THE UNIT GROUP OF A REAL QUADRATIC FIELD

While the unit group of an imaginary quadratic field is very simple, the unit group of a real quadratic field has nontrivial structure. Its study involves some geometry and analysis, but also it relates to Pell's equation and continued fractions, topics from elementary number theory. These ideas quickly lead to an ideal class number formula for real quadratic fields, similar to its imaginary quadratic counterpart.

Contents

1. Review

Let $F = \mathbb{Q}(\sqrt{n})$ be a real quadratic field. Thus $n > 1$ is not a square, and we take n squarefree. Recall various facts about F.

- The nontrivial automorphism of F is the conjugation function,
$$^- : F \longrightarrow F, \quad \overline{a + b\sqrt{n}} = a - b\sqrt{n}.$$
- The trace function of F is the abelian group homomorphism
$$\mathrm{tr} : F \longrightarrow \mathbb{Q}, \quad \mathrm{tr}(x) = x + \overline{x}.$$
Specifically,
$$\mathrm{tr}(a + b\sqrt{n}) = (a + b\sqrt{n}) + (a - b\sqrt{n}) = 2a.$$
The norm function of F is the abelian group homomorphism
$$\mathrm{N} : F^\times \longrightarrow \mathbb{Q}^\times, \quad \mathrm{N}(x) = x\,\overline{x}.$$
Specifically,
$$\mathrm{N}(a + b\sqrt{n}) = (a + b\sqrt{n})(\overline{a + b\sqrt{n}}) = a^2 - b^2 n.$$
Sometimes we also define $\mathrm{N}(0) = 0$.

- The unit group $\mathcal{O}_F^\times$ of $F^\times$ consists precisely of the elements of $\mathcal{O}_F$ such that $\mathrm{N}(x) = \pm 1$.
- The discriminant of F is

$$D_F = \begin{cases} n & \text{if } n = 1 \pmod 4, \\ 4n & \text{if } n = 2, 3 \pmod 4, \end{cases}$$

and the integer ring of F is

$$\mathcal{O}_F = \mathbb{Z}\left[\frac{D_F + \sqrt{D_F}}{2}\right].$$

- An ideal of $\mathcal{O}_F$ is a subset $\mathfrak{a} \subset \mathcal{O}_F$ that forms an abelian group and is closed under multiplication by $\mathcal{O}_F$. The norm of a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_F$, denoted $\mathrm{N}(\mathfrak{a})$, is characterized by the conditions

$$\mathfrak{a}\overline{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})\mathcal{O}_F, \quad \mathrm{N}(\mathfrak{a}) \in \mathbb{Z}^+.$$

We quickly show that for any positive integer m, only finitely many ideals $\mathfrak{a}$ of $\mathcal{O}_F$ have norm m. Indeed, for any such ideal,

$$m\mathcal{O}_F = \mathfrak{a}\overline{\mathfrak{a}} \subset \mathfrak{a} \subset \mathcal{O}_F,$$

giving a surjection $\mathcal{O}_F/m\mathcal{O}_F \longrightarrow \mathcal{O}_F/\mathfrak{a}$. Thus $|\mathcal{O}_F/\mathfrak{a}| \mid |\mathcal{O}_F/m\mathcal{O}_F| = m^2$, and so it suffices to show that for any positive integer ℓ only finitely many ideals $\mathfrak{a}$ exist such that $|\mathcal{O}_F/\mathfrak{a}| = \ell$. (In fact $|\mathcal{O}_F/\mathfrak{a}| = m$, but we do not show this here.) Let $\left[\begin{smallmatrix} g_1 \\ g_2 \end{smallmatrix}\right]$ be a basis of $\mathcal{O}_F$, and let $\left[\begin{smallmatrix} h_1 \\ h_2 \end{smallmatrix}\right]$ be a basis of $\mathfrak{a}$. Thus

$$\begin{bmatrix} h_1 \\ h_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} g_1 \\ g_2 \end{bmatrix}, \quad a, b, c, d \in \mathbb{Z}.$$

Because the basis of $\mathcal{O}_F$ can be left multiplied by any $\mathrm{GL}_2(\mathbb{Z})$ matrix and remain a basis, and similarly for the basis of $\mathfrak{a}$, in fact $\mathfrak{a}$ is described by the double coset

$$\mathrm{GL}_2(\mathbb{Z}) \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathrm{GL}_2(\mathbb{Z}).$$

Finding a canonical representative of this double coset is precisely the process in the proof of the structure theorem for finitely generated abelian groups. Thus the index-ℓ ideal is described by a unique matrix

$$\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}, \quad 1 \le d_1 \mid d_2,\ d_1 d_2 = \ell.$$

There are only finitely many such matrices, hence only finitely many such ideals.

- In consequence of the previous bullet, we have:

> *Let $\{x_j\}_{j \in \mathbb{Z}^+}$ be a sequence in $\mathcal{O}_F$ all of whose elements satisfy $|\mathrm{N}(x_j)| \le \alpha$ for some constant α. Then for some pair of distinct positive integers j and j',*
>
> $$x_{j'} = u x_j, \quad u \in \mathcal{O}_F^\times.$$

The proof is that there are only finitely many ideals $\langle x_j \rangle$, because $\mathrm{N}(\langle x_j \rangle) = |\mathrm{N}(x_j)|$.

2. Geometric Results

Lemma 2.1. *Let Λ be a lattice in $\mathbb{R}^2$, and let E be a measurable subset of $\mathbb{R}^2$ such that $\mu(E) > \mu(\mathbb{R}^2/\Lambda)$. Then there exist distinct points $x, x' \in E$ such that $x' - x \in \Lambda$.*

Here the set E is not assumed to be compact or connected, only measurable. The lemma is a sort of measure theory pigeonhole principle.

Proof. Let (e, f) be a $\mathbb{Z}$-basis of Λ, so that corresponding fundamental parallelogram of $\mathbb{R}^2/\Lambda$ is

$$\Pi = \{\xi e + \eta f : \xi, \eta \in [0, 1]\}.$$

Thus

$$\text{area}(\Pi) < \mu(E) = \sum_{\lambda \in \Lambda} \mu(E \cap (\lambda + \Pi)).$$

But measure is translation invariant, so rather than summing the measures of E in the translations of the parallelogram, we may sum the measures of the translations of E in the parallelogram itself,

$$\text{area}(\Pi) < \sum_{\lambda \in \Lambda} \mu((\lambda + E) \cap \Pi).$$

Thus the intersection $(\lambda+E)\cap(\lambda'+E)\cap\Pi$ is nonempty for some distinct $\lambda, \lambda' \in \Lambda$. (The reader may enjoy drawing a picture of this argument.) In particular,

$$\lambda + x = \lambda' + x' \quad \text{for some } x, x' \in E.$$

This gives $x' - x = \lambda - \lambda' \in \Lambda - \{0\}$ as desired. □

Proposition 2.2. *Let Λ be a lattice in $\mathbb{R}^2$, and let E be a compact measurable subset of $\mathbb{R}^2$ that is symmetric about 0 and convex and such that $\mu(E) \geq 4\mu(\mathbb{R}^2/\Lambda)$. Then E contains a nonzero point of Λ.*

Taking $\Lambda = \mathbb{Z}^2$, the reader may enjoy gaining a feel by picture that any set E meeting the conditions of the proposition really must contain a nonzero lattice point. For example, a thin ellipse that is tilted to avoid lattice points near the origin must be long enough to contain some lattice point far away in its long direction.

