JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

PETER STEVENHAGEN

Frobenius distributions for real quadratic orders

Journal de Théorie des Nombres de Bordeaux, tome 7, nº 1 (1995), p. 121-132

<http://www.numdam.org/item?id=JTNB_1995__7_1_121_0>

Journal de Théorie des Nombres
de Bordeaux 7 *(1995), 121–132*

Frobenius distributions for real quadratic orders

par Peter STEVENHAGEN

ABSTRACT. – We present a density result for the norm of the fundamental unit in a real quadratic order that follows from an equidistribution assumption for the infinite Frobenius elements in the class groups of these orders.

1. Introduction

This paper deals with the distribution of the Frobenius element of the infinite prime over the class group in certain families of real quadratic orders. It contains precise results for these distributions that are at this moment mostly conjectural, but provide a satisfactory 'explanation' for observations that have not been understood otherwise, such as those concerning the frequency of real quadratic fields having fundamental unit of norm -1. They are somewhat similar in spirit to the Cohen-Lenstra heuristics [3], which 'explain' the average behavior of class groups of number fields. However, our underlying assumptions are of a more specific nature than those in [3], and weak versions of our density results can actually be proved. Our conjectures answer an old open question that goes back at least to Euler, but does not seem to appear explicitly in the literature any earlier than in a 1932 paper by Nagell [5].

Nagell's question concerns the solvability of the well known *negative Pell equation*

$$x^2 - dy^2 = -1$$

for non-square $d \in \mathbf{Z}_{>1}$ in integers $x, y \in \mathbf{Z}$. A necessary condition for solvability is obviously that -1 is a square modulo all divisors of d, i.e. that d is not divisible by 4 or a prime $p \equiv 3 \bmod 4$. This can be phrased more concisely by stating that d is the sum of two coprime squares. Thus, let us denote by $\mathcal{S}$ the set of integers that can be written as the sum of two coprime squares. With $\mathcal{S}^-$ denoting the set of integers d for which

1991 *Mathematics Subject Classification.* Primary 11R11, 11R45, 11R65; Secondary 11D09.

Mots clefs : Real quadratic fields, quadratic units, Pell equation.

Manuscrit reçu le 16 Février 1994, version définitive le 27 Avril 1995.

$x^2 - dy^2 = -1$ has integral solutions, Nagell's question is: does $\mathcal{S}^-$ have a natural density in $\mathcal{S}$, i.e. does the limit

$$Q = \lim_{X\to\infty} \frac{\#\{d \in \mathcal{S}^- : d \leq X\}}{\#\{d \in \mathcal{S} : d \leq X\}}$$

exist? It appears that the well known characterization of $\mathcal{S}^-$ as the set of integers $d > 1$ for which $\sqrt{d}$ has a continued fraction expansion with odd period length is not of any use in answering this question, and it is not even known whether the liminf and the limsup of this expression are in the open interval $(0, 1)$. The same applies to the somewhat simpler question that is obtained by restricting to squarefree d in Nagell's problem or, equivalently, by posing the problem for real quadratic fields. More precisely, let $\mathcal{D}$ be the set of real quadratic fields K for which -1 is in the norm image $N_{K/\mathbf{Q}}K^*$ and $\mathcal{D}^- \subset \mathcal{D}$ the subset of fields $K \in \mathcal{D}$ for which the norm of the fundamental unit equals -1. Then we have $\mathcal{D} = \{\mathbf{Q}(\sqrt{d}) : d \in \mathcal{S}\}$ and—even though $\mathcal{O}_K$ may not be of the form $\mathbf{Z}[\sqrt{d}]$—also $\mathcal{D}^- = \{\mathbf{Q}(\sqrt{d}) : d \in \mathcal{S}^-\}$. The analogue of Nagell's question, which has been studied extensively by Rédei [7], can now be phrased as: does the limit

$$P = \lim_{X\to\infty} \frac{\#\{K \in \mathcal{D}^- : \Delta(K) \leq X\}}{\#\{K \in \mathcal{D} : \Delta(K) \leq X\}}$$

exist and, if it does, what is its value? Existing tables as those occurring in [1] and [5] show that the value of this fraction is around .860 for $X = 10^4$ and decreases slowly to assume the value .799 for $X = 10^7$. The considerations in this paper make it very plausible that the answer to both questions is the following.

