} \sum_{\deg t_i = T} d(t_1^2 m_2^g - t_2^2 m_1^g)\\ &\ll q^{\epsilon L} \sum_{\deg m_i = M} \sum_{\deg t_i = T} 1\\ &= q^{\epsilon L + 2M + 2T}.\end{aligned}$$

6. Proof of Theorem 1

In this section we first determine a suitable optimal value of the parameter T so that the inequality (6) is justified.

Substituting the values of M and N from (3) in (6) and rearranging the terms we obtain

$$T/L \ge \frac{(g-2)}{4(g+1)} - \frac{\epsilon g}{2(g+1)}. \tag{21}$$

Thus in view of (21), the obvious optimal choice for T/L is

$$T/L = \frac{g-2}{4(g+1)}.$$

Therefore we take

$$T = \frac{L(g-2)}{4(g+1)}. \tag{22}$$

Now substituting the value of T from (22) in (7), we conclude that the number of solutions to equation (2) is

$$\gg q^{L(\frac{1}{2} + \frac{3}{2(g+1)} - \epsilon)}.$$

Therefore, it follows from Proposition 1 that

$$N_g(L) \gg q^{L(\frac{1}{2}+\frac{3}{2(g+1)}-\epsilon)},$$

and this completes the proof of the Theorem 1.

Acknowledgments

The authors would like to thank Prof. Jeffrey Achter for suggestions and especially for bringing their attention to [1], [2] and [11]. The authors are indebted to Professors M Ram Murty and K Soundararajan for their comments on an earlier version of this paper. The authors would also like to thank the anonymous referee for carefully going through the manuscript and suggesting important changes for a better presentation.

References

[1] Achter J D, The distribution of class groups of function fields, *J. Pure Appl. Algebra* **204** (2006) 316–333

[2] Achter J D, Results of Cohen-Lenstra type for quadratic function fields, Computational arithmetic geometry, 1–7, Contemp. Math. 463, Amer. Math. Soc., Providence, RI (2008)

[3] Ankeny N and Chowla S, On the divisibility of class numbers of quadratic fields, *Pacific J. Math.* **5** (1955) 321–324

[4] Artin E, Quadratische Körper im Gebiet der höheren Kongruenzen I, II, *Math. Zeitschrift* **19** (1924) 153–246

[5] Baker A, Linear forms in the logarithms of algebraic numbers. I, II, III, *Mathematica* **13** (1966) 204–216; *ibid.* **14** (1967) 102–107; *ibid.* **14** (1967) 220–228

[6] Baker A, Imaginary quadratic fields with class number 2, *Ann. Math.* **2** (1971) 139–152

[7] Borevich Z I and Shafarevich I R, Number Theory (1966) (London: Academic Press Inc.)

[8] Cohen H and Lenstra H W Jr, Heuristics on class groups of number fields, Lecture Notes in Mathematics **1068** (1984) (Springer) pp. 33–62

[9] Chakraborty K and Mukhopadhyay A, Exponents of class groups of real quadratic function fields, *Proc. Am Math. Soc.* **132** (2004) 1951–1955

[10] Davenport H and Heilbronn H, On the density of discriminants of cubic fields, II, *Proc. R. Soc. London Ser. A* **322** (1971) 405–420

[11] Ellenberg J S, Venkatesh A and Westerland C, Homological Stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, preprint 2009, arXiv:0912.0325v2 [math.NT]

[12] Friedman E and Washington L C, On the distribution of divisor class groups of curves over finite fields, in: Thèorie des nombres Quebec, PQ 1987 (1989) (Berlin: de Gruyter) pp. 227–239

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

[14] Hardy H and Wright E M, An Introduction to the theory of numbers (2008) (Oxford: Oxford University Press)

[15] Heegner K, Diophantische Analysis und Modulfunktionen, *Math. Zeitschrift* **56** (1952) 227–253

[16] Hartung P, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, *J. Number Theory* **6** (1974) 276–278

[17] Honda T, A few remarks on class numbers of imaginary quadratic fields, *Osaka. J. Math* **12** (1975) 19–21

[18] Merberg A, Divisibility of class numbers of imaginary quadratic function fields, *Involve* **1** (2008) 47–58

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

[20] Murty M R, Exponents of class groups of quadratic fields, Topics in number theory, Mathematics and its applications **467** (1997) (Dordrecht: Kluwer Academic) pp. 229–239

[21] Nagell T, Über die Klassenzahl imaginär quadratischer Zahlkörpar, *Abh. Math. Seminar Univ. Hamburg* **1** (1922) 140–150

[22] Pacelli A M, A lower bound on the number of cyclic function fields with class number divisible by n, *Canad. Math. Bull.* **49** (2006) 448–463

[23] Rosen M, Number Theory in Function Fields, GTM (2002) (New York: Springer-Verlag)

[24] Soundararajan K, Divisibility of class numbers of imaginary quadratic fields, *J. London. Math. Soc.* **61** (2000) 681–690

[25] Stark H M, A complete determination of the complex quadratic fields with class-number one, *Michigan Math. J.* **14** (1967) 1–27

[26] Stark H M, On complex quadratic fields with class-number two, *Math. Comp.* **29** (1975) 289–302

[27] Watkins M, Class numbers of imaginary quadratic fields, *Math. Comp.* **73** (2004) 907–938

[28] Weinberger P, Real quadratic fields with class number divisible by n, *J. Number Theory* **5** (1973) 237–241

[29] Wong S, Class number indivisibility for quadratic function fields, *J. Number Theory* **130** (2010) 2332–2340

[30] Yamamoto Y, On ramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970) 57–76

[31] Yu J-K, Toward the Cohen-Lenstra conjecture in the function field case, preprint 1997, http://www.math.purdue.edu/~jyu/preprints.php