Universiteit
Leiden
The Netherlands

The unit residue group

Dalla Torre, G.

Citation
Dalla Torre, G. (2019, December 18). *The unit residue group*. Retrieved from https://hdl.handle.net/1887/82075

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/82075

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/82075 holds various files of this Leiden University dissertation.

Author: Dalla Torre G.
Title: The unit residue group
Issue Date: 2019-12-18

CHAPTER 8

Three-ranks of ideal class groups of quadratic number fields

8.1 Introduction

Let $d \in \mathbb{Z}_{>1}$ be squarefree and let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. The biquadratic number field K contains a primitive 3-rd root of unity and has its 3-rd unit residue group [Definition 5.3] and 3-rd virtual group [Definition 5.15]. The number field extension $K/\mathbb{Q}$ is Galois and the description of the Galois module structure of these two groups is one of the main results of the chapter [Theorem 8.1].

Theorem 8.1. *Let $d \in \mathbb{Z}_{>1}$ be squarefree, let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$, and let G be the Galois group of the extension $K/\mathbb{Q}$. Then the 3-rd unit residue group of K is a free $(\mathbb{Z}/3\mathbb{Z})[G]$-module of rank 1. Moreover, the 3-rd virtual group of K is a submodule of the 3-rd unit residue group of K and corresponds to exactly one of the following modules:*

(a) *the kernel of the natural map $(\mathbb{Z}/3\mathbb{Z})[G] \to (\mathbb{Z}/3\mathbb{Z})[\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})]$,*
(b) *the kernel of the natural map $(\mathbb{Z}/3\mathbb{Z})[G] \to (\mathbb{Z}/3\mathbb{Z})[\mathrm{Gal}(\mathbb{Q}(\sqrt{-3d})/\mathbb{Q})]$.*

Proof. This follows from Theorem 8.18 and Theorem 8.17. □

A classical theorem of Scholz [Theorem 8.19] states that the difference between the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$ and the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$ is either 0 or 1. Theorem 8.2 shows that these two cases can

be distinguished by looking at the Galois module structure of the 3-rd virtual group of K.

Theorem 8.2. *Let $d \in \mathbb{Z}_{>1}$ be squarefree, let r be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$, let s be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$, and let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. Then in case* (a) *of* Theorem 8.1 *one has $s = r + 1$ and in case* (b) *of* Theorem 8.1 *one has $s = r$.*

Proof. This follows from the G-decompositions of the $(\mathbb{Z}/3\mathbb{Z})[G]$-modules in cases (a) and (b) of Theorem 8.1 and Theorem 8.17. □

As a byproduct we get a new proof of Scholz's theorem, but the ingredients are really the same as in earlier proofs. In Section 8.3 we show the G-decompositions of some $(\mathbb{Z}/3\mathbb{Z})[G]$-modules and use the duality given by the norm-residue symbol. In this way we simultaneously apply class field theory and Kummer theory, as is done more explicitly in the proof of Scholz's Theorem [Theorem 10.10 of Chapter 10 in [74]] by Washington.

In 1984 Dutarte [14] proposed a probabilistic model [Section 8.5] that leads to Conjecture 8.3 and studied the compatibility of the Cohen–Lenstra heuristics with Scholz's theorem. He showed that the Cohen–Lenstra heuristics for real quadratic fields, Scholz's theorem, and Conjecture 8.3 give the same result for the proportion of imaginary quadratic fields with prescribed 3-rank as the Cohen-Lenstra heuristics for imaginary quadratic fields.

Conjecture 8.3 (Dutarte [14])**.** *Let D^+ be the set of discriminants of real quadratic number fields. For each number field L let Cl_L be its ideal class group. Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a+1\}|}{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|} = \frac{1}{3^{a+1}}.$$

In Dutarte's model Conjecture 8.3 is a statement about the existence and the value of a conditional probability: the probability that the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3\Delta})$ is the positive integer $a+1$ given that Δ is a discriminant of a real quadratic number field whose ideal class group has 3-rank a.

Following his model we state Conjecture 8.4.

Conjecture 8.4. *Let the notation be as in* Conjecture 8.3*. Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|} = \frac{1}{3^{a}}.$$

A natural assumption is Conjecture 8.5.

Conjecture 8.5. *Let the notation be as in* Conjecture 8.3. *Then for each pair* $(a, b) \in \mathbb{Z}^2$ *the limit*

$$\lim_{x \to +\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = b\}|}{|\{\Delta \in D^+ : \Delta < x\}|}$$

exists. Moreover, if one denotes its value by $\Pr^+(r = a, s = b)$, *then one has*

$$\sum_{(a,b) \in \mathbb{Z}^2} \Pr^+(r = a, s = b) = 1.$$

Theorem 8.6. *Let the notation be as in* Conjecture 8.3. *Assume* Conjecture 8.3, Conjecture 8.4, *and* Conjecture 8.5. *Then for each nonnegative integer* a *the limit*

$$\lim_{x \to +\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D^+ : \Delta < x\}|}$$

equals

$$3^{-a(a+1)} \prod_{i=1}^{\infty} (1 - 3^{-i}) \prod_{i=1}^{a} (1 - 3^{-i})^{-1} \prod_{i=1}^{a+1} (1 - 3^{-i})^{-1}.$$

Proof. This follows from Theorem 8.31. □

Remark 8.7. The value of the limit in Theorem 8.6 is the value conjectured by Cohen and Lenstra [11].