Proof. The lemma says that for any $\varepsilon > 0$, the set

$$E' = \tfrac{1+\varepsilon}{2} E.$$

contains distinct points x and x' such that $x' - x \in \Lambda$. But also, using symmetry about 0, the nonzero difference $x' - x = (2x' + 2(-x))/2$ is a convex linear combination of points of $(1 + \varepsilon)E$, and hence a point of $(1 + \varepsilon)E$. That is, letting $\Lambda' = \Lambda - \{0\}$,

$$\Lambda' \cap (1 + \varepsilon)E \neq \emptyset.$$

Note that $\Lambda' \cap (1 + \varepsilon)E$ is compact—finite, for that matter—because it is the intersection of a discrete set and a compact set. Thus the nested intersection over all ε remains nonempty,

$$\bigcap_{\varepsilon > 0} (\Lambda' \cap (1 + \varepsilon)E) \neq \emptyset.$$

(The *finite intersection property* of compact sets rephrases the definition of compactness. If $\bigcap_\alpha K_\alpha = \emptyset$ then $\bigcup_\alpha K_\alpha^c = K_o$ gives an open cover of K_o, hence $K_\alpha^c = K_o$ for some α by the nestedness, hence $K_\alpha = \emptyset$, contradiction.) But the

nonempty intersection is, using the compactness of E again at the last step of the next display,

$$\bigcap_{\varepsilon>0}(\Lambda' \cap (1+\varepsilon)E) = \Lambda' \cap \bigcap_{\varepsilon>0}(1+\varepsilon)E = \Lambda' \cap \overline{E} = \Lambda' \cap E.$$

This completes the argument. □

The lemma and the proposition are special cases of results due to Minkowski about the *geometry of numbers*.

3. The Canonical Embedding

Definition 3.1. *The* **canonical embedding** *of F is the ring homomorphism*

$$\iota : F \longrightarrow \mathbb{R}^2, \quad x \longmapsto (x, \overline{x}).$$

Recall that our real quadratic field is $F = \mathbb{Q}(\sqrt{n})$, and that its discriminant is

$$D_F = \begin{cases} n & \text{if } n = 1 \pmod 4, \\ 4n & \text{if } n = 2, 3 \pmod 4. \end{cases}$$

The abelian group structure of the integer ring of F is a direct sum,

$$\mathcal{O}_F = \frac{D_F + \sqrt{D_F}}{2}\mathbb{Z} \oplus \mathbb{Z}.$$

The images of the basis elements under the fundamental embedding are

$$\iota(1) = (1, 1),$$
$$\iota\left(\frac{D_F + \sqrt{D_F}}{2}\right) = \left(\frac{D_F + \sqrt{D_F}}{2}\,,\, \frac{D_F - \sqrt{D_F}}{2}\right).$$

Thus $\iota(\mathcal{O}_F)$ is a lattice in $\mathbb{R}^2$ whose fundamental parallelogram has area

$$|\det \begin{bmatrix} 1 & 1 \\ \frac{D_F+\sqrt{D_F}}{2} & \frac{D_F-\sqrt{D_F}}{2} \end{bmatrix}| = \sqrt{D_F}.$$

That is, $\mu(\mathbb{R}^2/\iota(\mathcal{O}_F)) = \sqrt{D_F}$. Consequently, Proposition 2.2 says that any compact box B that is symmetric about the origin and has area $4\sqrt{D_F}$ contains a nonzero point of $\iota(\mathcal{O}_F)$. We will quote this fact below.

4. Finiteness of the Ideal Class Number

Before continuing, we quickly sketch a proof that the real quadratic field F has only finitely many ideal classes.

For any real $c \geq 0$, let

$$S_c = \{(x, y) \in \mathbb{R}^2 : |x| + |y| \leq c\}.$$

This set is symmetric about 0 and convex, and

$$\mu(S_c) = 2c^2.$$

As just shown, $\mu(\mathbb{R}^2/\iota(\mathcal{O}_F)) = \sqrt{D_F}$, and more generally, for an ideal $\mathfrak{a}_o$ of $\mathcal{O}_F$,

$$\mu(\mathbb{R}^2/\iota(\mathfrak{a}_o)) = \sqrt{D_F}\,\mathrm{N}(\mathfrak{a}_o).$$

By Proposition 2.2 and then by the arithmetic-geometric mean inequality:

> If $\mu(S_c) = 4\mu(\mathbb{R}^2/\iota(\mathfrak{a}_o))$ then S_c contains $\iota(\alpha)$ for some nonzero element α of $\mathfrak{a}_o$, and $|\mathrm{N}(\alpha)| \leq c^2/4$.

The condition $\mu(S_c) = 4\mu(\mathbb{R}^2/\iota(\mathfrak{a}_o))$ is $2c^2 = 4\sqrt{\mathcal{D}_K}\,\mathrm{N}(\mathfrak{a}_o)$, and so the bound is

$$|\mathrm{N}(\alpha)| \le \frac{1}{2}\sqrt{\mathcal{D}_K}\,\mathrm{N}(\mathfrak{a}_o).$$

Now consider an ideal class C. Take any ideal $\mathfrak{a}_o$ in the inverse class C^{-1}, and then any $\alpha \in \mathfrak{a}$ as just above. Then $(\alpha) = \mathfrak{a}_o\mathfrak{a}$ for some ideal $\mathfrak{a}$ in C, and

$$\mathrm{N}(\mathfrak{a}) = \frac{|\mathrm{N}(\alpha)|}{\mathrm{N}(\mathfrak{a}_o)} \le \frac{1}{2}\sqrt{\mathcal{D}_K}\,.$$

Because only finitely many ideals $\mathfrak{a}$ satisfy this condition, only finitely many ideal classes exist.

5. The Logarithmic Embedding

Definition 5.1. *The* **logarithmic embedding** *of $\mathcal{O}_F^\times$ is the group homomorphism*

$$\ell : \mathcal{O}_F^\times \longrightarrow \mathbb{R}^2, \quad u \longmapsto (\log|u|, \log|\overline{u}|).$$

Thus the logarithmic embedding takes the form

$$\ell = h \circ \iota\big|_{\mathcal{O}_F^\times}$$

where h is the continuous group homomorphism

$$h : (\mathbb{R}^\times)^2 \longrightarrow \mathbb{R}^2, \quad (x,y) \longmapsto (\log|x|, \log|y|).$$

Note that $\iota\big|_{\mathcal{O}_F^\times}$ is also a homomorphism of multiplicative groups. Because $u\overline{u} = \mathrm{N}(u)$ for $u \in \mathcal{O}_F^\times$, the image $\iota(\mathcal{O}_F^\times)$ lies in the "hyperbola"

$$H = \{(x,y) \in (\mathbb{R}^\times)^2 : xy = \pm 1\}.$$

Also note that the calculation

$$xy = \pm 1 \implies \log|x| + \log|y| = \log|xy| = \log 1 = 0$$

shows that h restricts to a continuous homomorphism from the hyperbola H to the line of slope -1,

$$L = \{(z,w) \in \mathbb{R}^2 : z + w = 0\}.$$

That is,

$$\iota(\mathcal{O}_F^\times) \subset H, \qquad \ell(\mathcal{O}_F^\times) \subset L.$$

Also, direct inspection shows that $\ker(\ell) = \{\pm 1\}$, and thus (the next display has a multiplicative group on the left and an additive group on the right)

$$\mathcal{O}_F^\times \cap \mathbb{R}_{>0} \approx \ell(\mathcal{O}_F^\times),$$

and thus

$$\mathcal{O}_F^\times = \{\pm 1\} \oplus (\mathcal{O}_F^\times \cap \mathbb{R}_{>0}) \approx (\mathbb{Z}/2\mathbb{Z}) \oplus \ell(\mathcal{O}_F^\times).$$

6. Unit Group Structure

We show that $\ell(\mathcal{O}_F^\times)$ is infinite cyclic. First we show that it is discrete.

Lemma 6.1. *For any nonnegative number $r \in \mathbb{R}_{\geq 0}$, $\ell^{-1}([-r,r]^2) \subset \mathcal{O}_F^\times$ is finite.*

Setting $r = 0$ in the lemma shows that $\ker(\ell)$ is finite. Because $\ker(\ell) = \{\pm 1\}$ in the real quadratic field case, we obtain nothing new here, but for number fields other than real quadratic fields, with the lemma modified accordingly, the result is of interest.

