ON PROPORTIONAL CONSTANTS OF THE MEAN VALUE OF CLASS NUMBERS OF QUADRATIC EXTENSIONS

TAKASHI TANIGUCHI

Abstract. In this article, we give a refinement of the mean value theorem for the class number of quadratic extensions obtained by Goldfeld-Hoffstein and Datskovsky. More specifically, we determine the proportional constants of the mean value for fields that satisfy any local conditions including wild ramification at places dividing 2.

1. Introduction

For a number field $k$ let $h_k$ and $R_k$ be the class number and the regulator, respectively. For a finite extension $F/k$ of number fields, let $\mathcal{N}(\Delta_{F/k})$ be the absolute norm of the relative discriminant. In this article, we will give a refinement of Datskovsky’s mean value theorem of $h_FR_F$ with respect to $\mathcal{N}(\Delta_{F/k})$ for certain families of quadratic extensions $F$ of a fixed number field $k$. Our main theorem is Theorem 3.2.

The roots of this topic go back to Gauss. Let $h_d$ be the number of $\text{SL}(2,\mathbb{Z})$-equivalence classes of primitive integral binary quadratic forms which are either positive definite or indefinite. In [G, Sections 302, 304] Gauss gives without proof (conjectures in modern terms) the average value for $h_d$. This conjecture was first proved by Lipschitz for the imaginary case, and by Siegel for the real case. Siegel also proved a density theorem for integral equivalence classes of quadratic forms in general.

M. Sato and T. Shintani formulated these kinds of density problems using the notion of prehomogeneous vector spaces. In [Sh] Shintani considered the zeta functions associated with the space of quadratic forms. There he reproved the density theorem for the case of binary quadratic forms and improved the error estimate. However, in Gauss’ conjecture all integers $d$ are allowed, and if $d = m^2d'$ and $d'$ is a square-free integer, then $h_d$ and $h_{d'}$ are related by a simple relation. Therefore we are counting essentially the same object infinitely many times. This ambiguity was first removed by Goldfeld and Hoffstein. In [GH], they give the mean value of $h_kR_k$ of quadratic fields $k$ by using Eisenstein series of half-integral weight.

Later Datskovsky investigated this subject from the point of view of prehomogeneous vector spaces. He constructed the necessary local theory and combined it with Shintani’s global theory [Sh]. He then generalized the Goldfeld-Hoffstein mean value theorem to quadratic extensions of an arbitrary fixed number field.
the proof [D], he also showed the existence of a mean value for the family of quadratic extensions which have a given local behavior at a finite number of places of $k$ and computed the proportional constants of the mean value explicitly for many types of local conditions. However, Datskovsky ran into some difficulty computing the proportional constants for quadratic ramified extensions, especially in the case of wild ramification at dyadic places (those dividing the place of $\mathbb{Q}$ at 2). Instead of computing individual constants, he gave the sum of proportional constants over certain arithmetically similar conditions. The purpose of this article is to determine each unevaluated proportional constant to complete Datskovsky’s work.

We follow Datskovsky’s approach. Our method is a natural modification of Kable and Yukie [KY], in which another prehomogeneous vector space is handled and a new mean value theorem is obtained. In [T] we find a mean value of $h$ and Yukie, in which another prehomogeneous vector space is handled and another field $k$. For a finite set $X$ we denote by $\#X$ its cardinality. The standard symbols $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}$ will denote respectively the set of rational, real and complex numbers and rational integers. If $V$ is a scheme defined over a ring $R$ and $S$ is an $R$-algebra, then $V_S$ denotes its $S$-rational points. For a finite field extension $L/F$, let $N\langle L/F \rangle$ denote the norm map.

The contents of this article are as follows. In Section 2 we recall the definition of the space of binary quadratic forms and review its fundamental properties. For later purposes, we define the representation over any ring. In Section 3 we first state the main theorem of this article, which is a refinement of Datskovsky’s mean value theorem [D]. After that we discuss the relation between the space of binary quadratic forms and the main theorem and point out what our remaining task is. This reduces the problem to determining certain orbital volumes in a vector space over a non-archimedean local field. The explicit computation of the volume is carried out in the final section.