Theorem 8.6 shows that Dutarte's assumption [Conjecture 8.3], an analogous assumption [Conjecture 8.4], and a natural assumption [Conjecture 8.5] are sufficient to compute the probability that a real quadratic number field has prescribed 3-rank. Moreover, the value of this probability is exactly the one predicted by the Cohen–Lenstra heuristics.

Under the same hypotheses we also get a similar result for complex quadratic number fields [Theorem 8.31], but the fields in our limit are ordered in a different way from the way they are ordered in the Cohen–Lenstra heuristics [Remark 8.35]. We are able to get the same order and again the values predicted by Cohen and Lenstra for both real and imaginary quadratic number fields, if we group together quadratic number fields according to the divisibility by 3 of their discriminants [Theorem 8.42 and Remark 8.44].

The idea of considering the divisibility by 3 in this context is not new. In 2010 Fouvry and Klüners [16] showed that Conjecture 8.3 follows from the Cohen–Lenstra heuristics for quadratic number fields grouped according to the divisibility by 3 of their discriminants.

Lee generalized Dutarte's results for the prime number 3 to every prime number. In Lee's papers Scholz's theorem is replaced by the Spiegelungssatz, which is a generalization of Scholz's theorem, and he works with both number fields [33] and function fields [34].

8.2 Two results on modules

Lemma 8.8. *Let p be a prime number, let G be a group of order coprime to p, and let A be a finite $\mathbb{Z}[G]$-module. Then the quotient A/pA and the p-torsion $A[p]$ are isomorphic $(\mathbb{Z}/p\mathbb{Z})[G]$-modules.*

Proof. The multiplication by p map $A \to A$, $a \mapsto pa$, gives rise to the exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to A[p] \to A \to A \to A/pA \to 0.$$

It follows that the $\mathbb{Z}[G]$-modules $A[p] \oplus A$ and $A/pA \oplus A$ are Jordan–Hölder isomorphic and therefore so are the $\mathbb{Z}[G]$-modules $A[p]$ and A/pA. Since $A[p]$ and A/pA are $(\mathbb{Z}/p\mathbb{Z})[G]$-modules, they are also Jordan–Hölder isomorphic as $(\mathbb{Z}/p\mathbb{Z})[G]$-modules. By Maschke's Theorem the group ring $(\mathbb{Z}/p\mathbb{Z})[G]$ is semisimple. The existence of a $(\mathbb{Z}/p\mathbb{Z})[G]$-module isomorphism between $A[p]$ and A/pA follows from the semisimplicity of $(\mathbb{Z}/p\mathbb{Z})[G]$. □

Theorem 8.9. *Let L/K be a Galois extension of number fields and let G be its Galois group. Let p be a prime not dividing $|G|$ and let Cl_K and Cl_L be the ideal class groups of K and L, respectively. Then for each $m \in \mathbb{Z}_{\geq 0}$ the norm map $\mathrm{N}_{L/K} : L \to K$ induces the split exact sequence of $\mathbb{Z}[G]$-modules*

$$1 \to \ker(\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]) \to \mathrm{Cl}_L[p^m] \xrightarrow{\mathrm{N}_{L/K}} \mathrm{Cl}_K[p^m] \to 1$$

and the submodule of Galois invariant elements of $\mathrm{Cl}_L[p^m]$ is isomorphic to $\mathrm{Cl}_K[p^m]$.

Proof. Let $\mathrm{I}_{L/K} : \mathrm{Cl}_K \to \mathrm{Cl}_L$ be the group homomorphism induced by the natural injective map from the group of fractional ideals of K to the group of fractional ideals of L and let $\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]$ be the group homomorphism induced by the norm map. The composite map

$$\mathrm{N}_{L/K} \circ \mathrm{I}_{L/K} : \mathrm{Cl}_K[p^m] \to \mathrm{Cl}_K[p^m]$$

is the group automorphism $\mathrm{Cl}_K[p^m] \xrightarrow{\sim} \mathrm{Cl}_K[p^m]$, $a \mapsto a^{|G|}$. Hence, the map

$$\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]$$

is surjective and the map

$$\mathrm{I}_{L/K} : \mathrm{Cl}_K[p^m] \to \mathrm{Cl}_L[p^m]$$

is injective. We get the exact sequence of $\mathbb{Z}[G]$-modules

$$1 \to \ker(\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]) \to \mathrm{Cl}_L[p^m] \xrightarrow{\mathrm{N}_{L/K}} \mathrm{Cl}_K[p^m] \to 1.$$

This exact sequence splits, because up to an automorphism of $\mathrm{Cl}_K[p^m]$ the map $\mathrm{I}_{L/K} : \mathrm{Cl}_K[p^m] \to \mathrm{Cl}_L[p^m]$ is a section of the sequence.

Let $\mathrm{Cl}_L[p^m]^G$ be the submodule of Galois invariant elements of $\mathrm{Cl}_L[p^m]$. The map $\mathrm{I}_{L/K} \circ \mathrm{N}_{L/K}$ restricted to $\mathrm{Cl}_L[p^m]^G$ equals the group automorphism

$$\begin{aligned} \mathrm{Cl}_L[p^m]^G &\xrightarrow{\sim} \mathrm{Cl}_L[p^m]^G, \\ a &\mapsto a^{|G|}. \end{aligned}$$

Hence, the maps $\mathrm{I}_{L/K}$ and $\mathrm{N}_{L/K}$ induce $\mathbb{Z}[G]$-module isomorphisms between $\mathrm{Cl}_K[p^m]$ and $\mathrm{Cl}_L[p^m]^G$. □

