Park, J.
Osaka J. Math.
53 (2016), 983–1002

NOTES ON QUADRATIC INTEGERS AND REAL QUADRATIC NUMBER FIELDS

JEONGHO PARK

(Received June 5, 2013, revised October 7, 2015)

Abstract

It is shown that when a real quadratic integer ξ of fixed norm μ is considered, the fundamental unit ε_d of the field $\mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{d})$ satisfies $\log \varepsilon_d \gg (\log d)^2$ almost always. An easy construction of a more general set containing all the radicands d of such fields is given via quadratic sequences, and the efficiency of this substitution is estimated explicitly. When $\mu = -1$, the construction gives all d's for which the negative Pell's equation $X^2 - dY^2 = -1$ (or more generally $X^2 - DY^2 = -4$) is soluble. When μ is a prime, it gives all of the real quadratic fields in which the prime ideals lying over μ are principal.

Introduction

The regulator is probably one of the most unpredictable constants related to a number field. Dirichlet's class number formula already gave a clear connection between the L-value, the class number, and the regulator, but while the first two have been admitting huge theories in various perspectives, the regulator seems to remain far from being exploited. Let d be a positive square-free integer and K the field $\mathbb{Q}(\sqrt{d})$ with discriminant D, class number h_d and fundamental unit ε_d. In this case Dirichlet's formula reduces to

$$h_d = \frac{\sqrt{D} L(1, \chi)}{2 \log \varepsilon_d}.$$

The L-value is known to stay in a relatively narrow range $D^{-\epsilon} \ll L(1, \chi) \ll \log D$ for arbitrary $\epsilon > 0$ [14], so we know that $D^{1/2-\epsilon} \ll h_d \log \varepsilon_d \ll D^{1/2+\epsilon}$. As for the class number, many things can be said about the primary parts of ideal class groups. Nevertheless we know very little about the fundamental unit, despite the fact that the computation of h_d is essentially impossible without computing $\log \varepsilon_d$.

Although $\log \varepsilon_d$ seems to vary in a wide range between $O(\log D)$ and $O(D^{1/2} \log D)$ in a somewhat uncontrolled way, concerning its average we have several precise conjectures in terms of h_d [2, 11, 13]. A problem that can be considered as a yardstick in this direction is to show that the regulator is in most cases much larger than the class number.

2010 Mathematics Subject Classification. Primary 11R29; Secondary 11R11, 11J68, 11Y40.

Supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (2010-0026473).

It is well known that the fundamental unit ε_d comes from the continued fraction expansion of $\sqrt{d}$ or $(\sqrt{d}+1)/2$ whose period l is the most dominant factor in the size of ε_d [1]. Naturally, many researches have been focused on the size of period and now its upper bound $l \ll \sqrt{d}\log d$ has fairly precise versions [3, 18]. As for the lower bound, it is generally believed that $\log\varepsilon_d \gg D^{1/2-\epsilon}$ holds for most of square-free integer d. However, the average order of ε_d is known only to the following extent; for almost all non-square d, one has $\varepsilon_d > d^{7/4-\epsilon}$ [6, 7].

Keeping this difficulty in mind, in this article we lay our interest on quadratic integers instead. When a quadratic integer ξ has norm a rational prime p, ξ generates a principal prime ideal, i.e., p splits or ramifies into principal prime ideals in $\mathbb{Q}(\xi)/\mathbb{Q}$. A simple fact is that the more there are rational primes $p \ll \sqrt{d}$ that split into principal primes $P\overline{P}$ in $\mathbb{Q}(\sqrt{d})$, the bigger the fundamental unit ε_d becomes [22]. Another fact is that (see Section 3) if $p < \sqrt{D}/2$ and ξ, $\tilde{\xi}$ are the least elements in P, $\overline{P}$ among those numbers greater than 1, then $\xi\tilde{\xi} = p\varepsilon_d$. This suggests that a full knowledge about a single principal prime and its conjugate gives full information about ε_d. This already justifies a study about quadratic integers, and we show in this article that $\log\varepsilon_d \gg \log^2 d$ is true in most cases, where 'most' shall be interpreted in an adequate fashion based on quadratic integers.

Now we formulate the main result. Let μ be a square-free integer with $|\mu| > 1$ and ξ a quadratic integer, i.e., a zero of a monic polynomial $X^2 - TX + \mu$ for some integer T. Since we will treat real quadratic fields which appear only when $T^2 - 4\mu > 0$, we shall fix the norm μ of ξ and let $|T| \to \infty$. For each integer T with $T^2 - 4\mu > 0$, let $\xi_\mu(T)$ be the large root of $X^2 - TX + \mu = 0$ and $D = D_\mu(T)$ the discriminant of $\mathbb{Q}(\xi_\mu(T))$ when $\xi_\mu(T)$ is irrational. Observe that $D_\mu(T) = D_\mu(-T)$, so it is no harm to consider positive T only. Let $d = d_\mu(T)$ be the radicand corresponding to D, viz., $d = D$ if $D \equiv 1 \bmod 4$ and $D/4$ otherwise. Let $f_{|\mu|}(N)$ be the number of distinct fields in $\{\mathbb{Q}(\xi_{-\mu}(T)) \mid 1 < T < N\} \cup \{\mathbb{Q}(\xi_\mu(T)) \mid 1 < T < N\}$. $\omega(\mu)$ denotes the number of distinct prime factors of μ.

Our main result is following

Theorem 0.1.

$$\liminf_{N\to\infty} \frac{f_{|\mu|}(N)}{N} \geq 2^{-\omega(\mu)} \tag{0.1}$$

and

$$\lim_{N\to\infty} \left(\frac{\sharp\{1 < T < N \mid \log\varepsilon_d > L_\mu(T)\}}{N} \right) = 1, \tag{0.2}$$

where

$$L_\mu(T) = \frac{1}{\log|\mu|}\left(\log\frac{\sqrt{D}}{2}\right)^2 - \left(3 - \frac{2\log 2}{\log|\mu|}\right)\log\frac{\sqrt{D}}{2} - 2\log 2 - \frac{2|\mu|}{|\mu|-1}.$$

Yamamoto already gave the infinitude of number fields that satisfy $\log \varepsilon_d \gg \log^{n+1} D$ for $n = 2$ [22], but he did not discuss how often such fields arise in nature. On the other hand, Reiter tried to make Yamamoto's bound effective [19], and in the process of doing so the original leading term $2^n(\log \sqrt{D})^{n+1}/((n+1)! \log p_1 \cdots \log p_n)$ was weakened to $(\log \sqrt{D}/2)^{n+1}/(2(n+1)! \log p_1 \cdots \log p_n)$. Theorem 0.1 gives a density result about the appearance of such fields for the case $n = 1$, and the lower bound for the regulator is also tighter than that of Reiter.

Recalling how little we know about ε_d in general, Theorem 0.1 suggests an interesting set of radicands, namely $\mathfrak{D} = \mathfrak{D}_\mu = \{d_\mu(T) \mid T > 0,\ T^2 - 4\mu > 0\}$. It would be desirable to list up the elements of $\mathfrak{D}$ according to their size and examine the density of $\mathfrak{D}$ in $\mathbb{Z}$, or to construct the set $\mathfrak{D}$ explicitly. Unfortunately we were not successful in this direction. Instead, we try to consider a bigger set that contains $\mathfrak{D}$ and whose construction is simple, explicit and has a sort of measurable efficiency. For this, as long as $\xi_\mu(T)$ and $\xi_\mu(T')$ generate distinct ideals in $\mathbb{Q}(\sqrt{d})$, we allow the radicand d to be counted again in $\mathfrak{D}$.