Notation. For a finite set $X$ we denote by $\#X$ its cardinality. The standard symbols $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}$ will denote respectively the set of rational, real and complex numbers and rational integers. If $V$ is a scheme defined over a ring $R$ and $S$ is an $R$-algebra, then $V_S$ denotes its $S$-rational points. For a finite field extension $L/F$, let $N\langle L/F \rangle$ denote the norm map.

2. Review of the space of binary quadratic forms

In this section, we briefly review the space of binary quadratic forms. Let $G = \text{GL}(1) \times \text{GL}(2)$ and $V = \text{Sym}^2 \text{Aff}^2$. We consider the natural action of $\text{GL}(2)$ on $V$. We define the action of $\text{GL}(1)$ on $V$ by the usual scalar multiplication. This defines a representation of $G$ on $V$. We regard $V$ as the space of binary quadratic forms of the variables $v = (v_1, v_2)$. Elements of $V$ are expressed in the form

$$x = x(v) = x(v_1, v_2) = x_0v_1^2 + x_1v_1v_2 + x_2v_2^2.$$ 

For the rest of this paper, we express elements of $G$ as

$$g = (t, g_2), \quad t \in \text{GL}(1), \quad g_2 = \begin{pmatrix} g_{211} & g_{212} \\ g_{221} & g_{222} \end{pmatrix} \in \text{GL}(2).$$

Then the action of $g$ is given by $x(v) \mapsto tx(vg_2)$, regarding $v$ as a row vector.

Let $P(x) = x_1^2 - 4x_0x_2$, the discriminant of $x(v)$. Let $\chi_i$ ($i = 1, 2$) be characters on $G$ defined by $\chi_1(g) = t$, $\chi_2(g) = \det(g_2)$, respectively. We define the character $\chi$ on $G$ by $\chi = \chi_1\chi_2$. Then $P$ becomes a relative invariant polynomial with respect to the character $\chi^2$; i.e., $P(gx) = (\chi(g))^2 P(x)$ for all $g \in G, x \in V$. If $x$ is a rational point of $V$, we can consider the stabilizer of $x$ as a group scheme, in the sense of [GIT, p.3]. We denote this group scheme by $G_x$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Let $x = v_1^2 + a_1 v_1 v_2 + a_2 v_2^2$ be a rational point of $V$. For these forms of $x$, we put
\[
A_x(c, d) = \begin{pmatrix} c & d \\ -a_2d & c + a_1d \end{pmatrix}
\]
and then define the subgroup $N_x$ of $G$ by
\[
N_x = \{ n_x(c, d) = (\det(A_x(c, d))^{-1}, A_x(c, d)) \mid A_x(c, d) \in \GL(2) \}.
\]
By computation, one could see that $N_x$ is a subgroup of $G_x$.

We now consider the representation $(G, V)$ over a fixed field $K$. Let $V_K^s = \{ x \in V \mid P(x) \neq 0 \}$ and call it the set of semi-stable points. By definition, $x \in V_K^s$ is an element of $V_K^s$ if and only if $x(v)$ has distinct roots in $\mathbb{P}^1_K$.

**Definition 2.1.** For $x \in V_K^s$, we define
\[
Z_x = \Proj K[v_1, v_2]/(x(v)),
\]
\[
K(x) = \Gamma(Z_x, \mathcal{O}_{Z_x}).
\]

Note that $K(x)$ may not be a field. Since $V_K^s$ is the set of $x$ such that $F_x$ does not have a multiple root, $Z_x$ is a reduced scheme over $k$ and $K(x)$ is a separable quadratic algebra over $K$. Also note that if $x(v)$ is irreducible over $K$, then $K(x)$ is the splitting field of $x(v)$. The following proposition is easy to see, and we omit the proof.