8.3 Galois group decompositions of modules

Notation 8.10. Let $d \in \mathbb{Z}_{>1}$ be squarefree. Given a number field L, we denote by Cl_L its ideal class group. Let r and s be the 3-ranks of $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ and $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-3d})}$, respectively. Let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$, let E be the group of units of the ring of integers of K, and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. The group G is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Let σ and τ be the generators of the Galois groups $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3d}))$ and $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{d}))$, respectively. The group G has four characters $G \to \{\pm 1\}$. We denote the trivial character by ϵ. The three nontrivial characters of G factor through the quotient groups of G corresponding to the three quadratic fields $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{-3d})$, and $\mathbb{Q}(\sqrt{-3})$. We denote these characters by φ, ψ, and ω, respectively. Since 3 does not divide the order of G, by Maschke's Theorem the group ring $(\mathbb{Z}/3\mathbb{Z})[G]$ is semisimple. Given a $(\mathbb{Z}/3\mathbb{Z})[G]$-module M, we write it as direct sum of its G-components

$$M = M^{(\varepsilon)} \oplus M^{(\varphi)} \oplus M^{(\psi)} \oplus M^{(\omega)},$$

where on each component G acts by the corresponding character.

Let J be the group of ideles of K [Definition 4.19] and U be the group of unit ideles of K [Definition 4.21]. Given a subgroup S of J, we will write $\overline{S}$ for the quotient group $(S \cdot J^3)/J^3$. For any subgroup $H \subseteq \overline{J}$ we will denote by $H^\perp$ its annihilator in $\overline{J}$ with respect to the norm-residue symbol $(\cdot,\cdot) : \overline{J} \times \overline{J} \to \mu_3$, where μ_3 is the group of 3-rd roots of unity in K.

Theorem 8.11. *Let the notation be as in* Notation 8.10. *Then there is a natural* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module isomorphism*

$$E/E^3 \xrightarrow{\sim} \overline{E}$$

and the four groups in the direct sum of the G*-decomposition of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module* $\overline{E}$

$$\overline{E} = \overline{E}^{(\varepsilon)} \oplus \overline{E}^{(\varphi)} \oplus \overline{E}^{(\psi)} \oplus \overline{E}^{(\omega)}$$

have 3*-ranks* 0, 1, 0, *and* 1, *respectively.*

Proof. By Lemma 4.51 we get a natural $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$E/E^3 \xrightarrow{\sim} \overline{E}.$$

Let L be a subfield of K, let E_L the group of units of its ring of integers, and let H be the Galois of the extension K/L. Composing the natural inclusion $E_L \to E$ with the norm map $\mathrm{N}_{K/L} : K \to L$ induces the group automorphism

$$\begin{aligned} E_L/(E_L)^3 &\xrightarrow{\sim} E_L/(E_L)^3, \\ a &\mapsto a^{|H|}. \end{aligned}$$

Hence, the group homomorphism $E_L/(E_L)^3 \to E/E^3$ induced by the natural inclusion $E_L \to E$ is injective. Dirichlet's unit theorem implies the statement in Theorem 8.11. □

Theorem 8.12. *Let the notation be as in* Notation 8.10 *and let* M *one of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-modules* $\overline{J}/(\overline{K^*} \cdot \overline{U})$, $\mathrm{Cl}_K[3]$, *and* $\mathrm{Cl}_K \,/\, \mathrm{Cl}_K^3$. *Then the four groups in the direct sum of the* G*-decomposition of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module* M

$$M = M^{(\varepsilon)} \oplus M^{(\varphi)} \oplus M^{(\psi)} \oplus M^{(\omega)}$$

have 3*-ranks* 0, r, s, *and* 0, *respectively.*

Proof. Theorem 8.9 applied to the extension $K/\mathbb{Q}$ states that the submodule of G-invariant elements of $\mathrm{Cl}_K[3]$ is isomorphic to $\mathrm{Cl}_{\mathbb{Q}}[3]$. The submodule of G-invariant elements of $\mathrm{Cl}_K[3]$ is $\mathrm{Cl}_K[3]^{(\varepsilon)}$ and therefore we have the $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\mathrm{Cl}_K[3]^{(\varepsilon)} \xrightarrow{\sim} \mathrm{Cl}_{\mathbb{Q}}[3].$$

Since $\mathbb{Q}$ has class number one, the submodule $\mathrm{Cl}_{\mathbb{Q}}[3]^{(\varepsilon)}$ is trivial. Hence $\mathrm{Cl}_K[3]^{(\varphi)}$ is the submodule of τ-invariant elements of $\mathrm{Cl}_K[3]$. Now applying Theorem 8.9 to the Galois extension $K/\mathbb{Q}(\sqrt{d})$, whose Galois group is generated by τ, gives a $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\mathrm{Cl}_K[3]^{(\varphi)} \xrightarrow{\sim} \mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}[3].$$

Hence, we have $\operatorname{rk}_3 \operatorname{Cl}_K[3]^{(\varphi)} = r$. Similarly, we get the $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphisms

$$\operatorname{Cl}_K[3]^{(\psi)} \xrightarrow{\sim} \operatorname{Cl}_{\mathbb{Q}(\sqrt{-3d})}[3] \quad \text{and} \quad \operatorname{Cl}_K[3]^{(\omega)} \xrightarrow{\sim} \operatorname{Cl}_{\mathbb{Q}(\sqrt{-3})}[3].$$

Hence, we have $\operatorname{rk}_3 \operatorname{Cl}_K[3]^{(\psi)} = s$. Since the ideal class group of $\mathbb{Q}(\sqrt{-3})$ is trivial, we have $\operatorname{rk}_3 \operatorname{Cl}_K[3]^{(\omega)} = 0$.