Proof. Let $r \geq 0$ and suppose that some element $u \in \mathcal{O}_F^\times$ satisfies

$$\ell(u) \cap [-r,r]^2.$$

That is, $(\log|u|, \log|\overline{u}|) \in [-r,r]^2$, so that

$$|u|, |\overline{u}| \in [e^{-r}, e^r].$$

Consequently

$$|\mathrm{tr}(u)| = |u + \overline{u}| \leq 2e^r \quad \text{and} \quad |\mathrm{N}(u)| = |u\overline{u}| \leq e^{2r}.$$

But the characteristic relation of u over $\mathbb{Z}$ is

$$u^2 - \mathrm{tr}(u)u + \mathrm{N}(u) = 0, \quad \mathrm{tr}(u), \mathrm{N}(u) \in \mathbb{Z}.$$

Thus there are only finitely many possibilities for the characteristic polynomial, and hence there are only finitely many possibilities for u. □

Recall that $\mathcal{O}_F^\times \approx (\mathbb{Z}/2\mathbb{Z}) \oplus \ell(\mathcal{O}_F^\times)$. The lemma shows that $\ell(\mathcal{O}_F^\times)$ is a discrete subgroup of L. Because $L \approx \mathbb{R}$, the question now is whether $\ell(\mathcal{O}_F^\times) = \{0\}$ or $\ell(\mathcal{O}_F^\times) \approx \mathbb{Z}$.

Theorem 6.2. $\ell(\mathcal{O}_F^\times) \approx \mathbb{Z}$.

Proof. For any positive real number λ, the compact box

$$B = [-\lambda, \lambda] \times [-\sqrt{D_F}/\lambda, \sqrt{D_F}/\lambda]$$

is symmetric about the origin, and its area is $4\sqrt{D_F}$. As explained in section 3, the geometry of numbers shows that there exists a nonzero integer $x_1 \in \mathcal{O}_F$ such that $\iota(x_1) \in B$. The fact that $\iota(x_1) = (x_1, \overline{x}_1)$ lies in B says that

$$|\mathrm{N}(x_1)| \leq \sqrt{D_F}.$$

Also, the condition $|\mathrm{N}(x_1)| \geq 1$ holds because $x_1 \in \mathcal{O}_F$, so $\iota(x_1)$ lies outside the four hyperbolic segments $xy = \pm 1$. These segments meet the top and bottom of the box at $|x| = \lambda/\sqrt{D_F}$, so

$$\lambda/\sqrt{D_F} \leq |x_1| \leq \lambda.$$

Repeat the process with a second positive real number $\lambda' > \sqrt{D_F}\,\lambda$ to get $x_2 \in \mathcal{O}_F$ with $|\mathrm{N}(x_2)| \leq \sqrt{D_F}$ and

$$\lambda < \lambda'/\sqrt{D_F} \leq |x_2| \leq \lambda'.$$

The previous two displays combine to give $|x_1| < |x_2|$. Figure 6 shows the upper right quarters of the two boxes used in this argument, with $|x_1| < |x_2|$ by the geometry of the configuration.

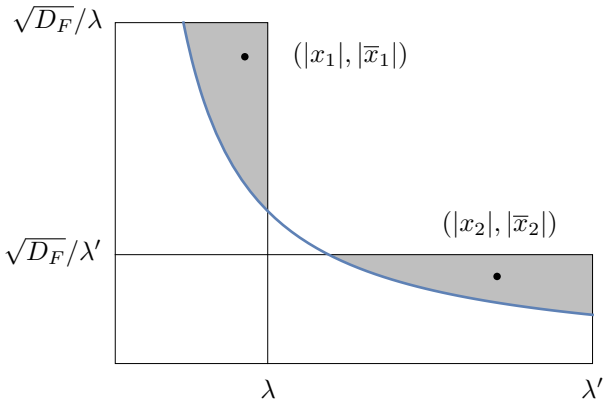

FIGURE 1. Hyperbola and boxes

Continue in this fashion to get a sequence $\{x_j\}$ in $\mathcal{O}_F$ such that

$$|\mathrm{N}(x_j)| \leq \sqrt{D_F} \text{ for all } j \qquad \text{and} \qquad |x_1| < |x_2| < |x_3| < \cdots .$$

The bounded norms and the increasing absolute values are compatible because in our real quadratic field setting, norm is not squared absolute value. As explained at the end of the review section above, the first condition in the previous display implies that $x_{j'} = ux_j$ for some distinct indices j, j' and some unit $u \in \mathcal{O}_F^\times$. The second condition in the previous display gives $|u| \neq 1$, and therefore $\log|u| \neq 0$. This shows that $\ell(\mathcal{O}_F^\times) \neq \{0\}$, and consequently $\ell(\mathcal{O}_F^\times) \approx \mathbb{Z}$ as desired. □

7. The Fundamental Unit

Definition 7.1. *The unique element $u_1 \in \mathcal{O}_F^\times$ such that*

$$\mathcal{O}_F^\times = \{\pm 1\} \times \langle u_1 \rangle = \{\pm 1\} \times \{u_1^i : i \in \mathbb{Z}\}, \quad u_1 > 1.$$

is the **fundamental unit** *of F.*

If the fundamental unit is

$$u_1 = a + b\sqrt{n}, \quad a, b \in \mathbb{Q}$$

then because $\mathrm{N}(u_1) = \pm 1$, altogether

$$u_1, u_1^{-1}, -u_1, -u_1^{-1} = \pm a \pm b\sqrt{n}.$$

Because the fundamental unit is the largest of the four elements in the previous display, in fact

$$u_1 = a + b\sqrt{n}, \quad a, b \in \mathbb{Q}^+,$$

and u_1 is the *smallest* such element $a + b\sqrt{n}$ of $\mathcal{O}_F$. The units $u > 1$ are overall

$$u_k = u_1^k = (a + b\sqrt{n})^k, \quad k = 1, 2, 3, \ldots .$$

Introduce the constant

$$c = \begin{cases} 2 & \text{if } n = 1 \pmod 4 \\ 1 & \text{if } n = 2, 3 \pmod 4. \end{cases}$$

This constant gives a uniform description of the integer ring of F,

$$\mathcal{O}_F = \left\{ \tfrac{1}{c}(a + b\sqrt{n}) : a, b \in \mathbb{Z},\ a = b \pmod{c} \right\}.$$

The fundamental unit takes the form

$$u_1 = \tfrac{1}{c}(a_1 + b_1\sqrt{n}), \quad a_1, b_1 \in \mathbb{Z}^+,\ a_1 = b_1 \pmod{c},\ a_1^2 - nb_1^2 = \pm c^2.$$

Its positive powers are

$$u_1^k = \tfrac{1}{c^k}(a_k + b_k\sqrt{n}) = \tfrac{1}{c^k}(a_1 + b_1\sqrt{n})^k.$$

Because $b_{k+1} = a_k b_1 + b_k a_1$, the sequence $\{b_k\}$ is strictly increasing. Thus, an algorithm to find the fundamental unit for $n = 1 \pmod 4$ is:

> *Test $b_1 = 1, 2, 3, \ldots$ until either of $nb_1^2 \pm c^2$ is a perfect square. Let a_1 be the positive integer such that $a_1^2 - nb_1^2 = \pm c^2$. Then $u_1 = \frac{1}{c}(a_1 + b_1\sqrt{n})$.*

Some fundamental units are shown in figure 2.

n	u_1
2	$1 + \sqrt{2}$
3	$2 + \sqrt{3}$
5	$\frac{1}{2}(1 + \sqrt{5})$
6	$5 + 2\sqrt{6}$
7	$8 + 3\sqrt{7}$
10	$3 + \sqrt{10}$
11	$10 + 3\sqrt{11}$
13	$\frac{1}{2}(3 + \sqrt{13})$
14	$15 + 4\sqrt{14}$
15	$4 + \sqrt{15}$
17	$4 + \sqrt{17}$
19	$170 + 39\sqrt{19}$
21	$\frac{1}{2}(5 + \sqrt{21})$

FIGURE 2. Some fundamental units

8. Continued Fractions and the Fundamental Unit

A more efficient method for finding the fundamental unit uses *continued fractions*. The exposition to follow is drawn from **The Higher Arithmetic** by Davenport.