Let $I^{(0)}(\mu) = \{(y, x) \in \mathbb{Z}^2 \mid 0 \le x < y,\ \gcd(x, y) = 1,\ x^2 \equiv \mu \pmod{y}\}$, $I^{(1)}(\mu) = \{(y, x) \in I^{(0)}(\mu) \mid y \text{ is odd}\}$ and

$$\tilde{y} = \begin{cases} \dfrac{y}{2} & \text{if } y \text{ is even,} \\ y & \text{otherwise.} \end{cases}$$

We use $\mathbb{N}$ to denote the set of nonnegative integers. Define

$$\mathfrak{D}^{(0)}(\mu; y; t) = \{\tilde{y}^2 k^2 + 2k(\tilde{y}/y)\sqrt{\mu + y^2 t} + t \mid k \in \mathbb{N}\},$$
$$\mathfrak{D}^{(1)}(\mu; y; t) = \{4y^2 k^2 + 4k\sqrt{4\mu + y^2 t} + t \mid k \in \mathbb{N}\}$$

which are quadratic progressions, and let

$$\hat{\mathfrak{D}}^{(j)}(\mu; y; t) = \{d \in \mathfrak{D}^{(j)}(\mu; y; t) \mid d \text{ is square-free}\}.$$

Then we have

Proposition 0.2. (1) *There exist maps* $\phi_\mu^{(j)} \colon I^{(j)}(\mu) \to \mathfrak{D}$ *for* $j = 0, 1$ *such that*

$$\mathfrak{D} \subset \bigcup_{j=0,1} \bigcup_{(y,x) \in I^{(j)}(\mu)} \mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x)).$$

(2) *For each* (j, y, x) *there exists an arithmetic progression* $\{T_{y,x}^{(j)}(d) \mid d \in \mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x))\}$ *satisfying* $d_\mu(T_{y,x}^{(j)}(d)) = d$ *for* $d \in \mathfrak{D} \cap \mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x))$, *such that*

$$\sum_{j=0,1} \sum_{(y,x) \in I^{(j)}(\mu)} \sum_{d \in \mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y,x))} \frac{1}{(T_{y,x}^{(j)}(d))^s} \tag{0.3}$$

has a simple pole at $s = 1$ *with residue* $R(\mu) \ll 1$.

The proof of Proposition 0.2 is simple but is constructive and shows that the maps $\phi_\mu^{(j)}$ and $T_{y,x}^{(j)}$ can be determined in a canonical way.

What Proposition 0.2 says is the following. Since $|\xi_\mu(T) - T| \ll |\mu/T|$, one has $\sum \xi_\mu(T)^{-s} - \sum T^{-s} \ll 1$ as $s \to 1+$. It turns out by Theorem 3.2 that even when we pick the traces T in a way that the ideals generated by $\xi_\mu(T)$ are all distinct, the series $\sum T^{-s}$ still have the same residue with $\zeta(s)$ at $s = 1$. We may say for this that the residue corresponding to $\mathfrak{D}$ is 1. In Proposition 0.2, (1) suggests that $\mathfrak{D}$ can be approximated by a union of quadratic progressions, and by (2), its correspondent residue $R(\mu)$ may be considered as a measure of this approximation quality.

To specify how much this union is bigger than $\mathfrak{D}$, let $\hat{R}(\mu)$ be the residue in (0.3) that we shall obtain when $\mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x))$ is replaced by $\hat{\mathfrak{D}}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x))$ in the innermost sum. We first observe that $\hat{R}(\mu) = 1$. This is because $T_{y,x}^{(j)}(d)^2 - 4\mu = y^2 d$ under our construction, and if we assume d is square-free, there is only one quadruple (j, y, x, d) satisfying $T_{y,x}^{(j)}(d) = T$ for a fixed T. Since $R(\mu)$ is the sum of all the residues of the innermost sums in (0.3), computing the density of square-free numbers in $\mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x))$ shall give an estimate of $R(\mu)$. Write $[N] = \{1, 2, \ldots, N\}$ and put

$$f_{y,x}^{(j)}(N) = |\mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x)) \cap [N]|,$$
$$\hat{f}_{y,x}^{(j)}(N) = |\hat{\mathfrak{D}}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x)) \cap [N]|.$$

Then we have

Proposition 0.3. *For each pair* $(y, x) \in I^{(j)}(\mu)$,

$$\lim_{N\to\infty} \frac{\hat{f}_{y,x}^{(j)}(N)}{f_{y,x}^{(j)}(N)}$$
$$= \left(1 - \frac{\omega_d(2)}{4}\right) \cdot \prod_{p|y}{}' \left(1 - \frac{1}{p^2}\right) \cdot \prod_{p^2|\mu}{}' \left(1 - \frac{1}{p}\right) \cdot \prod_{p\nmid \mu y,\, (\mu/p)=1}{}' \left(1 - \frac{2}{p^2}\right)$$

where the restricted products are over odd primes, and

$$\omega_d(2) = \begin{cases} 2 & \text{if } j = 0,\ y \text{ is odd and } \mu \equiv 0 \text{ or } 1 \pmod 4; \\ 2 & \text{if } j = 0,\ y \equiv 2 \pmod 4,\ \mu \equiv 1 \pmod 8; \\ 1 & \text{if } j = 0,\ y \equiv 0 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

EXAMPLE 0.4. Let $C_\mu^{(j)}(y, x)$ be the limit in Proposition 0.3 and consider $\mu = 2$. For any pair $(y, x) \in I^{(0)}(2)$, 2 must be a square modulo y. If y is odd, this is

possible exactly when every prime factor of y is congruent to ± 1 modulo 8. Since $\gcd(x,y)=1$, y cannot be even and we thus have $I^{(0)}(2)=I^{(1)}(2)=\{(1,0),(7,3),(7,4),(17,6),(17,11),\dots\}$. It is easy to see that $\omega_d(2)=0$ always, and numerically one can show that

$$\begin{aligned} C_2^{(j)}(y,x) &= \prod_{p\mid y}\left(1-\frac{1}{p^2}\right)\cdot \prod_{\substack{p\nmid y\\ p\equiv\pm 1 \pmod 8}}\left(1-\frac{2}{p^2}\right) \\ &\geq \prod_{p\equiv\pm 1 \pmod 8}\left(1-\frac{2}{p^2}\right) \\ &= 0.94\cdots \end{aligned}$$

which implies that $0.94R(2)<\hat{R}(2)=1$. The union of quadratic progressions can be therefore considered as a nice substitution for $\mathfrak{D}$ in this case. The choice $\mu=2$ might seem to be especially good, but in fact $\prod_{p:\text{odd}}(1-2/p^2)>0.64$ and the probability to get a square-free integer from $\mathfrak{D}^{(j)}(\mu;y;\phi_\mu^{(j)}(y,x))$ is very often close to 1, and hence so is $R(\mu)$. Note that the product in Proposition 0.3 does not involve any odd prime p with $(\mu/p)=-1$, and the value of the infinite product is affected very little by large primes. The probability $C_\mu^{(j)}(y,x)$ is therefore particularly close to 1 when $\mu\equiv 2$ or 3 (mod 4), μ is square-free and $(\mu/p)=-1$ for small odd primes p so that $4\nmid y$, $\omega_d(2)=0$ and many small primes are excluded in the infinite product.

Next remarks are all about Proposition 0.2.

REMARK 0.5 (Quadratic units). We assumed μ is square-free, but Propositions 0.2 and 0.3 are valid for $\mu=\pm 1$ too and quadratic units can be dealt with in the same way. Suppose $\mu=\pm 1$. If $d\in\hat{\mathfrak{D}}^{(0)}(\mu;y,\phi_\mu^{(0)}(y,x))$, the fundamental solution to the Pell's equation $X^2-dY^2=\mu$ is $(\lfloor\sqrt{d}\rfloor y+x)^2-dy^2=\mu$. Once $\phi_\mu^{(j)}$ is determined naturally, the notion of *leasts to i* in [17] means the least element of $\hat{\mathfrak{D}}^{(0)}(\mu;y,\phi_\mu^{(0)}(y,x))$ for each $(y,x)\in I^{(0)}(\mu)$. So Propositions 0.2 and 0.3 may be considered as a generalization of the result in [17] to quadratic integers with norm other than ± 1.