Lemma 8.8 implies the existence of a $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\operatorname{Cl}_K[3] \xrightarrow{\sim} \operatorname{Cl}_K / \operatorname{Cl}_K^3 .$$

By the short exact sequence 4.81 there is a $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \xrightarrow{\sim} \operatorname{Cl}_K / \operatorname{Cl}_K^3 .$$

The statement in Theorem 8.12 follows. □

Lemma 8.13. *Let the notation be as in* Notation 8.10. *Then the norm-residue symbol*

$$(\cdot,\cdot) : \overline{J} \times \overline{J} \to \mu_3$$

splits into four perfect pairings

$$\overline{J}^{(\varepsilon)} \times \overline{J}^{(\omega)} \to \mu_3, \qquad \overline{J}^{(\omega)} \times \overline{J}^{(\varepsilon)} \to \mu_3,$$
$$\overline{J}^{(\varphi)} \times \overline{J}^{(\psi)} \to \mu_3, \qquad \overline{J}^{(\psi)} \times \overline{J}^{(\varphi)} \to \mu_3.$$

Proof. Let $\chi_1, \chi_2 \in \{\epsilon, \varphi, \psi, \omega\}$ and consider the pairing

$$\overline{J}^{(\chi_1)} \times \overline{J}^{(\chi_2)} \to \mu_3.$$

By Corollary 3.101 for each $g \in G$ we have $(ga, gb) = g\,(a, b)$. This implies that G acts on the image of the pairing through the character $\chi_1 \cdot \chi_2$. The group G acts on μ_3 through ω. If one has $\omega \neq \chi_1 \cdot \chi_2$, then the groups $\overline{J}^{(\chi_1)}$ and $\overline{J}^{(\chi_2)}$ are orthogonal. Since by Theorem 4.50 the norm-residue symbol is a perfect pairing, the statement in Lemma 8.13 follows. □

Lemma 8.14. *Let the notation be as in* Notation 8.10. *Then the norm-residue symbol induces a perfect pairing of finite abelian groups*

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \times \overline{K^*} \cap \overline{U}^{\perp} \to \mu_3$$

that splits into two perfect pairings of finite abelian groups

$$(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\varphi)} \times (\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \to \mu_3$$

and

$$(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\psi)} \times (\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mu_3.$$

Proof. The diagram in Section 4.8 shows that the annihilator of $\overline{K^*} \cap \overline{U}^{\perp}$ with respect to the norm-residue symbol is $\overline{K^*} \cdot \overline{U}$. Hence, the norm-residue symbol induces a perfect pairing of finite abelian groups

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \times \overline{K^*} \cap \overline{U}^{\perp} \to \mu_3.$$

The statement in Lemma 8.14 follows from Theorem 8.12 and Lemma 8.13. □

Theorem 8.15. *Let the notation be as in* Notation 8.10. *Then the four groups in the direct sum of the G-decomposition of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module $\overline{K^*} \cap \overline{U}^{\perp}$*

$$\overline{K^*} \cap \overline{U}^{\perp} = (\overline{K^*} \cap \overline{U}^{\perp})^{(\varepsilon)} \oplus (\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \oplus (\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \oplus (\overline{K^*} \cap \overline{U}^{\perp})^{(\omega)}$$

have 3-ranks 0, s, r, and 0, respectively.

Proof. By Theorem 8.12 we have

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) = (\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\varphi)} \oplus (\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\psi)}$$

and the 3-ranks of $(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\varphi)}$ and $(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\psi)}$ equal r and s, respectively. Lemma 8.14 implies that by duality these 3-ranks are equal to the 3-ranks of $(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)}$ and $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)}$, respectively. □

Theorem 8.16. *Let the notation be as in* Notation 8.10. *Then the four groups in the direct sum of the G-decomposition of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module $\overline{K^*} \cap \overline{U}$*

$$\overline{K^*} \cap \overline{U} = (\overline{K^*} \cap \overline{U})^{(\varepsilon)} \oplus (\overline{K^*} \cap \overline{U})^{(\varphi)} \oplus (\overline{K^*} \cap \overline{U})^{(\psi)} \oplus (\overline{K^*} \cap \overline{U})^{(\omega)}$$

have 3-ranks 0, $r+1$, s, and 1, respectively.

Proof. The group homomorphisms in Corollary 5.27 and Theorem 5.29 are $(\mathbb{Z}/3\mathbb{Z})[G]$-modules homomorphisms. Corollary 5.27 implies that the 3-Selmer group $\{3\text{-virtual units of } K\}/{K^*}^3$ of K and the group $\overline{K^*} \cap \overline{U}$ are isomorphic $(\mathbb{Z}/3\mathbb{Z})[G]$-modules. Using the short exact sequence of $(\mathbb{Z}/3\mathbb{Z})[G]$-modules

$$1 \longrightarrow E/E^3 \longrightarrow \{3\text{-virtual units of } K\}/{K^*}^3 \longrightarrow \mathrm{Cl}_K[3] \longrightarrow 1$$

given by Theorem 5.29, the statement in Theorem 8.16 follows from Theorem 8.11 and Theorem 8.12. □

Theorem 8.17. *Let the notation be as in* Notation 8.10 *and let V be the 3-rd virtual group of K* [Definition 5.15]. *Then the 3-ranks of the four groups in the direct sum of the G-decomposition of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module V*

$$V = V^{(\varepsilon)} \oplus V^{(\varphi)} \oplus V^{(\psi)} \oplus V^{(\omega)}$$

are either 0, 1, 0, and 1, or 0, 0, 1, and 1, respectively. Moreover, in the first case one has $s = r$ and in the second case one has $s = r + 1$.