8.1. **The continued fraction of a rational number.** Let c/d be a nonzero rational number, with $d > 0$. The Euclidean algorithm gives

$$\begin{aligned}
\frac{c}{d} &= q_0 + \frac{r_0}{d}, \quad q_0 \in \mathbb{Z}, \quad 0 < r_0 < d,\\
\frac{d}{r_0} &= q_1 + \frac{r_1}{r_0}, \quad q_1 > 0, \quad 0 < r_1 < r_0,\\
\frac{r_0}{r_1} &= q_2 + \frac{r_2}{r_1}, \quad q_2 > 0, \quad 0 < r_2 < r_1,\\
&\vdots\\
\frac{r_{m-2}}{r_{m-1}} &= q_m, \qquad q_m > 1.
\end{aligned}$$

Letting $\alpha_0 = c/d$, this rewrites as

$$\begin{aligned}
\alpha_0 &= q_0 + \frac{1}{\alpha_1}, \quad q_0 \in \mathbb{Z}, \quad \alpha_1 > 1,\\
\alpha_1 &= q_1 + \frac{1}{\alpha_2}, \quad q_1 > 0, \quad \alpha_2 > 1,\\
\alpha_2 &= q_2 + \frac{1}{\alpha_3}, \quad q_2 > 0, \quad \alpha_3 > 1,\\
&\vdots\\
\alpha_m &= q_m, \qquad q_m > 1.
\end{aligned}$$

Specifically, $q_n = \lfloor \alpha_n \rfloor$ and $\alpha_{n+1} = 1/(\alpha_n - q_n)$ for each $n = 0, \dots, m-1$, and then α_m is an integer at least 2, and the last quotient is $q_m = \alpha_m$. Either way the algorithm is written,

$$\frac{c}{d} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots + \cfrac{1}{q_m}}}}.$$

Working productively with the notation of the previous display is hopeless. A standard remedy is to write instead

$$\frac{c}{d} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots\,\frac{1}{q_m}.$$

Note that also, using the fact that the last quotient q_m is at least 2,

$$\frac{c}{d} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots\,\frac{1}{(q_m-1)+}\,\frac{1}{1}.$$

The expression in the previous three displays is the **continued fraction** expression of c/d.

For any $n = 0, 1, \dots, m-1$ we have

$$\frac{c}{d} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots\,\frac{1}{q_n+}\,\frac{1}{\alpha_{n+1}}. \tag{1}$$

Here the last denominator isn't an integer unless $n = m-1$, when $\alpha_{n+1} = q_m$ and we have the entire continued fraction expression of c/d.

The **convergents** of the continued fraction are the successive approximations of c/d that omit the reciprocal noninteger at the end of the previous display,

$$\frac{h_n}{k_n} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots\,\frac{1}{q_n}, \qquad n = 0, \dots, m.$$

The first few convergents are

$$\begin{aligned}
\frac{h_0}{k_0} &= q_0 = \frac{q_0}{1},\\
\frac{h_1}{k_1} &= q_0 + \frac{1}{q_1} = \frac{q_0q_1+1}{q_1},\\
\frac{h_2}{k_2} &= q_0 + \frac{1}{q_1+}\,\frac{1}{q_2} = q_0 + \frac{q_2}{q_1q_2+1} = \frac{q_0q_1q_2+q_0+q_2}{q_1q_2+1},\\
\frac{h_3}{k_3} &= q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\frac{1}{q_3} = q_0 + \frac{q_2q_3+1}{q_1q_2q_3+q_1+q_3}\\
&= \frac{q_0q_1q_2q_3+q_0q_1+q_0q_3+q_2q_3+1}{q_1q_2q_3+q_1+q_3}\,.
\end{aligned}$$

We use angle brackets to denote the numerator h_n of the nth convergent,

$$\langle q_0, q_1, \ldots, q_n\rangle = h_n.$$

Thus, for example, the penultimate display gives

$$\begin{aligned}
\langle q_0\rangle &= q_0,\\
\langle q_0, q_1\rangle &= q_0q_1+1,\\
\langle q_0, q_1, q_2\rangle &= q_0q_1q_2+q_0+q_2,\\
\langle q_0, q_1, q_2, q_3\rangle &= q_0q_1q_2q_3+q_0q_1+q_0q_3+q_2q_3+1.
\end{aligned}$$

The denominator requires no symbol of its own because, as the small examples have shown, it is simply $\langle q_1, \ldots, q_n\rangle$. The inductive step of showing this in general is

$$\frac{h_n}{k_n} = q_0 + \frac{\langle q_2, \ldots, q_n\rangle}{\langle q_1, \ldots, q_n\rangle} = \frac{q_0\langle q_1, \ldots, q_n\rangle + \langle q_2, \ldots, q_n\rangle}{\langle q_1, \ldots, q_n\rangle}.$$

This also shows the recurrence

$$\langle q_0, q_1, q_2, \ldots, q_n\rangle = q_0\langle q_1, \ldots, q_n\rangle + \langle q_2, \ldots, q_n\rangle.$$

Euler gave the explicit formula

$$\langle q_0, \ldots, q_n\rangle = q_0\cdots q_n + \sum_i \frac{q_0\cdots q_n}{q_iq_{i+1}} + \sum_{i,j} \frac{q_0\cdots q_n}{q_iq_{i+1}q_jq_{j+1}} + \cdots.$$

That is,

- multiply all the q's together,
- then multiply them together omitting *consecutive* pairs,
- then multiply them together omitting *pairs* of consecutive pairs,
- and so on.

Euler's formula demands extending the numerator-symbol to include the case

$$\langle\,\rangle = 1.$$

A consequence of Euler's formula is symmetry,

$$\langle q_0, q_1, \ldots, q_n\rangle = \langle q_n, \ldots, q_1, q_0\rangle,$$

making the recurrence given above also

$$\langle q_0, q_1, q_2, \ldots, q_n\rangle = \langle q_0, \ldots, q_{n-1}\rangle q_n + \langle q_0, \ldots, q_{n-2}\rangle,$$

and similarly starting at q_1, so that we have

$$\begin{bmatrix} h_n \\ k_n \end{bmatrix} = \begin{bmatrix} h_{n-1} \\ k_{n-1} \end{bmatrix} q_n + \begin{bmatrix} h_{n-2} \\ k_{n-2} \end{bmatrix}, \quad n \geq 1,$$

remembering that we interpret $h_{-1} = \langle\,\rangle$ as 1, and interpreting k_{-1} as 0. Thus the convergents are easy to compute in succession from the quotients. Also,

$$\begin{vmatrix} h_0 & h_{-1} \\ k_0 & k_{-1} \end{vmatrix} = \begin{vmatrix} \langle q_0 \rangle & \langle\,\rangle \\ \langle\,\rangle & 0 \end{vmatrix} = \begin{vmatrix} q_0 & 1 \\ 1 & 0 \end{vmatrix} = -1,$$

and

$$\begin{bmatrix} h_n & h_{n-1} \\ k_n & k_{n-1} \end{bmatrix} = \begin{bmatrix} h_{n-1} & h_{n-2} \\ k_{n-1} & k_{n-2} \end{bmatrix} \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix}, \quad n \geq 1,$$

so that by induction,

$$\begin{vmatrix} h_n & h_{n-1} \\ k_n & k_{n-1} \end{vmatrix} = (-1)^{n+1}, \quad n \geq 0.$$