**Proposition 2.2.** The map $x \mapsto K(x)$ gives a bijection between the set of rational orbits $G_k \backslash V_K^s$ and the set of equivalence classes of separable quadratic algebras over $K$.

**Remark 2.3.** For $x \in V_K^s$, the identity component of the stabilizer of $x$, denoted by $G_x^s$, is isomorphic to $R_{K(x)/K}(\mathbb{G}_m)$, the scalar restriction of $\mathbb{G}_m$ with respect to $K(x)/K$. Hence if $K$ is a number field and $K(x)$ is a quadratic extension of $K$, then the unnormalized Tamagawa number of $G_x^s$ is a constant multiple of $h_{K(x)}R_{K(x)}$, and this is the reason why the study of the representation $(G, V)$ leads to the mean value theorem of the class number times the regulator of quadratic extensions.

The proof of the following proposition is straightforward, and we omit the details.

**Proposition 2.4.** Let $x = v_1^2 + x_1 v_1 v_2 + x_2 v_2^2 \in V_K^s$ be an irreducible form over $k$ and $x = (v_1 + \alpha_1 v_2)(v_1 + \alpha_2 v_2)$ for $\alpha_1, \alpha_2 \in K(x)$. Then the map
\[
\psi_{x,K} : N_x K \longrightarrow K(x)^\times \quad \text{as} \quad n_x(c, d) \mapsto c + \alpha_1 d
\]
gives an isomorphism of these groups. Moreover the following diagram is commutative:
\[
\begin{array}{ccc}
N_x K & \xrightarrow{\chi_2} & K^\times \\
\psi_{x,K} \downarrow & & \downarrow \\
K(x)^\times & \xrightarrow{N_{K(x)/K}} & K^\times
\end{array}
\]
Note that in the case of the proposition above, $N_x$ coincides with the identity component of the stabilizer $G_x$ as an algebraic group over $K$. 

---

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
3. The mean value theorem

In this section, we state the main theorem of this article, which is a refinement of Datskovsky’s \([D]\). After that, we point out the remaining task. The explicit computations are done in the next section.

To state the main theorem, we prepare some notation. For the rest of this paper we fix a number field \(k\). Let \(\mathfrak{M}, \mathfrak{M}_\infty, \mathfrak{M}_f, \mathfrak{M}_S\) and \(\mathfrak{M}_C\) denote respectively the set of all places of \(k\), all infinite places, all finite places, all real places and all complex places. We let \(r_1, r_2, h_k, R_k\) and \(\epsilon_k\) be respectively the number of real places, the number of complex places, the class number, the regulator and the number of roots of unity contained in \(k\). We set \(\xi_k = 2^{s_1}(2\pi)^{r_2}h_kR_k\epsilon_k^{-1}\). We denote by \(\zeta_k(s)\) the Dedekind zeta function of \(k\). For \(v \in \mathfrak{M}\) let \(k_v\) denote the completion of \(k\) at \(v\) and \(|\cdot|_v\) the normalized absolute value of \(k_v\). For \(v \in \mathfrak{M}_f\), we denote by \(q_v\) the cardinality of the residue field at \(v\). For a finite extension \(L_v/k_v\) at \(v \in \mathfrak{M}_f\), let \(\Delta_{L_v/k_v}\) denote the relative discriminant of \(L_v\) over \(k_v\).

Let \(S \supset \mathfrak{M}_\infty\) be a finite set of places. We consider \(S\)-tuples \(L_S = (L_v)_{v \in S}\) where each \(L_v\) is a separable quadratic algebra over \(k_v\). Let \(F\) be a quadratic extension of \(k\). We write \(F \cong L_v\) to mean that \(F \otimes_k k_v\) is isomorphic to \(L_v\) as a \(k_v\)-algebra. For \(L_S = (L_v)_{v \in S}\) we shall write \(F \cong L_S\) if and only if \(F \cong L_v\) for all \(v \in S\). For \(v \in \mathfrak{M}\) and \(L_v\) a separable quadratic algebra over \(k_v\), we define the constant \(\epsilon_v(L_v)\) as follows.