CONJECTURE. *The limit values P and Q exist and are equal to*

$$P = 1 - \prod_{j\geq 1 \text{ odd}} (1 - 2^{-j}) = .5805775582\ldots$$

and

$$Q = P \cdot \prod_{\substack{p \text{ prime} \\ p\equiv 1 \bmod 4}} \left(1 + \frac{\psi(p)}{p^2 - 1}\right)\left(1 - \frac{1}{p^2}\right) = .57339\ldots,$$

where $\psi(p)$ is defined as

$$\psi(p) = \frac{2 + (1 + 2^{1-v_p})p}{2(p+1)},$$

with v_p denoting the number of factors 2 occurring in $p-1$.

We will see in the next section why the convergence to these limit values is extremely slow.

The densities in our conjecture give rise to absolute estimates for the number of $d \in \mathcal{S}^-$ and $K \in \mathcal{D}^-$, as the counting functions for the sets $\mathcal{S}$ and $\mathcal{D}$ are known to satisfy the asymptotic relations

$$\#\{d \in \mathcal{S} : d \leq X\} \sim \Big\{\frac{3}{2\pi} \prod_{\substack{p \text{ prime} \\ p\equiv 1 \bmod 4}} (1-p^{-2})^{-1/2}\Big\} \cdot \frac{X}{\sqrt{\log X}}.$$

and

$$\#\{K \in \mathcal{D} : \Delta(K) \leq X\} \sim \Big\{\frac{9}{8\pi} \prod_{\substack{p \text{ prime} \\ p\equiv 1 \bmod 4}} (1-p^{-2})^{1/2}\Big\} \cdot \frac{X}{\sqrt{\log X}}.$$

These relations are consequences of results of Rieger [8].

2. The fundamental case

In this section we reduce the density problem for real quadratic fields from the introduction to a statement on Frobenius distributions and explain how this gives rise to the indicated value of P.

Suppose we are given a quadratic field $K \in \mathcal{D}$ with discriminant D, ring of integers $\mathcal{O}$ and class group Cl. Denote by C the narrow class group of K, which may be identified with the class group of binary quadratic forms of discriminant D. There is a natural surjection $C \twoheadrightarrow Cl$ whose kernel is generated by the class $F_\infty \in C$ of the principal ideal generated by $\sqrt{D}$. If $\mathcal{O}$ contains a unit ε of negative norm, then the ideal $\sqrt{D}\cdot\mathcal{O}$ can be generated by the element $\varepsilon\sqrt{D}$ of norm $D > 0$ and F_∞ is the unit element in C. If all units in $\mathcal{O}$ have norm 1, then F_∞ has order 2 in C. Thus, we have $K \in \mathcal{D}^-$ if and only if F_∞ is the trivial element in C.

By class field theory, we can identify C with the Galois group over K of the narrow Hilbert class field H of K. The maximal real subextension H^+/K of H/K corresponds to the factor group Cl of C, so F_∞ generates the decomposition group of the real prime in $H/\mathbf{Q}$ and can be viewed as the *Frobenius element at infinity*. Our conjecture for real quadratic fields tells us that we should expect the Frobenius F_∞ for the family $\mathcal{D}$ of real quadratic fields to be trivial with probability P. The Cohen-Lenstra heuristics on the average behavior of class groups explicitly exclude the 2-parts of quadratic class groups that we have to deal with here. The reason for this is that these 2-parts are not at all 'random' in their sense of the word, and consequently we should not expect F_∞ to behave as a 'random 2-torsion element in a random abelian 2-group'.