In particular, $\gcd(h_n, k_n) = 1$ for all $n \geq 0$, showing that the nth convergent is in lowest terms. Because

$$\frac{h_n}{k_n} - \frac{h_{n-1}}{k_{n-1}} = \frac{(-1)^{n+1}}{k_n k_{n-1}}, \quad n \geq 1,$$

it follows that the sequence $\{h_n/k_n\}_{n\geq 1}$ is Leibniz. For $n = 0, 1, \ldots, m-1$, equation (1) on page 9 gives

$$\frac{c}{d} = \frac{\langle q_0, q_1, \ldots, q_n, \alpha_{n+1} \rangle}{\langle q_1, \ldots, q_n, \alpha_{n+1} \rangle} = \frac{h_n \alpha_{n+1} + h_{n-1}}{k_n \alpha_{n+1} + k_{n-1}},$$

and so adding fractions gives

$$\left| \frac{c}{d} - \frac{h_n}{k_n} \right| = \left| \frac{h_{n-1}k_n - h_n k_{n-1}}{(k_n \alpha_{n+1} + k_{n-1})k_n} \right| = \frac{1}{(k_n \alpha_{n+1} + k_{n-1})k_n},$$

and because $\alpha_{n+1} \geq q_{n+1}$, so that $k_n \alpha_{n+1} + k_{n-1} \geq k_n q_{n+1} + k_{n-1} = k_{n+1}$, this gives

$$\left| \frac{c}{d} - \frac{h_n}{k_n} \right| \leq \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}.$$

8.2. **The continued fraction of an irrational number.** Let $\alpha = \alpha_0$ be an irrational number. Similarly to before, we have

$$\begin{aligned}
\alpha_0 &= q_0 + 1/\alpha_1, && q_0 \in \mathbb{Z}, && \alpha_1 > 1, \\
\alpha_1 &= q_1 + 1/\alpha_2, && q_1 > 0, && \alpha_2 > 1, \\
\alpha_2 &= q_2 + 1/\alpha_3, && q_2 > 0, && \alpha_3 > 1, \\
&\vdots \\
\alpha_m &= q_m + 1/\alpha_{m+1}, && q_m > 0, && \alpha_{m+1} > 1,
\end{aligned}$$

with $q_n = \lfloor \alpha_n \rfloor$ and $\alpha_{n+1} = 1/(\alpha_n - q_n)$ for each $n \geq 0$, but now the process doesn't terminate. Still, again as before,

$$\alpha = \frac{\langle q_0, \ldots, q_n, \alpha_{n+1} \rangle}{\langle q_1, \ldots, q_n, \alpha_{n+1} \rangle}, \quad n \geq 0,$$

and we have the recurrence

$$\langle q_0, \ldots, q_n, \alpha_{n+1} \rangle = \langle q_0, \ldots, q_n \rangle \alpha_{n+1} + \langle q_0, \ldots, q_{n-1} \rangle = h_n \alpha_{n+1} + h_{n-1}.$$

Similarly

$$\langle q_1, \dots, q_n, \alpha_{n+1} \rangle = k_n \alpha_{n+1} + k_{n-1},$$

and so

$$\alpha = \frac{h_n \alpha_{n+1} + h_{n-1}}{k_n \alpha_{n+1} + k_{n-1}}. \tag{2}$$

Precisely as before, it follows that the sequence $\{h_n/k_n\}_{n \geq 1}$ is Leibniz, and

$$\left| \alpha - \frac{h_n}{k_n} \right| < \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}.$$

Thus

$$\alpha = \lim_n \frac{h_n}{k_n} = q_0 + \frac{1}{q_1+} \, \frac{1}{q_2+} \, \cdots \, \frac{1}{q_n+} \, \dots .$$

When the continued fraction context is clear, we write more concisely

$$\alpha = q_0, q_1, q_2, \dots, q_m, \dots .$$

8.3. **The quadratic irrational case.**

Definition 8.1. *A* **quadratic irrational number** *is a real number of the form*

$$\alpha = a + b\sqrt{n}, \quad a, b \in \mathbb{Q}, \ n \in \mathbb{Z}_{\geq 2} \text{ squarefree.}$$

The **conjugate** *of such a number is*

$$\alpha' = a - b\sqrt{n}.$$

A quadratic irrational number is **normalized** *if* $\alpha > 1$ *and* $-1 < \alpha' < 0$.

If α is quadratic irrational and normalized, then so is $\beta = -1/\alpha'$, as the reader can check. This idea will be used twice in proving the next proposition. Repeating the construction to define $\gamma = -1/\beta'$ gives α again. The condition $\beta = \alpha$, i.e., $\alpha\alpha' = -1$, is $a^2 - b^2 n = -1$, making α a unit in the quadratic field $\mathbb{Q}(\sqrt{n})$.

Proposition 8.2. *Let α be an irrational number. Then α is quadratic and normalized if and only if its continued fraction is periodic.*

For example, the golden ratio φ, defined by the conditions $\varphi - 1 = 1/\varphi$ and $\varphi > 1$, is quadratic and normalized, and $\varphi\varphi' = -1$, and the continued fraction of φ is $\overline{1}$.

Proof. ($\Longrightarrow$) Let α be quadratic and normalized. Thus $\alpha > 1$ and $-1 < \alpha' < 0$. For some $P, D, Q \in \mathbb{Z}$ with D a positive nonsquare and Q nonzero,

$$\alpha = \frac{P + \sqrt{D}}{Q}.$$

Because $2\sqrt{D}/Q = \alpha - \alpha' > 1 - 0 = 1$ we have $Q > 0$, and because $2P/Q = \alpha + \alpha' > 1 - 1 = 0$ we have $P > 0$, and because $(P - \sqrt{D})/Q = \alpha' < 0$ we have $P < \sqrt{D}$, and because $(P + \sqrt{D})/Q = \alpha > 1$ we have $Q < P + \sqrt{D}$. Further, because α and α' are the roots of a quadratic equation with integer coefficients,

$$ax^2 + bx + c = 0, \quad a, b, c \in \mathbb{Z}, \ a > 0,$$

it follows that $Q = 2a$ and therefore

$$P^2 - D = (P + \sqrt{D})(P - \sqrt{D}) = \alpha\alpha' Q^2 = (c/a)Q^2 = 2cQ = 0 \pmod{Q}.$$

For a given D there are only finitely many P and Q satisfying the conditions $0 < P < \sqrt{D}$ and $0 < Q < P + \sqrt{D}$ and $P^2 = D \pmod{Q}$ that we have just derived, and so there exist only finitely many normalized values $\alpha = (P + \sqrt{D})/Q$.

Let $\alpha_0 = \alpha$, so that from $\alpha_0 = q_0 + 1/\alpha_1$ we get

$$\alpha_1 = \frac{1}{\alpha_0 - q_0} \quad \text{and thus} \quad \alpha_1' = \frac{1}{\alpha_0' - q_0}.$$

Because $\alpha_0 - q_0 = \alpha_0 - \lfloor \alpha_0 \rfloor$ lies between 0 and 1 it follows that $\alpha_1 > 1$. Because $\alpha_0' - q_0 < -1$ it follows that $\alpha_1' < 0$ and that $\alpha_1' + 1 = (\alpha_0' - q_0 + 1)/(\alpha_0' - q_0) > 0$, which is to say that $\alpha_1' > -1$. That is, α_1 is again normalized. By a little algebra,

$$\alpha_1 = \frac{Q(P - q_0 Q - \sqrt{D})}{(P - q_0 Q)^2 - D},$$

and because the denominator is a multiple of Q in consequence of the congruence $P^2 = D \pmod{Q}$ from above, α_1 takes the form $(P_1 + \sqrt{D})/Q_1$ with the same D as in α_0. Thus the same applies to α_2 and so on. But there are only finitely many possibilities for P and Q, so eventually the sequence $\alpha_1, \alpha_2, \ldots$ repeats a value, and from then on it is periodic. What remains to be shown is that the period starts at α_0.