**Definition 3.1.** (1) If \(v \in \mathfrak{M}_f\), then we put

\[
\epsilon_v(L_v) = \begin{cases} 
2^{-1}(1 - q_v^{-2}) & L_v \cong k_v \times k_v, \\
2^{-1}(1 - q_v^{-1})^2 & L_v \text{ is quadratic unramified}, \\
2^{-1}\Delta_{L_v/k_v}|v^{-1}(1 - q_v^{-1})(1 - q_v^{-2}) & L_v \text{ is quadratic ramified}.
\end{cases}
\]

(2) For \(v \in \mathfrak{M}_R\), we define \(\epsilon_v(L_v) = 1/4\) if \(L_v \cong \mathbb{R} \times \mathbb{R}\), and \(\epsilon_v(L_v) = 1/(2\pi)\) if \(L_v \cong \mathbb{C}\).

(3) For \(v \in \mathfrak{M}_C\), we define \(\epsilon_v(L_v) = 1/(4\pi^2)\).

Let \(N(\Delta_{F/k})\) denote the absolute norm of the relative discriminant \(\Delta_{F/k}\) of \(F/k\). Then the following, a refinement of \([D]\), is the main result of this article.

**Theorem 3.2.** Let \(S \supset \mathfrak{M}_\infty\) and \(L_S = (L_v)_{v \in S}\) be an \(S\)-tuple. Then we have

\[
\lim_{X \to \infty} \frac{1}{X^{3/2}} \sum_{\substack{[F:k]=2, \, F \cong L_S, \\
N(\Delta_{F/k}) \leq X}} h_F R_F = \frac{\epsilon_k \xi_k^2 \zeta_k(2)}{3 \cdot 2^{s_1+r_2-1}} \prod_{v \in S} \epsilon_v(L_v) \prod_{v \in \mathfrak{M}\setminus S} (1 - q_v^{-2} - q_v^{-3} + q_v^{-4}).
\]

The contribution of this article is that we determine the constant \(\epsilon_v(L_v)\) for \(v \in \mathfrak{M}_f\) and \(L_v\) a quadratic ramified extension solely, whereas in \([D]\), the sum of \(\epsilon_v(L_v)\) for \(L_v\)’s with the same relative discriminants were calculated.

We will discuss the relation between the prehomogeneous vector space \((G, V)\) and the constant \(\epsilon_v(L_v)\). For the rest of this article we assume \(v \in \mathfrak{M}_f\). We denote by \(O_v\) the integer ring of \(k_v\). We consider the prehomogeneous vector space \((G, V)\) over \(O_v\) and over \(k_v\). Let \(\mathcal{K}_v = G_{O_v}\), which is the standard maximal compact subgroup of \(G_{k_v}\). On \(V_{k_v}\) we consider the additive Haar measure under which \(\text{vol}(V_{O_v}) = 1\).

As in Proposition 2.2 the set of rational orbits \(G_{k_v}/V_{k_v}^{ss}\) corresponds bijectively to the set of separable quadratic \(k_v\)-algebras. Following \([D]\) we select and fix a representative element from each orbit.
**Definition 3.3.** For each of the $G_{k_v}$-orbits in $V_{k_v}^{ss}$, we choose and fix an element $x$ as follows.

1. For the orbit corresponding to the algebra $k_v \times k_v$, we set $x = v_1v_2$.
2. For any orbit corresponding to a quadratic ramified extension $L$, set $x = N_{L/k_v}(v_1 + \theta v_2)$, where $\theta$ is a generator of the integer ring $O_L$ of $L$ over $O_v$.

We call such fixed orbital representatives the standard orbital representatives.

Note that if $x \in V_{k_v}^{ss}$ is a standard representative, then $P(x)$ generates the relative discriminant $\Delta_{k_v(x)/k_v}$.