What we have to take into account when studying the average behavior of the element $F_\infty \in C$ is that this Frobenius element is not only in the 2-torsion subgroup $C[2]$ of *ambigous ideal classes*, but also in the *principal genus* $C^2 \subset C$ of squares in C. If D has exactly t distinct prime divisors, then there are t ramified prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ in $\mathcal{O}$, and it is a classical theorem that the classes of these ideals in C generate the 2-torsion subgroup $C[2] \subset C$, subject to a single non-trivial relation. More precisely, if $V = \mathbf{F}_2^t$ is a vector space of dimension t with standard basis over the field of two elements and $\psi : V \to C[2]$ maps the i-th basis vector in V to the class of $\mathfrak{p}_i$ in C, then ψ is surjective and its kernel is 1-dimensional. As F_∞ is by definition the ideal class of $\prod_{i=1}^t \mathfrak{p}_i$ in C, we want to know how often $F_\infty = 0$ is the non-trivial relation between the classes of the ideals $\mathfrak{p}_i$, i.e. how often the element $u = (1)_{i=1}^t \in V$ mapping to F_∞ generates the kernel of ψ. We take into account that u lies in the subspace $V' = \psi^{-1}(C[2] \cap C^2)$, and that the dimension of V' equals $e+1$, where $e = \log_2(\#(C[2] \cap C^2))$ is the *4-rank* of the class group C.

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{F}_2 \cdot u \arrow[r] \arrow[d, equal] & V = \mathbf{F}_2^t \arrow[r, "\psi"] \arrow[d, phantom, "\cup"] & C[2] \arrow[r] \arrow[d, phantom, "\cup"] & 0 \\
0 \arrow[r] & \mathbf{F}_2 \cdot u \arrow[r] & V' \arrow[r] & C[2] \cap C^2 \arrow[r] & 0
\end{tikzcd}$$

This reduces the question to linear algebra on a vector space V' whose dimension does not depend on the 2-rank of C (which, as we have seen, is one less than the number t of prime divisors of D), but only on the 4-rank of C (which, a priori, is merely bounded by $t-1$). Thus for $e \geq 0$, we write $\mathcal{D}(e)$ for the set of real quadratic fields $K \in \mathcal{D}$ for which the 4-rank of the narrow class group C equals e. For $K \in \mathcal{D}(e)$, we want the non-zero element u in the $(e+1)$-dimensional vector space V' to be the generator of the 1-dimensional subspace $\ker \psi \subset V'$. If we assume (somewhat sloppily, given our present notation) that $\ker \psi$ should behave like a 'random 1-dimensional space of V', we expect the following to hold.

2.1. CONJECTURE. *For every $e \geq 0$, the subset $\mathcal{D}(e)^- = \mathcal{D}(e) \cap \mathcal{D}^-$ has natural density $(2^{e+1}-1)^{-1}$ in $\mathcal{D}(e)$.*

Extensive numerical evidence for this conjecture is provided in [2].

Conjecture 2.1 is a theorem for $e = 0$, in which case the 2-Hilbert class field of K equals the genus field of K, and it suffices to observe that the genus field of a real quadratic field is real if and only if we have $K \in \mathcal{D}$.

A serious problem in proving 2.1 seems to be that we cannot say anything without fixing the number of primes t in D. More precisely, the best thing that seems to be within reach at the moment is a result for the subset $\mathcal{D}_t$ of $\mathcal{D}$ consisting of discriminants having exactly t distinct prime divisors. Set $\mathcal{D}_t(e) = \mathcal{D}_t \cap \mathcal{D}(e)$ and $\mathcal{D}_t(e)^- = \mathcal{D}_t \cap \mathcal{D}(e)^-$. Then 2.1 can be formulated as follows for the sets $\mathcal{D}_t$.

2.2. Conjecture. *For every pair (t, e) of integers satisfying $0 \leq e < t$, the subset $\mathcal{D}_t(e)^-$ has natural density $(2^{e+1} - 1)^{-1}$ in $\mathcal{D}(e)$.*

So far, we can only prove upper and lower densities for $\mathcal{D}_t(e)^-$ in $\mathcal{D}_t(e)$ that are not too far from the conjectured density $(2^{e+1}-1)^{-1}$. For instance, it is shown in [11] that, for every $t > e$, the upper density of $\mathcal{D}_t(e)^-$ in $\mathcal{D}_t(e)$ is bounded by 2^{-e}, so the probability for the Frobenius $F_\infty \in C$ to be trivial decreases indeed exponentially with the 4-rank e of C. For the values $e = 1$ and $e = 2$ there are in addition the non-trivial lower bounds $1/4$ and $1/32$ for the lower density of $\mathcal{D}_t(e)^-$ in $\mathcal{D}_t(e)$.