Proof. The G-decomposition of the short exact sequence of $(\mathbb{Z}/3\mathbb{Z})[G]$-modules

$$1 \longrightarrow \overline{K^*} \cap \overline{U}^{\perp} \longrightarrow \overline{K^*} \cap \overline{U} \longrightarrow V \longrightarrow 1$$

in Remark 5.16 gives rise to four short exact sequences of $(\mathbb{Z}/3\mathbb{Z})[G]$-modules. Theorem 8.15 and Theorem 8.16 imply that the 3-ranks of $V^{(\varepsilon)}$ and $V^{(\omega)}$ are 0 and 1, respectively. Since by Corollary 5.18 the 3-rank of V equals 2, the 3-ranks of $V^{(\varphi)}$ and $V^{(\psi)}$ are either 1 and 0 or 0 and 1, respectively. Using again Theorem 8.15 and Theorem 8.16 we get the following. If the 3-ranks of $V^{(\varphi)}$ and $V^{(\psi)}$ are 1 and 0, respectively, then one has $s = r$, otherwise one has $s = r + 1$. □

Theorem 8.18. *Let the notation be as in* Notation 8.10. *Then the* 3*-rd unit residue group of* K [Definition 5.3] *is a free* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module of rank* 1.

Proof. By Theorem 5.10 the 3-rd unit residue group of K has 3-rank 4. Since it contains the 3-rd virtual group of K and is a skew abelian group by Corollary 5.2, the statement in Theorem 8.18 follows from Theorem 8.17 and Lemma 8.13. □

8.4 Scholz's theorem

A classical theorem in algebraic number theory about the 3-ranks of ideal class groups of quadratic number fields is Scholz's theorem [Theorem 8.19], which Scholz proved in 1932. It is often called the 'Mirror theorem' or the 'Reflection theorem'. These names are also used for Leopoldt's Spiegelungssatz [41], which is a generalization of Scholz's theorem.

Theorem 8.19 (Scholz [63])**.** *Let* $d \in \mathbb{Z}_{>1}$ *be squarefree, let* r *be the* 3*-rank of the ideal class group of* $\mathbb{Q}(\sqrt{d})$*, and let* s *be the* 3*-rank of the ideal class group of* $\mathbb{Q}(\sqrt{-3d})$*. Then one has*

$$r \leq s \leq r + 1.$$

Proof. This follows from Theorem 8.2. □

In our setting the proof of Scholz's theorem [Theorem 10.10 of Chapter 10 in [74]] by Washington gives rise to Theorem 8.20.

Theorem 8.20. *Let the notation be as in* Notation 8.10 *and let*

$$\overline{K^*} \cap \overline{U}^{\perp} \to \mathrm{Cl}_K[3] \tag{8.21}$$

be the $(\mathbb{Z}/3\mathbb{Z})[G]$*-module homomorphism obtained by composing the natural* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module homomorphism*

$$\overline{K^*} \cap \overline{U}^{\perp} \to (\overline{K^*} \cap \overline{U})/\overline{E}$$

with the $(\mathbb{Z}/3\mathbb{Z})[G]$*-module isomorphism*

$$(\overline{K^*} \cap \overline{U})/\overline{E} \xrightarrow{\sim} \mathrm{Cl}_K[3]$$

given by the short exact sequence 4.82*. Then the* G*-decomposition of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module homomorphism* 8.21 *gives rise to a group homomorphism with kernel of* 3*-rank at most* 1

$$(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mathrm{Cl}_K[3]^{(\varphi)}$$

from a group of 3*-rank* s *to a group of* 3*-rank* r *and an injective group homomorphism*

$$(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \to \mathrm{Cl}_K[3]^{(\psi)}$$

from a group of 3*-rank* r *to a group of* 3*-rank* s*.*

Proof. It follows from Theorem 8.12 and Theorem 8.15 that both the groups $\mathrm{Cl}_K[3]^{(\varphi)}$ and $(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)}$ have 3-rank r and both the groups $\mathrm{Cl}_K[3]^{(\psi)}$ and $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)}$ have 3-rank s. By Theorem 8.11 the 3-ranks of $\overline{E}^{(\varphi)}$ and $\overline{E}^{(\psi)}$ equal 1 and 0, respectively. Since the kernel of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module homomorphism

$$\overline{K^*} \cap \overline{U}^{\perp} \to (\overline{K^*} \cap \overline{U})/\overline{E}$$

is contained in $\overline{E}$, the statement in Theorem 8.20 follows. □

Remark 8.22. The cases $s = r + 1$ and $s = r$ in Theorem 8.19 both occur. For instance, we have $r = 0$ and $s = 1$ for $d = 29$ and $r = s = 1$ for $d = 79$. Theorem 8.20 suggests distinguishing three cases.

(a) One has $s = r$ and the map $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mathrm{Cl}_K[3]^{(\varphi)}$ is an isomorphism.

(b) One has $s = r$ and the map $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mathrm{Cl}_K[3]^{(\varphi)}$ has both kernel and cokernel of dimension 1 over $\mathbb{Z}/3\mathbb{Z}$.

(c) One has $s = r + 1$.

Note that the last case occurs if and only if the injective group homomorphism

$$(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \to \mathrm{Cl}_K[3]^{(\psi)}$$

is not an isomorphism. We have examples of these three cases for $d = 142$, for $d = 79$, and for $d = 29$, respectively.