Let $x \in V_{k_v}^{ss}$ be any standard representative. Datskovsky showed in [D] that $v_i(k(x)) = \text{vol}(K_v)$. He then computed $\text{vol}(K_v)$ if $x$ corresponds to $k_v \times k_v$ or to the quadratic unramified extension, and $\sum_x \text{vol}(K_v)$ where $x$ runs through all standard representatives corresponding to quadratic extensions with the given relative discriminant $\Delta_{k_v(x)/k_v}$. Hence, to obtain Theorem 3.2 we will determine the value $\text{vol}(K_v)$ for each standard representative $x$ corresponding to a quadratic ramified extension. Since the value for $v \notin M_{dy}$ is given in [D] without a proof, we choose to carry out the computation for any $v \in M$.

4. THE ORBITAL VOLUMES

Let $v$ be an arbitrary finite place. In this section, we compute the volume $\text{vol}(K_v)$ for standard representatives $x$ corresponding to quadratic extensions. Our purpose in this section is to prove the following.

**Proposition 4.1.** Let $x \in V_{k_v}^{ss}$ be one of the standard representatives corresponding to quadratic ramified extensions. Then $$\text{vol}(K_v) = 2^{-1}|\Delta_{k_v(x)/k_v}| v_f^{-1}(1 - q_v^{-1})(1 - q_v^{-2}).$$

For the rest of this section we drop the subscript $v$ from $K_v, O_v$ and write $K, O$ instead. We denote by $p$ the prime ideal of $O$. We consider the cases $v \notin M_{dy}$ and $v \in M_{dy}$ simultaneously. Let $\text{ord}_v: k_v^* \to \mathbb{Z}$ be the normalized discrete valuation.

We put $m = \text{ord}_v(2)$. Note that $m = 0$ if $v \notin M_{dy}$.

Let $x = v_1^2 + a_1v_1v_2 + a_2v_2^2 \in V_{k_v}^{ss}$ be a standard representative corresponding to a quadratic ramified extension. In this case $x(v_1, 1)$ is an Eisenstein polynomial, i.e., $a_1 \in p$ and $a_2 \in p \setminus p^2$. We put $\Delta_{k_v(x)/k_v} = p^{\delta_x}$. By definition, $\delta_x = 2\text{ord}_v(a_1)$ if $1 \leq \text{ord}_v(a_1) \leq m$ and $\delta_x = 2m + 1$ if $\text{ord}_v(a_1) \geq m + 1$. Hence $\delta_x$ takes one of the values $2, 4, \ldots, 2m, 2m + 1$ (in the case $v \notin M_{dy}$ and hence $m = 0$). $\delta_x$ only takes the value 1.

Let $x = N_{k_v(x)/k_v}(v_1 + \omega v_2)$. Then $\omega$ is a prime element of the ring of integers $O_{k_v(x)}$ of $k_v(x)$.

Let $i$ be a positive integer. For an $O$-scheme $X$, let $\tau_{X,i}$ denote the reduction map $X_O \to X_{O/p^i}$. If the situation is obvious we drop $X$ and write $\tau_i$ instead. For rational points $y_1, y_2 \in X_O$, we use the notation $y_1 \equiv y_2 (p^i)$ if $\tau_i(y_1) = \tau_i(y_2)$. This coincides with the classical notation.

We put $n = \delta_x + 2m + 1$. To compute $\text{vol}(K_x)$ we consider congruence relations modulo $p^n$ of the representation $(G_O, V_O)$.