Let the earliest repeat value be $\alpha_{n+k} = \alpha_n$, with $n \geq 0$ and $k > 0$, so that α is periodic from α_n onward. We want to show that $n = 0$. Let $\beta_m = -1/\alpha_m'$ for any $m \geq 0$, which is normalized because α_m is, and note that

$$\alpha_m = q_m + \frac{1}{\alpha_{m+1}} \implies \alpha_m' = q_m + \frac{1}{\alpha_{m+1}'} \implies \beta_{m+1} = q_m + \frac{1}{\beta_m}\,.$$

Thus $\lfloor \alpha_m \rfloor = \lfloor \beta_{m+1} \rfloor$, their shared value being q_m. Note also that $\beta_{n+k} = \beta_n$ because $\alpha_{n+k} = \alpha_n$ and $\beta_m = -1/\alpha_m'$ for all m. Assuming that $n > 0$, we have

$$q_{n-1+k} = \lfloor \alpha_{n-1+k} \rfloor = \lfloor \beta_{n+k} \rfloor = \lfloor \beta_n \rfloor = \lfloor \alpha_{n-1} \rfloor = q_{n-1},$$

from which

$$\alpha_{n-1+k} = q_{n-1+k} + \frac{1}{\alpha_{n+k}} = q_{n-1} + \frac{1}{\alpha_n} = \alpha_{n-1},$$

so the periodicity of α is already in effect at generation $n-1$. This contradicts that the periodicity starts at generation n, making the assumption $n > 0$ untenable. That is, beyond being eventually periodic, α is immediately periodic.

($\Longleftarrow$) Let α be periodic,

$$\alpha = q_0, \ldots, q_m, q_0, \ldots, q_m, q_0, \ldots, q_m, \ldots = \overline{q_0, \ldots, q_m}.$$

Thus $\alpha > q_0 \geq 1$, giving $\alpha > 1$. Next, equation (2) and the periodicity of α give the characteristic relation of α,

$$\alpha = \frac{h_m \alpha + h_{m-1}}{k_m \alpha + k_{m-1}},$$

and this rewrites as the characteristic polynomial equation of α,

$$k_m \alpha^2 + (k_{m-1} - h_m)\alpha - h_{m-1} = 0,$$

showing that α is quadratic. Now consider the reverse-order periodic continued fraction,

$$\beta = \overline{q_m, \ldots, q_0}.$$

Similarly to α, now $\beta > 1$ because q_m is a positive integer, and the characteristic relation of β is almost the same as that of α,

$$\beta = \frac{h_m\beta + k_m}{h_{m-1}\beta + k_{m-1}}.$$

Consequently, the characteristic relation of $-1/\beta$ is

$$-1/\beta = \frac{k_{m-1}(-1/\beta) - h_{m-1}}{-k_m(-1/\beta) + h_m},$$

so that the characteristic equation of $-1/\beta$ is

$$k_m(-1/\beta)^2 + (k_{m-1} - h_m)(-1/\beta) - h_{m-1} = 0.$$

That is, α and $-1/\beta$ satisfy the same quadratic equation, so $-1/\beta$ is one of α, α'. Because $\alpha > 1$ and $-1 < -1/\beta < 0$, we see that $-1/\beta = \alpha'$ and consequently $-1 < \alpha' < 0$. That is, α is normalized. □

Now consider a positive integer n that is not a perfect square. Let

$$q_0 = \lfloor \sqrt{n} \rfloor, \qquad \alpha = \sqrt{n} + q_0.$$

Then $\alpha > 1$ and $\alpha' = -\sqrt{n} + q_0 \in (-1, 0)$, showing that α is normalized. Note also that

$$\alpha' = -\alpha + 2q_0.$$

By " $\Longrightarrow$ " of the previous proposition, with the initial quotient for α being $2q_0$,

$$\alpha = \overline{2q_0, q_1, \ldots, q_m} = 2q_0, \overline{q_1, \ldots, q_m, 2q_0},$$

so that

$$\frac{1}{\alpha - 2q_0} = \overline{q_1, \ldots, q_m, 2q_0}.$$

Also, from the proof of " $\Longleftarrow$ " of the proposition,

$$-1/\alpha' = \overline{q_m, \ldots, q_1, 2q_0}.$$

But because $\alpha' = -\alpha + 2q_0$, the left sides of the two previous displays are equal, hence so are the right sides, and thus

$$q_1, \ldots, q_m \quad \text{is palindromic.}$$

This shows that $\sqrt{n} = \alpha - q_0$ has continued fraction

$$\boxed{\sqrt{n} = q_0, \overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}.}$$

For example,

$$\begin{aligned}
\sqrt{2} &= 1, \overline{2}, \\
\sqrt{3} &= 1, \overline{1, 2}, \\
\sqrt{13} &= 3, \overline{1, 1, 1, 1, 6}, \\
\sqrt{31} &= 5, \overline{1, 1, 3, 5, 3, 1, 1, 10}.
\end{aligned}$$

8.4. **The fundamental unit again.** Let the real quadratic number field $\mathbb{Q}(\sqrt{n})$ have discriminant D. Set

$$q_0 = \left\lfloor \frac{D+\sqrt{D}}{2} \right\rfloor, \qquad \alpha_0 = \frac{D+\sqrt{D}}{2} + q_0 - D = \frac{-D+\sqrt{D}}{2} + q_0\,.$$

We show that α_0 is normalized. First, note that

$$\alpha_0 = \frac{-D+\sqrt{D}}{2} + \left\lfloor \frac{D+\sqrt{D}}{2} \right\rfloor > \frac{-D+\sqrt{D}}{2} + \frac{D+\sqrt{D}}{2} - 1 = \sqrt{D} - 1,$$

and so $\alpha_0 > 1$ because $D \geq 5$. Second,

$$\overline{\alpha}_0 = \frac{-D-\sqrt{D}}{2} + q_0 = -\left(\frac{D+\sqrt{D}}{2} - \left\lfloor \frac{D+\sqrt{D}}{2} \right\rfloor \right),$$

and so $\overline{\alpha}_0 \in (-1, 0)$.

Because α_0 is normalized and has floor $2q_0 - D$,

$$\alpha_0 = \overline{2q_0 - D, q_1, \ldots, q_m} = 2q_0 - D, \overline{q_1, \ldots, q_m, 2q_0 - D}.$$

Thus, because $\frac{-D+\sqrt{D}}{2} = \alpha_0 - q_0$,

$$\begin{aligned} \frac{-D+\sqrt{D}}{2} &= q_0 - D, \overline{q_1, \ldots, q_m, 2q_0 - D} \\ &= q_0 - D, q_1, \ldots, q_m \overline{2q_0 - D, q_1, \ldots, q_m} \\ &= q_0 - D, q_1, \ldots, q_m, \alpha_0. \end{aligned}$$

That is, noting that $q_0 - D$ is the initial quotient of $\frac{-D+\sqrt{D}}{2}$,

$$\frac{-D+\sqrt{D}}{2} = \frac{h_m \alpha_0 + h_{m-1}}{k_m \alpha_0 + k_{m-1}} = \frac{h_m \left(\frac{-D+\sqrt{D}}{2} + q_0 \right) + h_{m-1}}{k_m \left(\frac{-D+\sqrt{D}}{2} + q_0 \right) + k_{m-1}},$$

or

$$k_m \left(\tfrac{-D+\sqrt{D}}{2} + q_0 \right) \tfrac{-D+\sqrt{D}}{2} + k_{m-1} \tfrac{-D+\sqrt{D}}{2} = h_m \left(\tfrac{-D+\sqrt{D}}{2} + q_0 \right) + h_{m-1}.$$

Here we have $\left(\frac{-D+\sqrt{D}}{2} \right)^2 = \frac{D(1-D)}{4} - D \cdot \frac{-D+\sqrt{D}}{2}$, so now

$$\tfrac{D(1-D)}{4} k_m + ((q_0 - D)k_m + k_{m-1}) \tfrac{-D+\sqrt{D}}{2} = q_0 h_m + h_{m-1} + h_m \tfrac{-D+\sqrt{D}}{2}\,.$$

Equate the coefficients of 1 and $\frac{-D+\sqrt{D}}{2}$ to get

$$\begin{bmatrix} h_{m-1} \\ k_{m-1} \end{bmatrix} = -q_0 \begin{bmatrix} h_m \\ k_m \end{bmatrix} + \begin{bmatrix} \frac{D(1-D)}{4} k_m \\ h_m + D k_m \end{bmatrix}.$$