REMARK 0.6 (Ramification and fundamental units). Suppose $d\equiv 2,3 \pmod 4$ and

$$d\in\mathfrak{D}^{(0)}(p;y;\phi_p^{(0)}(y,x)),\quad \sqrt{d}-1>p \text{ and } p \text{ is ramified in } \mathbb{Q}(\sqrt{d})/\mathbb{Q}.$$

Then (see Section 3 and the proof of Proposition 0.2)

$$\varepsilon_d=\frac{1}{p}(\lfloor\sqrt{d}\rfloor y+x+y\sqrt{d})^2. \tag{0.4}$$

Suppose that a real quadratic number field with discriminant $D=4d$, $\sqrt{d}-1>2$ has class number 1. Then 2 is ramified into a power of a principal ideal, say $(\xi)^2$,

where ξ comes from the continued fraction of $\sqrt{d}$ and corresponds to a pair $(y, x) \in I^{(0)}(2) \cup I^{(0)}(-2)$. It follows that all such fields have fundamental unit of the form (0.4) for some $(y, x) \in I^{(0)}(\mu)$ where we take $\mu = \pm 2$.

REMARK 0.7 (Decomposition into principal primes). In case μ is a prime, say p, the set $\mathfrak{D}_p \cup \mathfrak{D}_{-p}$ gives a complete list of real quadratic number fields in which p ramifies or splits into principal ideals. This is because any principal prime ideal of norm p has a generator ξ of norm $\pm p$ and $\mathfrak{D}_p \cup \mathfrak{D}_{-p}$ contains all of the positive radicands of such fields. Since the prime ideal over p is always principal when p is inert, this classifies all radicands for which the prime ideals of $\mathbb{Q}(\sqrt{d})$ over p are principal. A square-free integer d, though, can be contained in several quadratic progressions given by the construction.

The article is organized as follows. Section 1 gives requisites briefly. In Section 2 the relations between principal reduced ideals and reduced quadratic irrationals coming from the continued fraction of $\sqrt{d}$ or $(1 + \sqrt{d})/2$ are described. In Section 3 we state the distribution of minimal quadratic integers ξ, where a quadratic integer ξ is *minimal* if it is the least number greater than 1 in the ideal (ξ) it generates. Using the contents in Sections 2 and 3, the proof of Theorem 0.1 is given in Section 4. Section 5 covers details for Propositions 0.2 and 0.3. In Section 6 we discuss some technical issues for further research.

1. Preliminaries

In this article μ represents a square-free integer whose absolute value is comparatively small, and d a square-free positive integer which is usually considered to be large. Let $K_d = \mathbb{Q}(\sqrt{d})$ and O_d the ring of integers of K_d, D the discriminant of K_d. Put

$$\omega_d = \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4, \\ \sqrt{d} & \text{otherwise.} \end{cases}$$

Let $\omega_d = [a_0, a_1, a_2, \dots]$ be the simple continued fraction expansion of ω_d, l the period of ω_d, $p_n/q_n = [a_0, a_1, \dots, a_n]$ a convergent to ω_d, $\alpha_{n+1} = [a_{n+1}, a_{n+2}, \dots]$ the $(n+1)$-th total quotient. By convention we put $(p_{-1}, q_{-1}) = (1, 0)$, $(p_{-2}, q_{-2}) = (0, 1)$. For $x \in \mathbb{Q}(\sqrt{d})$, let $\overline{x}$ be its conjugate and $N(x) = x\overline{x}$. For the n-th convergent p_n/q_n of ω_d, put

$$\xi_n = \overline{p_n - q_n\omega_d} = \begin{cases} p_n - q_n + q_n\omega_d & \text{if } d \equiv 1 \bmod 4, \\ p_n + q_n\omega_d & \text{otherwise} \end{cases}$$

and let $\nu_n = |N(\xi_n)| = (-1)^{n+1}N(\xi_n)$. We say that a quadratic integer ξ *comes from* a convergent to ω_d when $\xi = \xi_n$ for some n.

Recall that a quadratic irrational α is *reduced* if $\alpha > 1$ and $-1 < \overline{\alpha} < 0$. It is a classical result that the continued fraction expansion of a real number x is purely periodic if and only if x is a reduced quadratic irrational (for example, see Theorem 7.2 of [16]). In particular $\sqrt{d} + \lfloor \sqrt{d} \rfloor$ and $(1 + \sqrt{d})/2 + \lfloor (1 + \sqrt{d})/2 \rfloor - 1$ are reduced, so one can write $\omega_d = [a_0, \overline{a_1, \ldots, a_l}]$ where $a_l = 2a_0 - 1$ if $d \equiv 1 \bmod 4$ and $a_l = 2a_0$ otherwise. We also recall

Proposition 1.1 ([1]). *$\varepsilon_d = \xi_{l-1}$, and the sequence $\{a_1, \ldots, a_{l-1}\}$ is symmetric.*

The following will be used freely. Let x be a positive real number, p_m/q_m be its m-th convergent and α_m the m-th total quotient.

Proposition 1.2 ([10]). *If $(p, q) = 1$ and*

$$\left| \frac{p}{q} - x \right| < \frac{1}{2q^2}$$

then p/q is a convergent to x.

Proposition 1.3 ([10]). $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$.

Proposition 1.4 ([10]).

$$x = [a_0, a_1, \ldots, a_n, \alpha_{n+1}] = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}.$$

2. Reduced ideals and the convergents to ω_d

Following the literature of [5], [12] and [21], an explicit correspondence between the set of reduced ideals of $\mathbb{Q}(\sqrt{d})$ and the set of reduced quadratic irrationals with discriminant D was given in [22]. For the sake of references in following sections, a short material in [22] is included here.

Write $\omega = (D + \sqrt{D})/2$ where D is the discriminant of $\mathbb{Q}(\sqrt{d})$, so that the ring of integers is $O_d = \mathbb{Z}[\omega]$. For $x_1, \ldots, x_n \in \mathbb{Q}(\sqrt{d})$, let $[x_1, \ldots, x_n]$ and $(x_1, \ldots, x_n)$ be the $\mathbb{Z}$-module and O_d-module generated by $x_1, \ldots, x_n$ (for example $O_d = [1, \omega] = (1)$). For each integral ideal I there is a unique canonical basis of the following form: $I = [a, b + c\omega]$ where a, b, c are integers satisfying

(i) $a > 0$, $c > 0$, $ac = N(I)$,

(ii) c divides a, b and $N(I)$ divides $N(b + c\omega)$, and

(iii) $-a < b + c\overline{\omega} < 0$.

We call the number

$$\alpha(I) = \frac{b + c\omega}{a}$$

the quadratic irrational associated with the ideal I. When $c = 1$ and $\alpha(I)$ is reduced, we say that I is reduced.

Two quadratic irrationals are said to be equivalent if their continued fraction expansions become identical at the tail, and the set of quadratic irrationals of discriminant D falls into h_d classes by this equivalence relation. By the above correspondence, the set of reduced ideals in O_d gives the set of reduced quadratic irrationals of discriminant D, and a reduced ideal I is in the principal ideal class if and only if $\alpha(I)$ is equivalent to ω_d.

We begin with a well-known correspondence.

Lemma 2.1 ([1], Sections 5.6 and 5.7)**.**

$$\alpha((\xi_n)) = \alpha_{n+1}.$$

Lemma 2.2 ([22])**.**

$$\prod_{i=1}^{l} \alpha_i = \varepsilon_d.$$

Lemma 2.3 ([22])**.** *An integral ideal* I *is reduced if*

(i) $N(I) < \sqrt{D}/2$ *and*

(ii) *the conjugate ideal* $\overline{I}$ *is relatively prime to* I.