**Definition 4.2.** We define $D_x = \{ y \in V_O \mid y \equiv x (p^n) \}$.

**Lemma 4.3.** We have $D_x \subset Kx$. 


Proof. Let \( y \in D_x \). First we show \( y \in G_{k_v}x \). Since \( y \equiv x \mod (p^n) \) and \( \text{ord}_v(P(x)) = \delta_x \), we have \( P(y)/P(x) \equiv 1 \mod (p^{2m+1}) \) and so \( P(y)/P(x) \in (k_v^n)^2 \). Therefore the splitting fields of \( x(v) \) and \( y(v) \) coincide and hence by Proposition 4.6 we may assume that \( y \in G_{k_v}x \). Let \( y = gx, g = (t, g_2) \in G_{k_v} \). Note that \( |\chi(g)|_v = |t \det(g_2)|_v = 1 \) since \( |P(x)|_v = |P(y)|_v \). By Proposition 4.4 multiplying \( g \) by an element of \( N_{x k_v} \) if necessary, we may assume that
\[
|t|_v = | \det(g_2) |_v = 1.
\]
Then since \( y(v) \in \text{Sym}^2 \mathcal{O}^2 \), we have
\[
y(1, 0) = tN_{k_v(x)/k_v}(g_{211} + g_{212} \varpi) \in \mathcal{O},
\]
\[
y(0, 1) = tN_{k_v(x)/k_v}(g_{221} + g_{222} \varpi) \in \mathcal{O}.
\]
Hence both \( N_{k_v(x)/k_v}(g_{211} + g_{212} \varpi) \) and \( N_{k_v(x)/k_v}(g_{221} + g_{222} \varpi) \) are elements of \( \mathcal{O} \), and so all entries of \( g_2 \) are in \( \mathcal{O} \). Since \( | \det(g_2) |_v = 1 \), we conclude \( g_2 \in \text{GL}(2)_{\mathcal{O}_v} \). Hence \( g \in \mathcal{K} \) and the lemma follows. \( \square \)

We will study the structure of \( G_x \mathcal{O}/p^n \) following the method of [KY]. We first consider the structure of \( N_x \).

**Proposition 4.4.** We have \( N_x \cong \mathcal{O}^\times_{k_v(x)} \) as a group scheme over \( \mathcal{O} \).

**Proof.** Let \( R \) be any \( \mathcal{O} \)-algebra. Then since \( \mathcal{O}_{k_v(x)} = \mathcal{O}[\varpi] \), we have \( \mathcal{O}_{k_v(x)} \otimes_{\mathcal{O}} R = R[\varpi] \). By a standard consideration, we could see that the map
\[
\psi_{xR} : N_x R \to R[\varpi]^\times, \quad n_x(c, d) \mapsto c + d \varpi
\]
gives an isomorphism of these groups, and this map satisfies the usual functorial property with respect to homomorphism of \( \mathcal{O} \)-algebras. This shows that there exists an isomorphism \( \psi_{x} : N_x \to \mathcal{O}^\times_{k_v(x)} \) as group schemes over \( \mathcal{O} \) such that \( \psi_{xR} \) is the induced isomorphism for all \( R \). \( \square \)

From this proposition we obtain the following.

**Corollary 4.5.** The group \( N_x \mathcal{O}/p^n \) is of order \( q_v^{2n-1}(q_v - 1) \).

We now consider \( G_x \mathcal{O}/p^n \).

**Lemma 4.6.** \( [G_x \mathcal{O}/p^n : N_x \mathcal{O}/p^n] = 2q_v^{\delta_x} \).

**Proof.** We shall count the number of elements of the right coset space \( N_x \mathcal{O}/p^n \setminus G_x \mathcal{O}/p^n \). We claim that each right coset contains an element of the form
\[
(4.1) \quad g = \left( 1, \begin{pmatrix} 1 & 0 \\ u & s \end{pmatrix} \right), \quad u \in \mathcal{O}/p^n, \quad s \in (\mathcal{O}/p^n)^\times.
\]
Let \( g \in G_x \mathcal{O}/p^n \). Since \( x(v) \) reduces to \( v_1^2 \) modulo \( p \), \( g_{221} \in p \) and therefore \( g_{222} \) is a unit, which implies that \( A_x(g_{222} - g_{212}) \in \text{GL}(2)_{\mathcal{O}/p^n} \). Hence multiplying \( n_x(g_{222} - g_{212}) \in N_x \) from the left if necessary, we may assume \( g_{212} = 0 \). Then multiplying \( n_x(g_{211}, 0) \) if necessary we further assume \( g_{211} = 1 \). Now comparing the coefficient of \( v_1^2 \) of \( gx \) and \( x \), we conclude that \( t = 1 \). This proves the claim.