8.5 Dutarte's probabilistic model

Let $d \in \mathbb{Z}_{>1}$ be squarefree and let r be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$. Scholz's theorem [Theorem 8.19] states that the 3-rank of the ideal

class group of $\mathbb{Q}(\sqrt{-3d})$ is either r or $r+1$. These two cases are characterized in Theorem 8.2 using the Galois module structure of the 3-rd virtual group of the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. In 1984 Dutarte [14] proposed a probabilistic model, which we present in our setting.

Theorem 8.23. *Let the notation be as in* Notation 8.10. *Then the following are equivalent.*

(i) *The natural group homomorphism* $(\overline{K^*} \cap \overline{U})^{(\varphi)} \to (\overline{U}/\overline{U}^{\perp})^{(\varphi)}$ *is trivial.*
(ii) *One has* $s = r+1$.

Proof. By Remark 5.16 the kernel of the natural group homomorphism

$$(\overline{K^*} \cap \overline{U})^{(\varphi)} \to (\overline{U}/\overline{U}^{\perp})^{(\varphi)}$$

is $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)}$, which has 3-rank s by Theorem 8.15. The group $(\overline{K^*} \cap \overline{U})^{(\varphi)}$ has 3-rank $r+1$ by Theorem 8.16. The statement in Theorem 8.23 follows. □

Remark 8.24. By Theorem 8.18 the group $(\overline{U}/\overline{U}^{\perp})^{(\varphi)}$ in Theorem 8.23 has 3-rank 1. Hence, the natural group homomorphism in Theorem 8.23 is a group homomorphism from an elementary abelian 3-group of rank $r+1$ to a group of order 3.

Let a be a nonnegative integer and let D_a^+ be the set of discriminants of real quadratic number fields whose ideal class groups have 3-rank a. To each $\Delta \in D_a^+$ we associate the natural group homomorphism in Theorem 8.23 for the number field $K = \mathbb{Q}(\sqrt{\Delta},\sqrt{-3})$, which is a group homomorphism from an elementary abelian 3-group of rank $a+1$ to a group of order 3 by Remark 8.24. Since there are 3^{a+1} group homomorphisms from an elementary abelian 3-group of rank $a+1$ to a group of order 3, Dutarte assumes that the density in D_a^+ of the subset of discriminants with associated trivial group homomorphism is $1/3^{a+1}$. Hence, he writes that $1/3^{a+1}$ is the value of the probability that the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3\Delta})$ is the positive integer $a+1$ given that one has $\Delta \in D_a^+$. The formalization of this assumption is Conjecture 8.3.

Theorem 8.25. *Let the notation be as in* Notation 8.10. *Then the following are equivalent.*

(i) *The natural group homomorphism* $(\overline{K^*} \cap \overline{U})^{(\psi)} \to (\overline{U}/\overline{U}^{\perp})^{(\psi)}$ *is trivial.*
(ii) *One has* $s = r$.

Proof. By Remark 5.16 the kernel of the natural group homomorphism

$$(\overline{K^*} \cap \overline{U})^{(\psi)} \to (\overline{U}/\overline{U}^{\perp})^{(\psi)}$$

is $(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)}$, which has 3-rank r by Theorem 8.15. The group $(\overline{K^*} \cap \overline{U})^{(\psi)}$ has 3-rank s by Theorem 8.16. The statement in Theorem 8.25 follows. □

8.6 Some consequences

Notation 8.26. Let D^+ be the set of discriminants of real quadratic number fields. Given a number field L we denote by Cl_L its ideal class group. We define the maps

$$r : D^+ \to \mathbb{Z}_{\geq 0} \qquad \text{and} \qquad s : D^+ \to \mathbb{Z}_{\geq 0}$$
$$\Delta \mapsto \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} \qquad\qquad \Delta \mapsto \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})}$$

in order to evaluate the 3-ranks of ideal class groups of quadratic number fields. Let A be a subset of D^+. We define the probability $\Pr^+(A)$ of A as being equal to the limit, if it exists,

$$\Pr^+(A) = \lim_{x \to +\infty} \frac{|\{\Delta \in A : \Delta < x\}|}{|\{\Delta \in D^+ : \Delta < x\}|}.$$

To shorten the notation, for each integer a we will write $\Pr^+(r = a)$ and $\Pr^+(s = a)$ for the probability of the subsets $\{\Delta \in D^+ : \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}$ and $\{\Delta \in D^+ : \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}$ of D^+, respectively. Moreover, we denote by D_0^+ and D_*^- the sets $\{\Delta \in D^+ : \Delta \equiv 0 \bmod 3\}$ and $\{\Delta \in D^- : \Delta \not\equiv 0 \bmod 3\}$, respectively.

Remark 8.27. The left-hand sides of the equalities in Conjecture 8.3 and Conjecture 8.4 can be thought of as conditional probabilities. We will denote them by $\Pr^+(s = a + 1 \mid r = a)$ and $\Pr^+(r = a \mid s = a)$, respectively.

In the proof of Theorem 8.31 we will use some identities of power series that come from the generating function for the number of partitions of positive integers.

Definition 8.28 (Durfee number)**.** The *Durfee number* of a partition of a positive integer is the largest integer i such that the partition contains at least i summands of size at least i.

Remark 8.29. The Durfee number of a partition of a positive integer is the size of the largest square that is contained within the Ferrers diagram of the partition.

Lemma 8.30 follows from Corollary 6.7 in [11] by Cohen and Lenstra, but it can also be proved directly, as we do here.