Lemma 2.4. *For* $n \geq 0$

$$\alpha_{n+1} = \frac{\sqrt{D}}{\nu_n} - \frac{q_{n-1}}{q_n} + \frac{(-1)^{n+1}}{q_n \xi_n}.$$

In particular,

$$\frac{\sqrt{D}}{\nu_n} - 1 < \alpha_{n+1} < \frac{\sqrt{D}}{\nu_n}.$$

Proof. The cases $d \equiv 2$ and $3 \pmod 4$ are easier in computation, so here we assume $d \equiv 1 \pmod 4$ and $\omega_d = (1 + \sqrt{d})/2$. Recall that the continued fraction expansion of ω_d has a natural geometric interpretation on xy-plane. Let $O = (0,0)$ be the origin of the xy-plane, $A = (q_{n-1}, p_{n-1})$, $B = (q_n, p_n)$, C the intersection of $\overline{AB}$ and the line $y = \omega_d x$, and $D = (q_n, \omega_d q_n)$. Then $[\overline{AC} : \overline{CB}] = [\alpha_{n+1} : 1]$ and the area of $\triangle OAB$ is $1/2$. Observe that the area of $\triangle OBD$ is $|(p_n - q_n\omega_d)q_n|/2$. Let $B' = (0, p_n)$, $D' = (0, \omega_d q_n)$.

We have

$$\frac{\xi_n \overline{\xi_n}}{q_n^2} = \left(\frac{p_n}{q_n} - 1 + \omega_d\right)\left(\frac{p_n}{q_n} - 1 + 1 - \omega_d\right) = (-1)^{n+1}\frac{\nu_n}{q_n^2}$$

or

$$\frac{p_n}{q_n} - \omega_d = \frac{(-1)^{n+1}\nu_n}{q_n(p_n - q_n + \omega_d q_n)}$$

and therefore

$$\begin{aligned}
|\square B'BDD'| &= |(p_n - q_n\omega_d)q_n| \\
&= \frac{\nu_n}{p_n/q_n - 1 + \omega_d} \\
&= \frac{\nu_n}{2\omega_d - 1 + (-1)^{n+1}\nu_n/(q_n(p_n - q_n + \omega_d q_n))} \\
&= \frac{\nu_n}{2\omega_d - 1}\left(\frac{1}{1 + (-1)^{n+1}\nu_n/((2\omega_d - 1)q_n(p_n - q_n + \omega_d q_n))}\right) \\
&= \frac{\nu_n}{\sqrt{d}}(1 + \epsilon_n)^{-1}
\end{aligned}$$

where $\epsilon_n = (-1)^{n+1}\nu_n/(\sqrt{d}q_n\xi_n)$. Examining the ratios of the coordinates of A, B and C, it is easily deduced that the area of $\triangle BCD$ is $((1 - q_{n-1}/q_n)/(1 + \alpha_{n+1}))(\nu_n/(2\sqrt{d}))(1 + \epsilon_n)^{-1}$, and hence

$$\begin{aligned}
|\triangle OBC| &= |\triangle OBD| - |\triangle BCD| \\
&= \left(1 - \frac{1 - q_{n-1}/q_n}{1 + \alpha_{n+1}}\right)\frac{\nu_n}{2\sqrt{d}}(1 + \epsilon_n)^{-1} \\
&= \left(\frac{\alpha_{n+1} + q_{n-1}/q_n}{1 + \alpha_{n+1}}\right)\frac{\nu_n}{2\sqrt{d}}(1 + \epsilon_n)^{-1}.
\end{aligned}$$

But $|\triangle OBC| = |\triangle OAB|/(1 + \alpha_{n+1}) = 1/(2(1 + \alpha_{n+1}))$, whence $(\alpha_{n+1} + q_{n-1}/q_n)(\nu_n/\sqrt{d})(1 + \epsilon_n)^{-1} = 1$. Thus

$$\alpha_{n+1} = \frac{\sqrt{d}}{\nu_n} - \frac{q_{n-1}}{q_n} + \frac{(-1)^{n+1}}{q_n\xi_n}.$$

Recall that $q_{-1} = 0 < q_0 = 1 \le q_1$, $q_{n-1} < q_n$ for $n \ge 2$, and $\xi_n \ge q_n\omega_d > q_n$ for $n \ge 0$. Therefore we have $\sqrt{D}/\nu_n - 1 < \alpha_{n+1} < \sqrt{D}/\nu_n$ for $n \ge 0$, which proves the lemma in case $d \equiv 1 \pmod 4$.

When $d \equiv 2$ or $3 \pmod 4$, exactly the same computation with continued fraction of $\omega_d = \sqrt{d}$ completes the proof. □

Suppose $\xi \in \mathbb{Q}(\sqrt{d})$ is a quadratic integer with square-free norm μ and $(\mu, d) = 1$. Then (ξ) is a principal integral ideal which is relatively prime to its conjugate, and (ξ^n) is relatively prime to its conjugate too. Hence the conditions of Lemma 2.3 are satisfied by (ξ^m) if $|N(\xi^m)| \le \omega_d - 1$. Combining Lemmas 2.1, 2.2 and 2.4, one easily

sees that ε_d is large if there are many quadratic integers $\xi \in \mathbb{Q}(\sqrt{d})$ with square-free norm $|N(\xi)| < \sqrt{D}/2$. In this sense, the problem of fundamental units is naturally translated to the problem of quadratic integers of small norms.

3. Quadratic integers of small norms

Assume $\xi = a + b\omega_d \in O_d$ where a, b are positive integers that are relatively prime and $|N(\xi)| = \nu < \omega_d - 1$. Assuming $d \equiv 1 \bmod 4$ (or $d \equiv 2, 3 \bmod 4$), it easily follows that $(a+b)/b - \omega_d < 1/(2b^2)$ (or $a/b - \omega_d < 1/(2b^2)$), which implies $(a+b)/b$ (or a/b) is a convergent to ω_d and hence ξ comes from a convergent to ω_d. Lemma 2.3 in fact tells us that this is true if $\nu < \sqrt{D}/2$. Recall that for every positive integer ν there are only finitely many non-associated (quadratic) integers in O_d of norm $\pm\nu$. As the unit rank of O_d is 1, in each class of associated integers one can choose the least element among those irrational ones greater than 1. Let $F_{(d,\nu)} = \{\xi_1, \ldots, \xi_t\}$ be the set of these least elements, and define $E_\nu(x) = \left|\mathbb{R}_{>1}^{<x} \cap \left(\bigcup_{d:\,\text{square-free}} F_{(d,\nu)}\right)\right|$.

Proposition 3.1. *If $\omega_d = [a_0, \overline{a_1, \ldots, a_l}]$, $\omega_d - 1 > \nu \geq 1$ and ν is square-free, then the elements of $F_{(d,\nu)}$ are of the form $a + b\omega_d$ where $(a+b)/b$ (or a/b) $= [a_0, a_1, \ldots, a_n]$ for some $n < l$.*

Proof. Clear from Proposition 1.2. □

Assume $p < \omega_d - 1$ is a rational prime that splits or ramifies into principal prime ideals in $K_d/\mathbb{Q}$. Write $pO_d = P\overline{P}$. Let $\xi \in P$ and $\tilde{\xi} \in \overline{P}$ be the least elements of P, $\overline{P}$ among those greater than 1. Then $1 < \xi, \tilde{\xi} < \varepsilon_d$ and $\xi\tilde{\xi}$ is an algebraic integer associated to p. By Proposition 3.1 one can write $\xi = a + b\omega_d > \omega_d$ where $(a+b)/b$ or a/b is a convergent to ω_d, whence $|\overline{\xi}| = p/\xi < 1$. Thus $\tilde{\xi} \neq \overline{\xi}$ and $\xi\tilde{\xi}$ is not a rational integer. This shows that $\xi\tilde{\xi} = p\varepsilon_d$.

The distribution of minimal quadratic integers is given in the following

Theorem 3.2. *Let $\nu < M < x$. Then*

(i) $E_\nu(x) < 2x - 2\sqrt{\nu} + O(1)$,

(ii) $E_\nu(x) > 2(1 - 1/(2M-1))x - \left(\sum_{\omega_d < M} |F_{(d,\nu)}|/\log \varepsilon_d\right) \log x + O(1)$.