Also it is easy to see that each coset has exactly one representative in the form (4.1). Hence we will consider when such an element actually lies in \( G_x \mathcal{O}/p^n \). Suppose that \( g \) is in the form (4.1). By computation,
\[
(gx)(v_1, v_2) = v_1^2 + (a_1 s + 2u)v_1 v_2 + (u^2 + a_1 u s + a_2 s^2)v_2^2.
\]
Hence we can reduce the proof of this lemma to the lemma below. \( \square \)
Lemma 4.7. Let \( u \in \mathcal{O}/p^n \) and \( s \in (\mathcal{O}/p^n)^\times \). Then the system of congruence equations
\[
(4.2) \quad a_1 s + 2u \equiv a_1 (p^n), \quad u^2 + a_1 us + a_2 s^2 \equiv a_2 (p^n)
\]
has \( 2q_v^\delta \) solutions \((u, s)\).

Proof. In the analysis of this system it will be convenient to adopt the usual abuse of notation by which classes in \( \mathcal{O}/p^n \) and their representatives in \( \mathcal{O} \) are denoted by the same symbol. We put \( \pi = a_2 \), which is a uniformizer of \( \mathcal{O} \) since \( \text{ord}_v(\pi) = 1 \).

We first consider the case \( \delta = 2m + 1 \) and hence \( n = 4m + 2 \). In this case, we may assume \( a_1 = 0 \). Then it is easy to see that the system (4.2) is equivalent to
\[
u \equiv 0 (p^{3m+2}), \quad s^2 \equiv 1 (p^{4m+1}).
\]
Therefore for \( u \) there are \( q_v^m \) choices. We consider the latter equation for \( s \), which is equivalent to \( \text{ord}_v(s + 1) + \text{ord}_v(s - 1) \geq 4m + 1 \). Since \( s + 1 - (s - 1) = 2 \) and \( \text{ord}_v(2) = m \), this condition is satisfied if and only if \( s \in \pm 1 + p^{3m+1} \). Hence there are \( 2q_v^{m+1} \) possibilities for \( s \). Thus there are \( 2q_v^{2m+1} \) solutions of \((u, s)\) in all, which proves the lemma in this case.

We next consider the case that \( \delta \) is one of \( 2, \ldots, 2m \), which occurs only if \( v \in \mathfrak{M}_{l_0} \). We put \( l = \delta/2 \). Then \( l \) is an integer between 1 and \( m \). Note that \( 2/a_1 \in \mathcal{O} \) since \( \text{ord}_v(a_1) = l \leq m \). By definition, \( n = 2l + 2m + 1 \). From the second equation of (4.2), we have \( u \in \mathfrak{p} \). We put \( r = u/\pi \), which we regard as an element of \( \mathcal{O}/p^n-1 \). Then the system (4.2) is equivalent to
\[
s + (2/a_1)\pi r \equiv 1 (p^{l+2m+1}), \quad \pi r^2 + a_1 sr + s^2 \equiv 1 (p^{2l+2m}).
\]
We will consider the second equation under the restrictions imposed by the first one. From the first equation, we have
\[
a_1 sr \equiv a_1 r - 2\pi r^2 (p^{2l+2m+1}) \quad \text{and} \quad s^2 \equiv 1 - (4/a_1)\pi r + (4/a_1^2)\pi^2 r^2 (p^{l+3m+1}),
\]
and therefore by computation we see that the second equation is equivalent to
\[
(4\pi^2/a_1^2 - \pi)r^2 + (a_1 - 4\pi/a_1) r \equiv 0 (p^{2l+2m}).
\]
Let \( b_1 = 4\pi^2/a_1^2 - \pi, b_2 = a_1 - 4\pi/a_1 \), and \( b = b_2/b_1 \). Then \( \text{ord}_v(b_1) = 1, \text{ord}_v(b_2) = l \) and \( \text{ord}_v(b) = l - 1 \), and the above equation is equivalent to
\[
r(r + b) \equiv 0 (p^{2l+2m-1}).
\]
We claim that this equation holds if and only if \( \text{ord}_v(r) \geq l + 2m \) or \( \text{ord}_v(r + b) \geq l + 2m \). In fact, if the equation is true, either the order of \( r \) or the order of \( r + b \) is greater than \( l - 1 \). Then since \( \text{ord}_v(b) = l - 1 \), we have \( \min \{ \text{ord}_v(r), \text{ord}_v(r + b) \} = l - 1 \) and therefore \( \max \{ \text{ord}_v(r), \text{ord}_v(r + b) \} \geq l + 2m \). Conversely, under this condition we have \( \min \{ \text{ord}_v(r), \text{ord}_v(r + b) \} = l - 1 \) and hence (4.3) holds.