Recall that

$$\begin{vmatrix} h_m & h_{m-1} \\ k_m & k_{m-1} \end{vmatrix} = (-1)^{m+1}.$$

The previous two displays give

$$h_m^2 + D h_m k_m + \tfrac{D(D-1)}{4} k_m^2 = \begin{vmatrix} h_m & \frac{D(1-D)}{4} k_m \\ k_m & h_m + D k_m \end{vmatrix} = \begin{vmatrix} h_m & h_{m-1} \\ k_m & k_{m-1} \end{vmatrix} = (-1)^{m+1}.$$

That is, because

$$\begin{aligned}\mathrm{N}(h+k\tfrac{D+\sqrt{D}}{2}) &= \left(h+\frac{Dk}{2}+\frac{\sqrt{D}\,k}{2}\right)\left(h+\frac{Dk}{2}-\frac{\sqrt{D}\,k}{2}\right)\\ &= \left(h+\frac{Dk}{2}\right)^2-\frac{Dk^2}{4}\\ &= h^2+Dhk+\tfrac{D(D-1)}{4}k^2,\end{aligned}$$

we have

$$\boxed{h_m+k_m\frac{D+\sqrt{D}}{2} \text{ is a unit of } \mathbb{Q}(\sqrt{n}).}$$

Here h_m and k_m are the mth convergents of $\frac{-D+\sqrt{D}}{2}$, not of $\frac{D+\sqrt{D}}{2}$, but there is no difference for $m \geq 1$.

9. The Real Quadratic Class Number Formula

Let F be a real quadratic number field, $F=\mathbb{Q}(\sqrt{n})$ with $n \neq 0,1$ squarefree, having discriminant D_F and fundamental unit u. Introduce a constant that incorporates these two values,

$$\kappa = \frac{2\log(u)}{\sqrt{D_F}}\,.$$

Briefly dropping the assumption that our quadratic field F is real, a more general definition of κ is as follows. Let r denote the number of embeddings $F \longrightarrow \mathbb{R}$, the *real embeddings* of F, and let s denote the number of pairs of complex conjugate embeddings $F \longrightarrow \mathbb{C}$, the *complex embeddings* of F; thus $(r,s)=(2,0)$ in the real quadratic case and $(r,s)=(0,1)$ in the imaginary quadratic case. Let w denote the number of roots of unity in F, so that $w=2$ except that $w=4$ when $F=\mathbb{Q}(i)$ and $w=6$ when $F=\mathbb{Q}(\sqrt{-3})$. The *regulator* of F is

$$\mathrm{reg}(F) = \begin{cases}\log u & \text{if } F \text{ is real quadratic}\\ 1 & \text{if } F \text{ is imaginary quadratic.}\end{cases}$$

Just as the discriminant measures the sparseness of the integer ring $\mathcal{O}_F$, the regulator measures the sparseness of the unit group $\mathcal{O}_F^\times$. Now the definition is

$$\kappa = \frac{2^r(2\pi)^s\,\mathrm{reg}(F)}{w\sqrt{|D_F|}}\,.$$

This gives $\kappa = \frac{2\log u}{\sqrt{D_F}}$ as above if F is real quadratic and $\kappa = \frac{2\pi}{w\sqrt{|D_F|}}$ if F is imaginary quadratic, and it extends to fields F beyond the quadratic case with $\mathrm{reg}(F)$ suitably generalized. With this comment made, we return to the case that F is real quadratic.

For any ideal class $\mathcal{C}$ and any positive integer n, define

$$A_n(\mathcal{C}) = \#\{\mathfrak{a} : \mathfrak{a} \in \mathcal{C},\ \mathrm{N}(\mathfrak{a}) \leq n\},$$

and with no reference to any ideal class, define

$$A_n = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \leq n\}.$$

The next proposition agrees with its counterpart Proposition 14.3 from the imaginary quadratic fields writeup.

Proposition 9.1. *With $\mathcal{C}$, n, $A_n(\mathcal{C})$, A_n, and κ as above, and with h the ideal class number of F,*

$$A_n(\mathcal{C}) = \kappa n + \mathcal{O}(n^{1/2}).$$

and

$$A_n = h\kappa n + \mathcal{O}(n^{1/2}).$$

Proof. Because the right side of the first equality is independent of $\mathcal{C}$, the second equality follows from the first. So we need only to establish the first equality.

Choose any ideal $\mathfrak{a}_o \in \mathcal{C}^{-1}$. The ideals $\mathfrak{a}$ such that

$$\mathfrak{a} \in \mathcal{C},\ \mathrm{N}(\mathfrak{a}) \le n$$

are the ideals $\mathfrak{a}$ such that

$$\mathfrak{a}_o\mathfrak{a} = (\alpha),\ |\mathrm{N}(\alpha)| \le \mathrm{N}(\mathfrak{a}_o)n,$$

which correspond bijectively to the principal ideals (α) of $\mathcal{O}_F$ such that

$$(\alpha) \subset \mathfrak{a}_o,\ |\mathrm{N}(\alpha)| \le \mathrm{N}(\mathfrak{a}_o)n.$$

Specifically, the correspondence is $\mathfrak{a} \mapsto \mathfrak{a}_o\mathfrak{a}$ and $(\alpha) \mapsto (\alpha)/\mathfrak{a}_o$.

Because we are in the real quadratic case, the sector

$$S_{\mathrm{N}(\mathfrak{a}_o)n} = \{(x,y) \in \mathbb{R}^2 : 0 \le x \le y \le u^2 x,\ xy \le \mathrm{N}(\mathfrak{a}_o)n\}$$

(see figure 9, in which $S_{\mathrm{N}(\mathfrak{a}_o)n}$ is the shaded region in the left side and the normalized sector S_1 is its darker part) and its reflection in second quadrant form a fundamental domain for the elements of $\iota(\mathcal{O}_F - 0)/\iota{\mathcal{O}_F}^\times$ having absolute norm at most $\mathrm{N}(\mathfrak{a}_o)n$. This sector's area is

$$\mu(S_{\mathrm{N}(\mathfrak{a}_o)n}) = \mathrm{N}(\mathfrak{a}_o)n\,\mu(S_1).$$

The normalized sector has area

$$\begin{aligned}\mu(S_1) &= \int_{\theta=\pi/4}^{\arctan(u^2)} \int_{r=0}^{\sqrt{\sec\theta\csc\theta}} r\,\mathrm{d}r\,\mathrm{d}\theta = \frac{1}{2}\int_{\theta=\pi/4}^{\arctan(u^2)} \sec\theta\csc\theta\,\mathrm{d}\theta \\ &= \frac{1}{2}\int_{\theta=\pi/4}^{\arctan(u^2)} \frac{\sec^2\theta\,\mathrm{d}\theta}{\tan\theta} = \frac{1}{2}\log\tan(\arctan(u^2)) = \log(u).\end{aligned}$$

Let P be a fundamental parallelogram for $\iota\mathfrak{a}_o$ centered at $(0,0)$,

$$P = [-1/2, 1/2]a_1 + [-1/2, 1/2]a_2 \quad \text{where } \{a_1, a_2\} \text{ is a basis of } \iota\mathfrak{a}_o,$$

and consider the set of translates $P_a = a + P$, where $a \in \iota\mathfrak{a}_o$, that intersect $S_{\mathrm{N}(\mathfrak{a}_o)n}$. These translates occur in two types, those that lie entirely in $S_{\mathrm{N}(\mathfrak{a}_o)n}$ and those that stick out of it,

$$\text{type 1: } P_a \subset S_{\mathrm{N}(\mathfrak{a}_o)n}, \qquad \text{type 2: } P_a \not\subset S_{\mathrm{N}(\mathfrak{a}_o)n}.$$