Proof. Observe that every quadratic integer y of norm $\pm\nu$ is a solution of the equation $X^2 + mX \pm \nu = 0$ for some $m \in \mathbb{Z}$. The number of real quadratic integers y greater than 1 with trace m and norm $\pm\nu$ is 2 if $m > 2\sqrt{\nu}$ and 1 if $m \leq 2\sqrt{\nu}$. With the expression $\xi = (m + \sqrt{m^2 \pm 4\nu})/2$ the first inequality is trivial. As for the second inequality, note that such y must be of the form $\xi\varepsilon_d^k$ for some $\xi \in F_{(d,\nu)}$ and $k \geq 0$. $E_\nu(x)$ counts the numbers with $k = 0$, so we can simply exclude the numbers $\xi\varepsilon_d^k$ less

than x with $k \geq 1$. But $\xi\varepsilon_d^k < x$ if and only if $k < (\log x - \log \xi)/\log \varepsilon_d$, and therefore

$$\#\{\xi\varepsilon_d^k < x \mid k \geq 1,\ \xi \in F_{(d,\nu)},\ \omega_d \leq M\} < \left(\sum_{\omega_d \leq M} \frac{|F_{(d,\nu)}|}{\log \varepsilon_d}\right) \log x.$$

Now consider $\omega_d > M$ and write $\xi\varepsilon_d^k < x \Leftrightarrow \xi < x$ and $\varepsilon_d^k < x/\xi$. Since $\omega_d > M > \nu$, as mentioned at the beginning of this section $\xi = n\acute{\xi}$ for some $n \in \mathbb{N}$ where $\acute{\xi}$ comes from a convergent to ω_d and hence $\xi \geq 2M - 1$. Therefore the contribution to $E_\nu(x)$ from $\omega_d > M$ and $k \geq 1$ is less than the number of quadratic units in the interval $(1, x/(2M-1))$, which is $(2/(2M-1))x + O(1)$. □

Let $a_{(d,\nu)}$ be the set of reduced integral ideals of norm ν in O_d. By Lemma 2.3, if ν is square-free and $\nu < \sqrt{D}/2$ then $|F_{(d,\nu)}| \leq |a_{(d,\nu)}|$.

Proposition 3.3. *Assume $\omega_d > \nu$ where ν is square-free. Let $\nu_1 = \gcd(\nu, 2d)$ and write $\nu = \nu_1\nu_2$. Then*

$$|a_{(d,\nu)}| = \begin{cases} 2^{\omega(\nu_2)} & \text{if } d \text{ is a square modulo } \nu,\ d \equiv 2 \text{ or } 3 \pmod 4, \\ 2^{\omega(\nu_2)} & \text{if } d \text{ is a square modulo } \nu,\ d \equiv 1 \pmod 4,\ \nu \text{ is odd}, \\ 2^{\omega(\nu_2)+1} & \text{if } d \text{ is a square modulo } \nu,\ d \equiv 1 \pmod 8,\ \nu \text{ is even}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $I \in a_{(d,\nu)}$ and write $\alpha(I) = (b + c\omega)/\nu$. Then I is reduced if and only if $c = 1$ and $\alpha(I) > 1$, $-1 < \overline{\alpha(I)} < 0$.

Suppose $d \equiv 2$ or $3 \pmod 4$ so that $\alpha(I) = (b + 2d + \sqrt{d})/\nu$. The condition $N(b + 2d + \sqrt{d}) \equiv 0 \pmod \nu$ implies $(b + 2d)^2 \equiv d \pmod \nu$, so we can write $b \equiv -2d + \zeta \pmod \nu$ where $\zeta^2 \equiv d \pmod \nu$. Hence if d is not a square modulo ν there is no such ideal. The condition $-\nu < b + c\overline{\omega} < 0$ implies b varies in a complete system of residues modulo ν; hence if d is a square modulo ν, the number of possible b's is the number of solutions to $\zeta^2 \equiv d \pmod \nu$. For an odd prime factor p of ν, the congruence $\zeta^2 \equiv d \pmod p$ has two roots if $p \nmid d$ and one root if $p \mid d$. The first case easily follows from this.

Now suppose $d \equiv 1 \pmod 4$. Then $\alpha(I) = (b + d/2 + \sqrt{d}/2)/\nu$ and in the same way as above we get $b^2 + db + d(d-1)/4 \equiv 0 \pmod \nu$ where b varies in a complete system of residues modulo ν. When ν is odd, 2 is a unit modulo ν so one can write $b \equiv -d/2 + \zeta \pmod \nu$ where $\zeta^2 \equiv d/4 \pmod \nu$. This proves the second case. When ν is even, write $\nu = 2\nu'$ and consider $b^2 + db + d(d-1)/4 \equiv 0 \pmod 2$ and $b^2 + db + d(d-1)/4 \equiv 0 \pmod{\nu'}$ separately. The latter has $2^{\omega(\nu_2)}$ solutions. The former has no solution when $d \equiv 5 \pmod 8$ and two solutions when $d \equiv 1 \pmod 8$, which proves the third case. □

4. Proof of Theorem 0.1

Now Theorem 0.1 can be proved easily in the philosophy of Theorem 3.1 in [22].

Proof of Theorem 0.1. Let $\xi \in F_{(d,|\mu|)}$ and put $L = \lfloor \log_{|\mu|}(\sqrt{D}/2) \rfloor$. The ideals (ξ^e) and $(\overline{\xi}^e)$ of O_d are reduced if $|\mu|^e < \sqrt{D}/2$ by Lemma 2.3. Now by Lemmas 2.1, 2.2 and 2.4 we have

$$\begin{aligned}\varepsilon_d &= \prod_{i=1}^{l} \alpha_i \\ &\geq \prod_{e=1}^{L} \alpha((\xi^e)) \prod_{e=1}^{L} \alpha((\overline{\xi}^e)) \\ &> \prod_{e=1}^{L} \left(\frac{\sqrt{D}}{|\mu|^e} - 1 \right)^2.\end{aligned}$$

Taking logarithm,

$$\begin{aligned}\log \varepsilon_d &> \sum_{e=1}^{L} 2 \log\left(\frac{\sqrt{D}}{|\mu|^e} - 1 \right) \\ &> 2 \sum_{e=1}^{L} \left(\log \sqrt{D} - e \log|\mu| - \left(\frac{\sqrt{D}}{|\mu|^e} - 1 \right)^{-1} \right).\end{aligned}$$

The last term can be written

$$\begin{aligned}\sum_{e=1}^{L} \left(\frac{\sqrt{D}}{|\mu|^e} - 1 \right)^{-1} &= \sum_{e=1}^{L} \frac{|\mu|^e}{\sqrt{D}} \left(\frac{1}{1 - |\mu|^e/\sqrt{D}} \right) \\ &< \sum_{e=1}^{L} \frac{2|\mu|^e}{\sqrt{D}} \\ &= \frac{2|\mu|^e}{\sqrt{D}} \left(\frac{|\mu|^L - 1}{|\mu| - 1} \right) \\ &< \frac{|\mu|}{|\mu| - 1},\end{aligned}$$

and therefore

$$\begin{aligned}\log \varepsilon_d &> 2L \log \sqrt{D} - L(L+1) \log|\mu| - \frac{2|\mu|}{|\mu| - 1} \\ &> 2\left(\frac{\log(\sqrt{D}/2)}{\log|\mu|} - 1 \right) \log \sqrt{D} - \log(\sqrt{D}/2) \left(\frac{\log(\sqrt{D}/2)}{\log|\mu|} + 1 \right) - \frac{2|\mu|}{|\mu| - 1} \\ &= \frac{1}{\log|\mu|} \left(\log \frac{\sqrt{D}}{2} \right)^2 - \left(3 - \frac{2 \log 2}{\log|\mu|} \right) \log \frac{\sqrt{D}}{2} - 2 \log 2 - \frac{2|\mu|}{|\mu| - 1}.\end{aligned}$$

(0.1) follows from Theorem 3.2 and Proposition 3.3 immediately. (0.2) also follows from Theorem 3.2 at once too. □

5. The quadratic progressions

In this section we give the proofs of Propositions 0.2 and 0.3. The constructive proofs also give quadratic progressions, which resemble the progressions that appeared in the inverse problem for Pell equation [17].