The problem of deriving density results for $\mathcal{D} = \cup_{t \geq 1} \mathcal{D}_t$ from results on the subsets $\mathcal{D}_t$ also arises when we want to prove that each subset $\mathcal{D}(e)$ has a natural density in $\mathcal{D}$, which is necessary to obtain the value of P in 1.1 from our conjecture 2.1. Again, if we fix the number of primes in D, there is the following precise result. For the details of the proof we refer again to [11].

2.3. Theorem. *For each pair (t, e) of non-negative integers satisfying $t > e$, the set $\mathcal{D}_t(e)$ has a natural density inside $\mathcal{D}_t$ that is equal to*

$$\alpha_t(e) = 2^{-\binom{e+1}{2}} \frac{\prod_{j=e+1}^{t-1}(1 - 2^{-j})}{\prod_{j=1}^{[(t-e-1)/2]}(1 - 2^{-2j})}.$$

In order to get rid of the dependence on t, one observes that the number $\omega(D)$ of distinct prime factors of D has a normal order that tends to infinity with D. More precisely, one can show [4, theorem 431] that for every $\epsilon > 0$, the set of D satisfying

$$(1 - \epsilon) \log\log(D) < \omega(D) < (1 + \epsilon) \log\log(D)$$

has density 1. It is therefore very plausible to expect that $\mathcal{D}(e)$ has a natural density in $\mathcal{D}$ for every $e \geq 0$, and that this density can be evaluated by passing to the limit $t \to \infty$ in 2.3, yielding a value

$$\alpha_\infty(e) = \lim_{t\to\infty} \alpha_t(e) = \frac{\prod_{j\geq 1 \text{ odd}}(1-2^{-j})}{\prod_{j=1}^{e}(2^j-1)} = \frac{1-P}{\prod_{j=1}^{e}(2^j-1)}.$$

However, the fact that we are dealing with a countable set $\mathcal{D}$, which does not carry a σ-additive measure, makes it unclear how this can be derived from theorem 2.3.

Combination of theorem 2.3 with our weaker conjecture 2.2 yields the following.

2.4. THEOREM. *Let $t \geq 1$ be an integer, and suppose that conjecture 2.2 holds for all pairs (t, e). Then the natural density of $\mathcal{D}_t^-$ inside $\mathcal{D}_t$ exists and equals*

$$P_t = \sum_{e=0}^{t-1} \frac{\alpha_t(e)}{2^{e+1}-1},$$

where the rational numbers $\alpha_t(e)$ are as defined in theorem 2.3.

The proven upper and lower bounds for the densities in conjecture 2.2 lead to unconditional results for the lower density $\underline{P}_t$ and the upper density $\overline{P}_t$ of $\mathcal{D}_t^-$ inside $\mathcal{D}_t$, for which we refer to [11]. This yields the following unconditional estimates for small t.

t	1	2	3	4	5	6	7	∞
$\overline{P}_t \leq$	1	.75000	.71875	.68555	.67865	.67128	.66960	.66667
P_t	1	.66667	.64286	.60000	.59476	.58532	.58405	.58058
$\underline{P}_t \geq$	1	.62500	.59766	.55029	.54431	.53392	.53248	.52865

As we already explained, the density result corresponding to 2.4 for the full set $\mathcal{D}$ is not a direct corollary of 2.1, since we do not know that $\mathcal{D}(e)$ has the required density $\alpha_\infty(e)$ in $\mathcal{D}$. However, under the assumption that this is indeed the case, we deduce from 2.1 that the natural density of $\mathcal{D}^-$ in $\mathcal{D}$ exists and is equal to

$$\sum_{e=0}^{\infty} \frac{\alpha_\infty(e)}{2^{e+1}-1} = \sum_{e=0}^{\infty} \alpha_\infty(e+1) = 1 - \alpha_\infty(0) = P.$$

This is the first half of the conjecture in section 1.