Lemma 8.30. *One has the identities of power series*

$$1 + \sum_{i>0} \frac{x^{i^2}}{\prod_{j=1}^{i} (1 - x^j)^2} = 1 + \sum_{i>0} x^i \prod_{j=1}^{i} \left(\frac{1}{1 - x^j} \right) = \prod_{i>0} \frac{1}{1 - x^i}.$$

Proof. We write the generating function for the number of partitions of positive integers. The first two expressions are obtained by grouping partitions according to their Durfee number and the size of their largest addend, respectively. The last one is the usual formula. □

Theorem 8.31. *Let the notation be as in* Notation 8.26. *Assume* Conjecture 8.3, Conjecture 8.4, *and* Conjecture 8.5. *Then for each nonnegative integer a one has*

$$\Pr^+(r = a) = 3^{-a(a+1)} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-1} \prod_{i=1}^{a+1}(1 - 3^{-i})^{-1}$$

and

$$\Pr^+(s = a) = 3^{-a^2} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-2}.$$

Proof. Let a be a nonnegative integer. Using the notation in Remark 8.27, Conjecture 8.3 states the equality

$$\Pr^+(s = a + 1 \mid r = a) = 1/3^{a+1}$$

and Scholz's theorem implies the equality

$$\Pr^+(s = a + 1 \mid r = a) + \Pr^+(s = a \mid r = a) = 1.$$

Hence, we have

$$\Pr^+(s = a \mid r = a) = 1 - 1/3^{a+1}.$$

Conjecture 8.5 states the existence of the probabilities $\Pr^+(r = a, s = a + 1)$ and $\Pr^+(r = a, s = a)$. From the equalities

$$\Pr^+(r = a, s = a + 1) = \Pr^+(s = a + 1 \mid r = a) \cdot \Pr^+(r = a)$$

and

$$\Pr^+(r = a, s = a) = \Pr^+(s = a \mid r = a) \cdot \Pr^+(r = a)$$

we get

$$\Pr^+(r = a, s = a + 1) = \Pr^+(s = a + 1 \mid r = a) \cdot \frac{\Pr^+(r = a, s = a)}{\Pr^+(s = a \mid r = a)}$$

and therefore

$$\Pr^+(r = a, s = a + 1) = \Pr^+(r = a, s = a)(3^{a+1} - 1)^{-1}. \tag{8.32}$$

Similarly, Conjecture 8.4 and Scholz's theorem imply for each nonnegative integer a the equality

$$\Pr^+(r = a+1, s = a+1) = \Pr^+(r = a, s = a+1)(3^{a+1} - 1)^{-1}. \tag{8.33}$$

The left-hand side of the equality

$$\sum_{(a,b)\in\mathbb{Z}^2} \Pr^+(r = a, s = b) = 1$$

in Conjecture 8.5 can be written as

$$\Pr^+(r = 0, s = 0) + \sum_{b=1}^{\infty} \sum_{a=b-1}^{b} \Pr^+(r = a, s = b).$$

Setting $y = \Pr^+(r = 0, s = 0)$ and using recursively (8.32) and (8.33) we get the equation in y

$$y\left(1 + \sum_{b=1}^{\infty}\left(\frac{3^b - 1}{\prod_{i=1}^{b}(3^i - 1)^2} + \frac{1}{\prod_{i=1}^{b}(3^i - 1)^2}\right)\right) = 1. \tag{8.34}$$

Since for all positive integers b we have

$$\frac{3^b - 1}{\prod_{i=1}^{b}(3^i - 1)^2} + \frac{1}{\prod_{i=1}^{b}(3^i - 1)^2} = \frac{3^b}{\prod_{i=1}^{b}(3^i - 1)^2} = \frac{(1/3)^{b^2}}{\prod_{i=1}^{b}(1 - (1/3)^i)^2},$$

we rewrite (8.34) as

$$y\left(1 + \sum_{b=1}^{\infty}\frac{(1/3)^{b^2}}{\prod_{i=1}^{b}(1 - (1/3)^i)^2}\right) = 1.$$

By Lemma 8.30 the solution is $y = \prod_{i=1}^{\infty}(1 - 3^{-i})$, which is the value predicted

by Cohen and Lenstra. Using (8.32) and (8.33), for all $a, b \in \mathbb{Z}_{\geq 0}$ we get

$$\Pr^+(r = a, s = b) = \begin{cases} 3^{-a(a+1)} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-2} & \text{if } b = a, \\ 3^{-(a+1)^2} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-1} \prod_{i=1}^{a+1}(1-3^{-i})^{-1} & \text{if } b = a+1, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, for each nonnegative integer a from the equality

$$\Pr^+(r = a) = \Pr^+(r = a, s = a) + \Pr^+(r = a, s = a+1)$$

we get the value conjectured by Cohen and Lenstra

$$\Pr^+(r = a) = 3^{-a(a+1)} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-1} \prod_{i=1}^{a+1}(1-3^{-i})^{-1}.$$

Similarly, for each nonnegative integer a we get

$$\Pr^+(s = a) = 3^{-a^2} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-2}. \qquad \square$$

Remark 8.35. Let D^- be the set of discriminants of complex quadratic number fields. The value conjectured by Cohen and Lenstra [11] of the limit

$$\lim_{x \to +\infty} \frac{|\{\Delta \in D^- : |\Delta| < x,\ \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D^- : |\Delta| < x\}|}$$

is the value of the probability

$$\Pr^+(s = a) = \lim_{x \to +\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\ \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D^+ : \Delta < x\}|}$$

in Theorem 8.31. Note that the complex quadratic number fields appear in different orders in the two limits. This is caused by the fact that D^- is not involved in any of the limits in Conjecture 8.3, Conjecture 8.4, and Conjecture 8.5.