Proof of Proposition 0.2. We prove (1) and (2) at the same time. Suppose $d \in \mathfrak{D}$. Then there exists a quadratic integer $\xi \in O_d$ of norm μ. Assume $\xi \in \mathbb{Z}[\sqrt{d}]$ first and write $\xi = ny + x + y\sqrt{d}$. Multiplying a unit if necessary, we may assume $0 \le x < y$ and $1 < \xi < \varepsilon_d$. Then

$$N(\xi) = n^2y^2 + 2nxy + x^2 - y^2d = \mu$$

and

$$x^2 \equiv \mu \pmod{y}$$

and

$$2xyn \equiv -x^2 + \mu \pmod{y^2}.$$

Since μ is square-free, $(x, y) = 1$ and so $2xyn \equiv -x^2 + \mu \pmod{y^2}$ if and only if $2n \equiv ((-x^3 + \mu x)/y)\mu^{-1} \pmod{y}$. Thus $(y, x) \in I^{(0)}(\mu)$, and n is uniquely determined modulo $\tilde{y}$. We write $n = n_0 + \tilde{y}k$ for this.

Conversely, if $x^2 \equiv \mu \pmod{y}$ and $2xyn \equiv -x^2 + \mu \pmod{y^2}$, put

$$d = n^2 + \frac{2x}{y}n + \frac{x^2 - \mu}{y^2} \tag{5.1}$$

and it immediately follows that

$$N(ny + x + y\sqrt{d}) = \mu.$$

We have proved that for each $d \in \mathfrak{D}$, in case $\xi \in \mathbb{Z}[\sqrt{d}]$, there exists a pair $(y, x) \in I^{(0)}(\mu)$, and for each $(y, x) \in I^{(0)}(\mu)$ there arises an arithmetic progression $\{n_0 + \tilde{y}k\}_k$ with common difference $\tilde{y}$, which gives rise to a quadratic progression $Q^{(0)} = \{d(k) = (n_0 + \tilde{y}k)^2 + (2x/y)(n_0 + \tilde{y}k) + (x^2 - \mu)/y^2\}_k$. It is easy to see that $Q^{(0)}$ is of the same form with $\mathfrak{D}^{(0)}(\mu; y; t)$ for some t.

Now assume $\xi = ny + x + y\omega_d \in \mathbb{Z}[\omega_d] \setminus \mathbb{Z}[\sqrt{d}]$. Then

$$N(ny + x + y\omega_d) = \left(ny + x + \frac{y}{2}\right)^2 - \frac{y^2}{4}d = \mu$$

or

$$((2n + 1)y + 2x)^2 - y^2d = 4\mu.$$

Since y is odd, we have

$$x^2 \equiv \mu \pmod{y}$$

and

$$(2n+1)xy \equiv -x^2 + \mu \pmod{y^2}$$

and n is uniquely determined modulo $y = \tilde{y}$.

Conversely, if $x^2 \equiv \mu \pmod{y}$ and $(2n+1)xy \equiv -x^2 + \mu \pmod{y^2}$, put

$$d = (2n+1)^2 + \frac{4x}{y}(2n+1) + \frac{4x^2 - 4\mu}{y^2} \tag{5.2}$$

so that $N(ny + x + y\omega_d) = \mu$. This gives another quadratic progression $Q^{(1)}$ which is of the same form as $\mathfrak{D}^{(1)}(\mu; y; t)$ for some t.

There is a canonical way of choosing $\phi_\mu^{(j)}$. Let n and d be in the relation as in (5.1). For each $(y, x) \in I^{(j)}(\mu)$, $Q^{(j)}$ have only finitely many d for which $ny + x + y\omega_d > \varepsilon_d$. This is because $|\mu| < \sqrt{D}/2$ implies $n + x/y$ (or $n + 1 + x/y$) is a convergent to ω_d; in this case, Lemma 2.4 shows that $ny + x + y\omega_d > \varepsilon_d$ can happen only when $\sqrt{D} = a + O(1)$ where a is the largest partial quotient in $x/y = [0, a_1, a_2, \ldots, a_m]$. Discarding these finite numbers, we choose $\phi_\mu^{(j)}(y, x)$ to be the smallest d in $Q^{(j)}$ satisfying $ny + x + y\omega_d < \varepsilon_d$.

In previous paragraphs, for each $d \in \mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y,x))$ there is a quadratic integer $ny + x + y\omega_d$ whose trace is $T_{y,x}^{(0)}(d) = 2ny + 2x$ or $T_{y,x}^{(1)}(d) = (2n+1)y + 2x$. It is clear that $d_\mu(T_{y,x}^{(j)}(d)) = d$ for $d \in \mathfrak{D} \cap \mathfrak{D}^{(j)}(\mu; y; \phi_\mu^{(j)}(y, x))$ and the traces $T_{y,x}^{(j)}(d)$ form an arithmetic progression from the expression $n = n_0 + \tilde{y}k$. To compute the sum (0.3), observe that $n \asymp \sqrt{d}$ and write

$$\begin{aligned}
&\sum_{j=0}^{1} \sum_{(y,x)\in I^{(j)}(\mu)} \sum_{d\in\mathfrak{D}^{(j)}(\mu;y;\phi_\mu^{(j)}(y,x))} \frac{1}{T_{y,x}^{(j)}(d)^s} \\
&\ll \sum_{j=0}^{1} \sum_{(y,x)\in I^{(j)}(\mu)} \sum_{k\geq 0} \frac{1}{\left(x + y\sqrt{\phi_\mu^{(j)}(y,x)} + y^2\right)^s} \\
&\ll \zeta(s)\left(\sum_{j=0}^{1} \sum_{(y,x)\in I^{(j)}(\mu)} \frac{1}{y^{2s}}\right) + \sum_{j=0}^{1} \sum_{(y,x)\in I^{(j)}(\mu)} \frac{1}{\left(y\sqrt{\phi_\mu^{(j)}(y,x)}\right)^s} \quad \text{as } s \to 1+.
\end{aligned}$$

For $(y, x) \in I^{(j)}(\mu)$, every odd prime factor q of y satisfies $(\mu/q) = 1$. Unless $\mu = 1$, the sum $\sum 1/y^s$ over all such y's involves only a half of the primes in the Euler product form of the zeta function. Hence its order is asymptotically $\asymp \zeta(s)^{1/2}$ as $s \to 1+$. Using the Chinese remainder theorem it is easy to see that the number of $x \in [0, y)$

satisfying $x^2 \equiv \mu \pmod{y}$ is a bounded multiple (that is, between a half and twice) of $2^{\omega(y)}$. Recalling $\sum_{n=1}^{\infty} 2^{\omega(n)}/n^s = \zeta(s)^2/\zeta(2s)$ (see Theorem 301 of [10]), one sees that

$$\sum_{(y,x)\in I^0(\mu)} \frac{1}{y^s} \asymp \sum_{y:\ \mu \text{ is a square mod } y} \frac{2^{\omega(y)}}{y^s} \asymp \zeta(s) \quad \text{as } s \to 1+$$

and $\sum_{j=0}^{1} \sum_{(y,x)\in I^{(j)}(\mu)} y^{-2s} \ll 1$. Besides, since there is an upper bound of the period of ω_d in terms of d [3, 15] which gives an upper bound of ε_d, we also have a lower bound of $\phi_\mu^{(j)}(y, x)$ (in terms of y, x) which goes to the infinity as y grows. Therefore

$$\sum_{(y,x)\in I^{(j)}(\mu)} \frac{1}{\left(y\sqrt{\phi_\mu^{(j)}(y, x)}\right)^s} = {}_o(\zeta(s)) \quad \text{as } s \to 1+,$$

which completes the proof. □

Now we give the number of elements in $\mathfrak{D}(\mu; y, x)$ that are square-free. We state a lemma first.