We finally observe that in order to observe numerically that the natural density of $\mathcal{D}^-$ in $\mathcal{D}$ tends to P, one has to consider quadratic fields $K \in \mathcal{D}$

in a range where $\omega(\Delta(K))$ has a large average value. In any interval of the form $(1, X)$ for which it is computationally feasible to count the number of $K \in \mathcal{D}^-$, the slow growth rate of $\log\log(\Delta(K))$ implies that this will not be the case. More precisely, the proportion of prime discriminants, which are all in $\mathcal{D}^-$, will be so high that one finds approximations of the required density that are considerably larger than P. However, even when working with small discriminants only one can check the numerical adequacy of the basic hypotheses 2.1 and 2.2 directly rather than from formal corollaries as theorem 2.4, see [11]. Extensive numerical evidence for our basic assumptions can be found in [2].

3. The general case

In order to answer Nagell's original question, we need to extend the analysis of the previous section to arbitrary real quadratic orders. We have seen that for the subset $\Sigma \subset \mathcal{S}$ of squarefree numbers d without prime divisors congruent to 3 mod 4, the density of $\Sigma^- = \Sigma \cap \mathcal{S}^-$ in Σ is conjecturally equal to the number P defined in the introduction. As $\mathcal{S}$ consists by definition of all non-square integers $D > 1$ that are not divisible by 4 or a prime congruent to 3 mod 4, standard arguments show that the subset Σ of squarefree elements in $\mathcal{S}$ has natural density

$$\prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} (1 - \frac{1}{p^2})$$

in $\mathcal{S}$. Now every element $D \in \mathcal{S}$ can uniquely be written as $D = f^2 d$ with $d \in \Sigma$ and $f \geq 1$, and there is the obvious implication $D = f^2 d \in \mathcal{S}^- \Rightarrow d \in \Sigma^-$. What we propose to do in this section is to define a function $\psi : \mathbf{Z}_{\geq 1} \rightarrow [0,1]$ such that, at least heuristically, $\psi(f)$ is the fraction of $d \in \Sigma^-$ for which the converse holds, i.e. the density in Σ^- of those d satisfying $f^2 d \in \mathcal{S}^-$. In particular, we will have $\psi(1) = 1$ and $\psi(f) = 0$ if f is divisible by 2 or a prime congruent to 3 mod 4.

The derivation of the heuristical density Q of $\mathcal{S}^-$ in $\mathcal{S}$ is then straightforward. As the counting function for $\mathcal{S}$ grows like $cX/\sqrt{\log X}$, the density in $\mathcal{S}$ of the numbers $D = f^2 d \in \mathcal{S}$ with given 'square part' f equals $f^{-2} \prod_{p \equiv 1 \bmod 4}(1 - p^{-2})$. If we require in addition that the squarefree part d be in Σ^-, this density gets multiplied by P, and if we finally want $f^2 d \in \mathcal{S}^-$ there is by definition of ψ an additional factor $\psi(f)$. Summing over f, we find the value

$$Q = \Big(\sum_{f \geq 1} \frac{\psi(f)}{f^2}\Big) \cdot P \cdot \prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} (1 - \frac{1}{p^2}).$$

We will see in a moment that ψ is a multiplicative function defined by $\psi(f) = \prod_{p|f \text{ prime}} \psi(p)$, so the Euler product expansion

$$\begin{aligned}\sum_{f\geq 1} \frac{\psi(f)}{f^2} &= \prod_{p \text{ prime}} (1 + \frac{\psi(p)}{p^2} + \frac{\psi(p)}{p^4} + \frac{\psi(p)}{p^6} + \dots) \\ &= \prod_{\substack{p \text{ prime} \\ p\equiv 1 \bmod 4}} (1 + \frac{\psi(p)}{p^2-1}).\end{aligned}$$

shows that our expression for Q is the same as the one occurring in the introduction.