The containments

$$\{\text{type 1 } P_a \text{ centers}\} \subset \mathfrak{a}_o \cap S_{\mathrm{N}(\mathfrak{a}_o)n} \subset \{\text{all } P_a \text{ centers}\}$$

and

$$\bigcup \text{type 1 } P_a \subset S_{\mathrm{N}(\mathfrak{a}_o)n} \subset \bigcup \text{all } P_a$$

give the numerical estimates

$$\#\{\text{type 1 } P_a\}| \le \#(\mathfrak{a}_o \cap S_{\mathrm{N}(\mathfrak{a}_o)n}) \le \#\{\text{all } P_a\}$$

and, because $\mu(P_a) = \sqrt{D_F}\mathrm{N}(\mathfrak{a}_o)$ for all a and $\mu(S_{\mathrm{N}(\mathfrak{a}_o)n}) = \mu(S_1)\mathrm{N}(\mathfrak{a}_o)n$,

$$\#\{\text{type 1 } P_a\} \le \frac{\mu(S_1)}{\sqrt{D_F}}n \le \#\{\text{all } P_a\}.$$

Because $\#(\mathfrak{a}_o \cap S_{\mathrm{N}(\mathfrak{a}_o)n}) = \frac{1}{2}A_n(\mathcal{C})$ and $\mu(S_1) = \log(u)$, the two numerical estimates combine to give

$$\left| A_n(\mathcal{C}) - \frac{2\log(u)}{\sqrt{D_F}}t \right| \le 2\#\{\text{type 2 } P_a\}.$$

Thus what needs to be shown is that the number of type 2 parallelograms P_a is $\mathcal{O}(n^{1/2})$. But the boundary of $S_{\mathrm{N}(\mathfrak{a}_o)n}$ consists of two line segments and one hyperbola segment whose lengths are proportional to $n^{1/2}$, so the result follows. For example, a linear change of coordinates reduces the situation to unit squares centered at integer points, and one can argue that the number of such squares that intersect a line segment or a conic section segment is at most some constant times the segment length. □

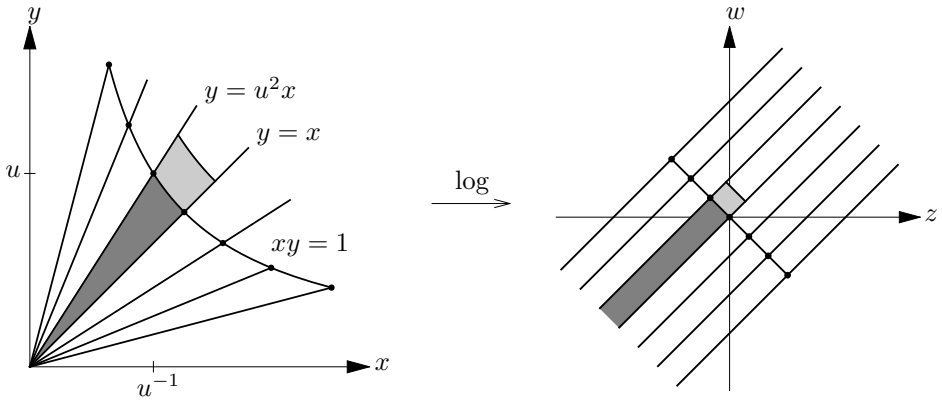

FIGURE 3. The logarithm map, a sector, and the normalized sector

From here, the real quadratic class number formula is proved by the argument from the imaginary quadratic fields writeup. Define

$$a_n = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = n\}.$$

By a weak form of the proposition's result that $A_n = h\kappa n + \mathcal{O}(n^{1/2})$,

$$\sum_{k=1}^{n} a_k = A_n = \mathcal{O}(n), \quad n \in \mathbb{Z}_{\ge 1},$$

and this estimate shows that the Dedekind zeta function of F,

$$\zeta_F(s) = \sum_{n\ge 1} \frac{a_n}{n^s},$$

is analytic on $\{\mathrm{Re}(s) > 1\}$. More incisively, because the proposition gives

$$\sum_{k=1}^{n} (a_k - h\kappa) = A_n - h\kappa n = \mathcal{O}(n^{1/2}), \quad n \in \mathbb{Z}_{\ge 1},$$

the difference

$$\zeta_F(s) - h\kappa\zeta(s) = \sum_{n\geq 1} \frac{a_n - h\kappa}{n^s}$$

is analytic on $\{\mathrm{Re}(s) > 1/2\}$; this says that $\zeta_F(s)$ and $h\kappa\zeta(s)$ have canceling poles at $s = 1$, and so

$$\mathrm{res}_{s=1}\, \zeta_F(s) = h\kappa.$$

But also $\zeta_F(s) = L(\chi_F, s)\zeta(s)$ for $\mathrm{Re}(s) > 1$ and then for $\mathrm{Re}(s) > 0$, giving

$$\mathrm{res}_{s=1}\, \zeta_F(s) = L(\chi_F, 1).$$

The two expressions for the residue give the real quadratic class number formula,

$$\boxed{h\kappa = L(\chi_F, 1),}$$

or

$$\frac{2h \log u}{\sqrt{D_F}} = L(\chi_F, 1).$$

In the imaginary quadratic case the boxed formula is

$$\frac{2\pi h}{w\sqrt{|D_F|}} = L(\chi_F, 1),$$

the main result of our imaginary quadratic field writeup.

Recall the formula for $L(\chi_F, 1)$ from Proposition 13.3 of the imaginary quadratic fields writeup,

$$L(\chi_F, 1) = -\frac{2}{\sqrt{D_F}} \sum_{1\leq r<D_F/2} \chi_F(r) \log(\sin(\pi r/D_F)) \quad \text{for } F \text{ real quadratic.}$$

This combines with the formula

$$h = \frac{\sqrt{D_F}}{2\log u} L(\chi_F, 1) = -\frac{1}{\log u} \sum_{1\leq r<D_F/2} \chi_F(r) \log(\sin(\pi r/D_F))$$

and with our previous table of fundamental units to give the table of real quadratic ideal class numbers in figure 4.

Some more results are shown in figure 5, in which *steps* reports the number of steps taken by the continued fraction algorithm to find the fundamental unit.

n	u	$\log u$	$\sum$	h
2	$1+\sqrt{2}$	0.881374	-0.881374	1
3	$2+\sqrt{3}$	1.31696	-1.31696	1
5	$\frac{1}{2}(1+\sqrt{5})$	0.481212	-0.481212	1
6	$5+2\sqrt{6}$	2.29243	-2.29243	1
7	$8+3\sqrt{7}$	2.76866	-2.76866	1
10	$3+\sqrt{10}$	1.81845	-3.63689	2
11	$10+3\sqrt{11}$	2.99322	-2.99322	1
13	$\frac{1}{2}(3+\sqrt{13})$	1.19476	-1.19476	1
14	$15+4\sqrt{14}$	3.40008	-3.40008	1
15	$4+\sqrt{15}$	2.06344	-4.12687	2
17	$4+\sqrt{17}$	2.09471	-2.09471	1
19	$170+39\sqrt{19}$	5.82894	-5.82894	1
21	$\frac{1}{2}(5+\sqrt{21})$	1.5668	-1.5668	1

FIGURE 4. Some real quadratic ideal class numbers

n	u	steps	h
127	$4730624+419775\sqrt{127}$	12	1
130	$57+5\sqrt{130}$	3	4
$4^{10}-1$	$2^{10}+\sqrt{4^{10}-1}$	2	2^5
$4^{11}-1$	$2^{11}+\sqrt{4^{11}-1}$	2	2^8
$4^{10}+1$	$2^{10}+\sqrt{4^{10}+1}$	3	90
$4^{11}+1$	$2^{11}+\sqrt{4^{11}+1}$	3	180
$4^{10}+2$	$4^{10}+1+2^{10}\sqrt{4^{10}+2}$	2	66
$4^{11}+2$	$4^{11}+1+2^{11}\sqrt{4^{11}+2}$	2	84

FIGURE 5. More real quadratic ideal class numbers