Lemma 5.1. *Let p be an odd prime and $f(x) \in \mathbb{Z}[x]$ a quadratic polynomial whose leading coefficient is not divisible by p. Then $f(x) \equiv 0 \pmod{p^m}$ has a solution if and only if the discriminant of $f(x)$ is a square modulo p^m.*

Proof. ($\Leftarrow$) The root formula for quadratic equations gives a solution.
($\Rightarrow$) Let $t \in \mathbb{Z}$ be a solution to the modular equation. Then

$$f(t + pj) = f(t) + f'(t)pj + \frac{f''(t)}{2} p^2 j^2.$$

Let $p^r \parallel f'(t)$. Choose α so that $f(t) + \alpha \equiv 0 \pmod{p^M}$ where M is sufficiently large. Note that α is necessarily divisible by p^m. We have

$$\begin{aligned} f(t + p^{r+1}j_1) + \alpha &= f(t) + \alpha + \frac{f'(t)}{p^r} p^{2r+1} j_1 + \frac{f''(t)}{2} p^{2r+2} j_1^2 \\ &\equiv f(t) + \alpha + \frac{f'(t)}{p^r} p^{2r+1} j_1 \pmod{p^{2r+2}}, \\ f(t + p^{r+1}j_1 + p^{r+2}j_2) + \alpha &= f(t + p^{r+1}j_1) + \alpha + f'(t + p^{r+1}j_1) p^{r+2} j_2 \\ &\quad + \frac{f''(t + p^{r+1}j_1)}{2} p^{2r+4} j_2^2. \end{aligned}$$

Writing $f'(t + p^{r+1}j_1) = f'(t) + f''(t)p^{r+1}j_1$,

$$\begin{aligned} &f(t + p^{r+1}j_1 + p^{r+2}j_2) + \alpha \\ &\equiv f(t + p^{r+1}j_1) + \alpha + \frac{f'(t)}{p^r}p^{2r+2}j_2 \pmod{p^{2r+3}}, \end{aligned}$$

and successively, there exists a unique sequence $(j_1, j_2, j_3, \dots)$ such that $t + p^{r+1}j_1 + p^{r+2}j_2 + p^{r+3}j_3 + \cdots \in \mathbb{Z}_p$ is a root of $f(x) + \alpha$. Since $\mathbb{Z}_p[x]$ is a UFD, it follows that the discriminant of $f(x) + \alpha$ is a square in $\mathbb{Z}_p$ and hence that of $f(x)$ is a square modulo p^m. □

We appeal to the next theorem. We only need its strength for quadratic polynomials, which can be proved unconditionally using the sieve of Eratosthenes [9].

Theorem 5.2 ([9])**.** *Suppose that $f(x) \in \mathbb{Z}[x]$ has no repeated root. Let B be the largest integer which divides $f(n)$ for all integer n, and select B' to be the smallest divisor of B for which B/B' is square-free. If the abc-conjecture is true, then there are $\sim C_f N$ positive integers $n \le N$ for which $f(n)/B'$ is square-free, where $C_f > 0$ is a positive constant, which we determine as follows*;

$$C_f = \prod_{p:\ prime} \left(1 - \frac{\omega_f(p)}{p^{2+q_p}}\right)$$

where, for each prime p, we let q_p be the largest power of p which divides B' and let $\omega_f(p)$ denote the number of integers a in the range $1 \le a \le p^{2+q_p}$ for which $f(a)/B' \equiv 0 \pmod{p^2}$.

Proof of Proposition 0.3. We first treat $\mathfrak{D}^{(0)}(\mu; y, \phi_\mu^{(0)}(y, x))$. Let $d_0 = \phi_\mu^{(0)}(y, x)$ be the least element of $\mathfrak{D}^{(0)}(\mu; y, \phi_\mu^{(0)}(y, x))$ and n_0 the associated integer in the context of the proof of Proposition 0.2. The elements of $\mathfrak{D}^{(0)}(\mu; y, \phi_\mu^{(0)}(y, x))$ are given by a quadratic polynomial

$$\begin{aligned} d = d(k) &= (n_0 + k\tilde{y})^2 + 2\frac{x}{y}(n_0 + k\tilde{y}) + \frac{x^2 - \mu}{y^2} \\ &= \tilde{y}^2k^2 + \left(\frac{2\tilde{y}}{y}x + 2\tilde{y}n_0\right)k + d_0 \end{aligned}$$

for nonnegative integers k.

We use the notations of Theorem 5.2. Let δ be the discriminant of the quadratic polynomial $d(k)$ and $\omega_d'(p)$ the number of solutions to $d(k) \equiv 0 \pmod{p^2}$ in the range $0 \le k < p^2$. When y is even, $\delta = (x + yn_0)^2 - y^2d_0 = \mu$ and similarly $\delta = 4\mu$ when

y is odd. Therefore $d(k)$ has no repeated root. Note that $\omega'_d(p) < p^2$ implies $p \nmid B'$ and hence $q_p = 0$.

We consider odd primes first. Clearly $d(k) \pmod p$ is degenerate if and only if $p \mid \tilde{y}\mu$. For $p \nmid \tilde{y}\mu$, every root of $d(k) \equiv 0 \pmod p$ has a unique lifting to a p-adic root. There exists such a root if and only if the discriminant is a square modulo p, whence we have

$$w'_d(p) = \begin{cases} 2 & \text{if } (\mu/p) = 1, \\ 0 & \text{if } (\mu/p) = -1. \end{cases}$$

If $p \mid \tilde{y}$, $d(k)$ is congruent to $(x + yn_0)k + d_0$ or $2(x + yn_0)k + d_0$ modulo p^2, which has a unique solution and hence $\omega'_d(p) = 1$.

When $p \mid \mu$, $d(k) \equiv 0 \pmod p$ has a double root. Let t be the root of this equation in the range $0 \le t < p$. From $d(t + pj) \equiv d(t) + d'(t)pj \pmod{p^2}$ and $d'(t) \equiv 0 \pmod p$, it follows that $d(k) \equiv 0 \pmod{p^2}$ has p roots if $d(t) \equiv 0 \pmod{p^2}$ or none otherwise. By Lemma 5.1, $d(k) \equiv 0 \pmod{p^2}$ has a root if and only if the discriminant μ (or 4μ) is a square modulo p^2, which in this case is equivalent to $p^2 \mid \mu$. Thus $\omega'_d(p) = p$ if $p^2 \mid \mu$ and $\omega'_d(p) = 0$ if not.

Now let $p = 2$. Assume y is odd (so $2y \equiv 2 \bmod 4$). Then

$$\begin{aligned} d(k) &\equiv k^2 + 2(x + yn_0)k + d_0 \\ &\equiv k^2 + 2(x + n_0)k + n_0^2 + 2xn_0 + x^2 - \mu \pmod 4 \end{aligned}$$

and

$$\begin{aligned} d(0) \equiv d(2) &\equiv n_0^2 + 2xn_0 + x^2 - \mu \pmod 4, \\ d(1) \equiv d(3) &\equiv n_0^2 + 2xn_0 + x^2 - \mu + 1 + 2x + 2n_0 \pmod 4. \end{aligned}$$

If n_0 is odd, $d(0) \equiv d(2) \equiv (x + 1)^2 - \mu \pmod 4$ and $d(1) \equiv d(3) \equiv x^2 - \mu \pmod 4$. If n_0 is even, $d(0) \equiv d(2) \equiv x^2 - \mu \pmod 4$ and $d(1) \equiv d(3) \equiv (x + 1)^2 - \mu \pmod 4$. It follows that $\omega'_d(2) = 2$ if $\mu \equiv 0, 1 \pmod 4$ and $\omega'_d(2) = 0$ otherwise.