In order to define the function ψ, we need to determine for every $f \geq 1$ the density $\psi(f)$ of those d in Σ^- that satisfy $f^2d \in \mathcal{S}^-$. A basic observation, due to Rédei [6], is that this only depends on the *set* of primes dividing f. He proves the following.

3.1. LEMMA. *Let d in Σ^- and $f \geq 1$ be given. Then f^2d is in $\mathcal{S}^-$ if and only if p^2d is in $\mathcal{S}^-$ for every prime number $p|f$. In addition, we have the following.*

(1) *if $p = 2$ or $p \equiv 3 \bmod 4$, then p^2d is not in $\mathcal{S}^-$;*
(2) *if p is odd and divides d, then p^2d is in $\mathcal{S}^-$;*
(3) *if $p \equiv 1 \bmod 4$ and $\left(\frac{d}{p}\right) = -1$, then p^2d is in $\mathcal{S}^-$.*

We are still left with the case that $p \equiv 1 \bmod 4$ is a prime that splits completely in $\mathbf{Q}(\sqrt{d})$. This is the most difficult case, and there is no criterion for solvability of the negative Pell equation for p^2d that is similar to those given in lemma 3.1. However, we can prove the following.

3.2. LEMMA. *Let d in Σ^- and a prime $p \equiv 1 \bmod 4$ that splits completely in $\mathbf{Q}(\sqrt{d})$ be given. Let ε_d be a fundamental unit in $\mathcal{O} = \mathbf{Z}[\sqrt{d}]$ and $\mathfrak{p}|p$ a prime in $\mathcal{O}$. Then p^2d is in $\mathcal{S}^-$ if and only if the order of ε_d in $(\mathcal{O}/\mathfrak{p})^*$ is congruent to $4 \bmod 8$.*

Proof. Note first that the condition that the order of ε_d be congruent to $4 \bmod 8$ does not depend on the choice of the fundamental unit.

We have $p^2d \in \mathcal{S}^-$ if and only if the order $\mathcal{O}_p = \mathbf{Z}[\sqrt{p^2d}]$ of index p in $\mathcal{O}$ contains units of negative norm, and this happens if and only if d is in Σ^- and the quotient of unit groups $\mathcal{O}^*/\mathcal{O}_p^*$, which is finite and generated by $\varepsilon_d \bmod \mathcal{O}_p^*$, has odd order. We use the natural embedding $\mathcal{O}^*/\mathcal{O}_p^* \rightarrowtail (\mathcal{O}/p\mathcal{O})^*/(\mathbf{Z}/p\mathbf{Z})^*$. In our case, the ring $\mathcal{O}/p\mathcal{O}$ is isomorphic to a product $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ in which the subring $\mathbf{Z}/p\mathbf{Z} \subset \mathcal{O}/p\mathcal{O}$ is embedded along the diagonal. Writing $R : \mathcal{O} \to \mathcal{O}/\mathfrak{p}$ for the reduction modulo a prime $\mathfrak{p}$ of $\mathcal{O}$ lying over p, we have a natural isomorphism

$$\begin{aligned} (\mathcal{O}/p\mathcal{O})^*/(\mathbf{Z}/p\mathbf{Z})^* &\xrightarrow{\sim} (\mathcal{O}/\mathfrak{p})^* \\ x \bmod p\mathcal{O} &\longmapsto R\Big(\frac{x^2}{N(x)}\Big). \end{aligned}$$

It follows that the image of ε_d for $d \in \Sigma^-$ has odd order in $(\mathcal{O}/p\mathcal{O})^*/(\mathbf{Z}/p\mathbf{Z})^*$ if and only if $R(-\varepsilon_d^2)$ has odd order in $(\mathcal{O}/\mathfrak{p})^*$. As the order of $(\mathcal{O}/\mathfrak{p})^*$ is divisible by 4, we arrive at the conclusion of the lemma. □

It follows from the preceding two lemmas that the probability with which we have $f^2d \in \mathcal{S}^-$ for fixed f depends strongly on the residue class of $d \in \Sigma^-$ modulo f. We now invoke a result of Rieger [8] that tells us how the elements of Σ are distributed over the residue classes modulo a given number f.