Remark 8.36. Let D^- be the set of discriminants of complex quadratic number fields. The natural definition of the map s in Notation 8.26 is

$$\begin{aligned} s : D^- &\to \mathbb{Z}_{\geq 0}, \\ \Delta &\mapsto \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})}\,. \end{aligned}$$

Similarly to the real case, given a subset A of D^-, we define the probability $\Pr^-(A)$ of A. Now the problem is the connection between $\Pr^+$ and $\Pr^-$, in particular the map between D^+ and D^-. A way of dealing with this problem is to restrict to subsets of D^+ and D^- that have an order-reversing bijection induced by the reflection map. For example, the maps

$$\begin{aligned} f : \{\Delta \in D^+ : \Delta \equiv 0 \bmod 3\} &\to \{\Delta \in D^- : \Delta \not\equiv 0 \bmod 3\}, \\ \Delta &\mapsto -\Delta/3, \end{aligned}$$

and

$$\begin{aligned} \{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\} &\to \{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}, \\ \Delta &\mapsto -3\Delta, \end{aligned}$$

are order-reversing bijections.

We restrict ourselves to considering the sets $\{\Delta \in D^+ : \Delta \equiv 0 \bmod 3\}$ and $\{\Delta \in D^- : \Delta \not\equiv 0 \bmod 3\}$. Conjecture 8.37, Conjecture 8.38, Conjecture 8.40, and Theorem 8.42. correspond to Conjecture 8.3, Conjecture 8.4, Conjecture 8.5, and Theorem 8.31, respectively. An analogous discussion can be given for the sets $\{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\}$ and $\{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}$ [Remark 8.44].

Conjecture 8.37. *Let the notation be as in* Notation 8.26. *Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a+1\}|}{|\{\Delta \in D_0^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|} = \frac{1}{3^{a+1}}$$

Conjecture 8.38. *Let the notation be as in* Notation 8.26. *Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_*^- : |\Delta| < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D_*^- : |\Delta| < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|} = \frac{1}{3^{a}}$$

Remark 8.39. The left-hand sides of the equalities in Conjecture 8.37 and Conjecture 8.38 can be thought of as conditional probabilities. We will denote them by $\Pr_0^+(s \circ f = a+1 \mid r = a)$ and $\Pr_*^-(r \circ f^{-1} = a \mid s = a)$, respectively.

Conjecture 8.40. *Let the notation be as in* Notation 8.26. *Then for each pair $(a, b) \in \mathbb{Z}^2$ the limit*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = b\}|}{|\{\Delta \in D_0^+ : \Delta < x\}|}$$

exists. Moreover, if one denotes its value by $\Pr_0^+(r = a, s \circ f = b)$*, then one has*

$$\sum_{(a,b)\in\mathbb{Z}^2} \Pr_0^+(r = a, s \circ f = b) = 1.$$

Remark 8.41. The limit in Conjecture 8.40 equals the limit

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_*^- : |\Delta| < x,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = b\}|}{|\{\Delta \in D_*^- : |\Delta| < x\}|},$$

because the map f is order-reversing. We will denote the equality of their values by

$$\Pr_0^+(r = a, s \circ f = b) = \Pr_*^-(r \circ f^{-1} = a, s = b).$$

Theorem 8.42. *Let the notation be as in* Notation 8.26*. For each nonnegative integer* a *let*

$$\Pr_0^+(r = a) = \lim_{x\to+\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D_0^+ : \Delta < x\}|}$$

and

$$\Pr_*^-(s = a) = \lim_{x\to+\infty} \frac{|\{\Delta \in D_*^- : |\Delta| < x,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D_*^- : |\Delta| < x\}|}.$$

Assume Conjecture 8.37*,* Conjecture 8.38*, and* Conjecture 8.40*. Then for each nonnegative integer* a *one has*

$$\Pr_0^+(r = a) = 3^{-a(a+1)} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-1} \prod_{i=1}^{a+1}(1 - 3^{-i})^{-1}$$

and

$$\Pr_*^-(s = a) = 3^{-a^2} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-2}.$$

Proof. Let a be a nonnegative integer. Conjecture 8.37 and Conjecture 8.38 state the equalities

$$\Pr_0^+(s \circ f = a + 1 \mid r = a) = \frac{1}{3^{a+1}}$$

and

$$\Pr_*^-(r \circ f^{-1} = a \mid s = a) = \frac{1}{3^a},$$

respectively. Conjecture 8.40 states the equality

$$\sum_{(a,b)\in\mathbb{Z}^2} \Pr_0^+(r = a, s \circ f = b) = 1.$$

Remark 8.41 states the equality

$$\Pr_0^+(r = a, s \circ f = b) = \Pr_*^-(r \circ f^{-1} = a, s = b).$$

Since the map f is order-reversing, we have

$$\Pr_*^-(s = a) = \lim_{x \to +\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x, \operatorname{rk}_3 \operatorname{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D_0^+ : \Delta < x\}|}.$$

We conclude by following the steps of the proof of Theorem 8.31 with $\Pr^+$ replaced by $\Pr_0^+$. □

Remark 8.43. The values of the limits in Theorem 8.42 are the values conjectured by Cohen and Lenstra [11].

Remark 8.44. Since the map

$$\begin{aligned} \{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\} &\to \{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}, \\ \Delta &\mapsto -3\Delta, \end{aligned}$$

is order-reversing, we can replace D_0^+ and D_*^- by $\{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\}$ and $\{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}$, respectively, in Conjecture 8.37, Conjecture 8.38, Conjecture 8.40, and Theorem 8.42.