Now assume y is even (and x is necessarily odd). Suppose $y = 2\tilde{y}$ where $\tilde{y}$ is odd. In a single line of computation we obtain

$$\begin{aligned} d(1) &\equiv d_0 + x + 3 \pmod 4, \\ d(2) &\equiv d_0 + 2x \pmod 4, \\ d(3) &\equiv d_0 + 3x + 3 \pmod 4 \end{aligned}$$

which shows that $\omega'_d(2) = 2$ when d_0 is even and $\omega'_d(2) = 0$ otherwise. Observe that

$$\mu = (x + yn_0)^2 - y^2 d_0 \equiv 1 + 4n_0 + 4n_0^2 - 4d_0 \equiv 1 - 4d_0 \pmod 8$$

and it follows that d_0 is even if and only if $\mu \equiv 1 \pmod 8$.

Finally, suppose $4 \mid y$. In this case $d(k) \equiv xk + d_0 \pmod 4$, which has a unique solution to $d(k) \equiv 0 \pmod 4$ and hence $\omega'_d(2) = 1$.

In every case $\omega'_d(p)$ is less than p^2 and $q_p = 0$.

To treat $\mathfrak{D}^{(1)}(\mu; y, \phi^{(1)}_\mu(y, x))$, write

$$\begin{aligned} d = d(k) &= (2(n_0 + yk) + 1)^2 + \frac{4x}{y}(2(n_0 + yk) + 1) + \frac{4x^2 - 4\mu}{y^2} \\ &= 4(n_0^2 + 2yn_0k + y^2k^2) + 1 + 4n_0 + 4yk + \frac{4x}{y}(2n_0 + 1 + 2yk) \\ &\quad + \frac{4x^2 - 4\mu}{y^2} \\ &= 4y^2k^2 + 4(2yn_0 + y + 2x)k + d_0. \end{aligned}$$

The computations for odd primes are exactly the same as the case $j = 0$. For $p = 2$, $\omega'_d(2) = 0$ because d is always congruent to 1 modulo 4. Applying Theorem 5.2 we complete the proof. □

6. The density of discriminants and further topics

It is very natural to ask the density of d's for which p splits or ramifies into principal prime ideals, or d's such that p is in the image of the norm map $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$. This is trivially zero because such d must not be divisible by any prime factor q with $(p/q) = -1$ and these 'special' integers constitute only a null set in $\mathbb{Z}$. More meaningful question is therefore to ask the portion of d's out of all those special integers.

When $\mu \neq 1$, the constructions of $I^{(j)}(\mu)$ and $\hat{\mathfrak{D}}^{(j)}(\mu; y; \phi^{(j)}_\mu(y, x))$ are pretty much the same as the case $\mu = -1$. We can therefore expect the density of

$$\bigcup_{(y,x)\in I^{(j)}(\mu)} \hat{\mathfrak{D}}^{(j)}(\mu; y; \phi^{(j)}_\mu(y, x))$$

for $\mu \neq 1$ to be always similar to that of

$$\bigcup_{(y,x)\in I^{(j)}(-1)} \hat{\mathfrak{D}}^{(j)}(-1; y, \phi^{(j)}_{-1}(y, x)).$$

This counts the square-free integers d such that O_d has an element of norm -1, i.e. the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm -1. This is possible only when every odd prime factor of d is congruent to 1 modulo 4, but not all of such integer d gives a field with $N(\varepsilon_d) = -1$. Assume $\mathfrak{P}$ is a set of prime numbers with Dirichlet density σ. Following the estimation in [20], one can deduce that the number of positive integers (or positive square-free integers) less than N and whose odd prime divisors are all in $\mathfrak{P}$ is of the order $\asymp N(\log N)^{-1+\sigma}$. In particular, when μ is not a square and

$\mathfrak{P} = \{p \mid p\text{: prime}, (\mu/p) = 1\}$, the number of such fundamental discriminants is of the order $N/\sqrt{\log N}$.

For $\mu = -1$, it is a recent result that between 41 % and 67 % out of such fundamental discriminants satisfies $N(\varepsilon_d) = -1$ [8]. We hope similar results to be found for prime numbers p instead of -1 too, but the situation is not that simple. Consider a prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{d})$ above p and its ideal class $[\mathfrak{p}]$. Then our problem is to show that $[\mathfrak{p}]$ is the principal class for a positive density of fundamental discriminants out of those $O(N(\log N)^{-1/2})$ numbers. As -1 is replaced by p, however, the argument in [8] only implies that the order of $[\mathfrak{p}]$ is not divisible by 2. This is because the whole reasoning stems from the theory of genera, which covers the 2-torsion elements (and 2-divisibility) in the ideal class group. The asymptotic behavior of 3-torsion elements is handled via class field theory [4], and the same technique seems to be applicable in obtaining some 3-divisibility result of $[\mathfrak{p}]$. Except these few results, not so much is known about density estimation. It will be very interesting if a family of ideal classes can be actually shown to be principal.

References

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

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

[3] J.H.E. Cohn: *The length of the period of the simple continued fraction of* $d^{1/2}$, Pacific J. Math. **71** (1977), 21–32.

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

[5] P.G.L. Dirichlet: Vorlesungen über Zahlentheorie, Braunschweig: F. Vieweg und Sohn, 1894.

[6] É. Fouvry and F. Jouve: *Size of regulators and consecutive square-free numbers*, Math. Z. **273** (2013), 869–882.

[7] É. Fouvry and F. Jouve: *A positive density of fundamental discriminants with large regulator*, Pacific J. Math. **262** (2013), 81–107.

[8] É. Fouvry and J. Klüners: *On the negative Pell equation*, Ann. of Math. (2) **172** (2010), 2035–2104.

[9] A. Granville: *ABC allows us to count squarefrees*, Internat. Math. Res. Notices (1998), 991–1009.

[10] G.H. Hardy and E.M. Wright: An Introduction to the Theory of Numbers, fifth edition, Oxford Univ. Press, New York, 1979.

[11] C. Hooley: *On the Pellian equation and the class number of indefinite binary quadratic forms*, J. Reine Angew. Math. **353** (1984), 98–131.

[12] E.L. Ince: Cycles of Reduced Ideals in Quadratic Fields, Mathematical Tables **4**, Cambridge Univ. Press, Cambridge, 1968.

[13] M.J. Jacobson, Jr.: *Experimental results on class groups of real quadratic fields* (*extended abstract*); in Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, 463–474, 1998.

[14] X. Li: *Upper bounds on L-functions at the edge of the critical strip*, Int. Math. Res. Not. IMRN (2010), 727–755.

[15] N. Ishii, P. Kaplan and K.S. Williams: *On Eisenstein's problem*, Acta Arith. **54** (1990), 323–345.
[16] I. Niven, H.S. Zuckerman and H.L. Montgomery: An Introduction to the Theory of Numbers, fifth edition, Wiley, New York, 1991.
[17] J. Park: *Inverse problem for Pell equation and real quadratic fields of the least type*, preprint.
[18] E.V. Podsypanin: *The length of the period of a quadratic irrationality*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **82** (1979), 95–99, (Russian).
[19] C. Reiter: *Effective lower bounds on large fundamental units of real quadratic fields*, Osaka J. Math. **22** (1985), 755–765.
[20] G.J. Rieger: *Über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke*, II, J. Reine Angew. Math. **217** (1965), 200–216, (German).
[21] T. Takagi: Shoto Seisuron Kogi, Kyoritsu, Tokyo, 1931, (Japanese).
[22] Y. Yamamoto: *Real quadratic number fields with large fundamental units*, Osaka J. Math. **8** (1971), 261–270.

Department of Mathematics
POSTECH
San 31 Hyoja Dong, Nam-Gu, Pohang 790-784
Korea
Tel. 82-10-3047-7793
e-mail: pkskng@postech.ac.kr