All of these arguments show that the system (4.2) holds if and only if either one condition of the following is valid:
\[
(A) \quad u \in p^{l+2m+1} \quad \text{and} \quad s \in 1 - 2u/a_1 + p^{l+2m+1},
\]
\[
(B) \quad u \in -b\pi + p^{l+2m+1} \quad \text{and} \quad s \in 1 - 2u/a_1 + p^{l+2m+1}.
\]
Since these conditions are mutually exclusive, we have \( 2q_v^{2l} \) solutions in all and this finishes the proof.

Now we give the proof of Proposition 4.1 by putting together the results we have obtained before.
Proof of Proposition 4.1. Let \( \tau_n \) be the reduction map \( G_\mathcal{O} \to G_\mathcal{O}/p^n \). Then by Lemma 4.3, the set \( K_x = G_\mathcal{O}x \) is equal to disjoint union of \( \#(G_\mathcal{O}/\tau_n^{-1}(G_x\mathcal{O}/p^n)) \)-copies of \( D_x \). Since

\[
G_\mathcal{O}/\tau_n^{-1}(G_x\mathcal{O}/p^n) \cong G_\mathcal{O}/p^n/G_x\mathcal{O}/p^n,
\]

by Lemma 4.6 and Corollary 4.5 we have

\[
\text{vol}(K_x) = \text{vol}(D_x) \cdot \frac{\#(G_\mathcal{O}/p^n)}{2q_v^{2n} \cdot \#(N_x\mathcal{O}/p^n)}
\]

\[
= q_v^{-3n} \cdot q_v^{n-1}(q_v-1) \cdot q_v^{4(n-1)}(q_v^2-1)(q_v^2-q_v) \frac{2q_v^{l} \cdot q_v^{2n-1}(q_v-1)}{2q_v^{2n} \cdot q_v^{2n-1}(q_v-1)}
\]

\[
= 2^{-1}q_v^{-\delta_x}(1-q_v^{-1})(1-q_v^{-2}).
\]

Since \( |\Delta_{k(x)/k}^v| = q_v^{\delta_x} \), we obtained the desired result.

\( \Box \)

Remark 4.8. It is well known that there are \( 2q_v^{l-1}(q_v-1) \) quadratic extensions of \( k_v \) with the norm of the relative discriminant \( q_v^{2l} \) for \( 1 \leq l \leq m \) and \( 2q_v^n \) quadratic extensions of \( k_v \) with the norm of the relative discriminant \( q_v^{2m+1} \). Hence we have

\[
\sum_{2 \leq \delta_x,v \leq 2m_v} \text{vol}(K_x) = q_v^{l-1}(1-q_v^{-1})^2(1-q_v^{-2}),
\]

\[
\sum_{\delta_x,v \geq 2m_v+1} \text{vol}(K_x) = q_v^{-(m+1)}(1-q_v^{-1})(1-q_v^{-2}),
\]

where \( x \) runs through all the standard representatives of local quadratic extensions with discriminant of a given norm. This result matches [T] Proposition 4.3.

References


Graduate School of Mathematical Sciences, University of Tokyo, 3–8–1 Komaba Meguro-ku, Tokyo 153–0041, Japan

E-mail address: tani@ms.u-tokyo.ac.jp