3.3. THEOREM. *Let $f > 1$ be a product of distinct primes congruent to $1 \bmod 4$, and define*

$$\delta_p(a) = \begin{cases} \frac{1}{p+1} & \text{if } a \equiv 0 \bmod p; \\ \frac{p}{p^2-1} & \text{if } a \not\equiv 0 \bmod p. \end{cases}$$

Then the set $\Sigma_f(a) = \{x \in \Sigma : x \equiv a \bmod f\}$ has a natural density inside Σ for each integer a, and this density equals

$$\delta_f(a) = \prod_{p|f} \delta_p(a).$$

In deriving the correct value of $\psi(f)$, we need two 'reasonable' assumptions that appear to be correct in practice, but are probably not so easy to prove. The first assumption is that the distribution result in 3.3, which is proved for Σ only, remains correct if we replace Σ by Σ^-. This is a natural assumption as no relations are known to exist between the residue class of the discriminant $\Delta(K)$ of a real quadratic field K modulo an odd prime $p \equiv 1 \bmod 4$ and the sign of the norm of the fundamental unit of K.

With this assumption, we try to establish for a given prime number p the natural density $\psi(p)$ of the set of $d \in \Sigma^-$ that satisfy $p^2d \in \mathcal{S}^-$ inside the full set Σ^-. For $p = 2$ and $p \equiv 3 \bmod 4$ we have $\psi(p) = 0$ in view of lemma 3.1 (1). For $p \equiv 1 \bmod 4$, we know by the same lemma that p^2d is in $\mathcal{S}^-$ if the Legendre symbol $\left(\frac{d}{p}\right)$ is equal to 0 or -1. These d contribute

$$\frac{1}{p+1} + \frac{p-1}{2} \cdot \frac{p}{p^2-1} = \frac{2+p}{2(p+1)}$$

to $\psi(p)$ by 3.3 and our assumption. For the remaining d, i.e. those d satisfying $\left(\frac{d}{p}\right) = 1$, we have to determine in view of lemma 3.2 whether the order of the fundamental unit ε_d modulo (a prime over) p is congruent to $4 \bmod 8$. At this point we need a second assumption, on which we will comment in a moment: the elements ε_d for $d \in \Sigma^-$ satisfying $\left(\frac{d}{p}\right) = 1$ are randomly distributed over the non-zero residue classes modulo p, so they have order congruent to $4 \bmod 8$ with probability 2^{1-v} for p a prime with $v \geq 2$ factors 2 in the factorization of $\#(\mathbf{Z}/p\mathbf{Z})^* = p-1$. Thus, writing v_p for the number of factors 2 in $p-1$, we expect a contribution

$$\frac{p-1}{2} \cdot \frac{p}{p^2-1} \cdot 2^{1-v_p} = \frac{2^{1-v_p}p}{2(p+1)}$$

to $\psi(p)$ from the $d \in \Sigma^-$ that lie in the $\frac{p-1}{2}$ residue classes modulo p satisfying $\left(\frac{d}{p}\right) = 1$. Summarizing, we see that $\psi(p)$ for p prime has to be defined by

$$\psi(p) = \begin{cases} 0 & \text{if } p = 2 \text{ or } p \equiv 3 \bmod 4; \\ \frac{2+(1+2^{1-v_p})p}{2(p+1)} & \text{if } p \equiv 1 \bmod 4, \end{cases}$$

with v_p denoting the number of factors 2 occurring in $p-1$. We now combine lemma 3.1 and the independence of the distributions modulo different primes p implied by 3.3 to arrive at the definition

$$\psi(f) = \prod_{p|f} \psi(p)$$

for arbitrary $f \geq 1$. Note that this is the multiplicative definition of ψ we used in our Euler product expansion.

The second assumption in the preceding heuristic derivation involves the distribution of the residue class of the fundamental unit ε_d modulo a prime ideal $\mathfrak{p}$ of fixed index p in $\mathcal{O} = \mathbf{Z}[\sqrt{d}]$, when d ranges over certain subsets of Σ or Σ^-. We assumed that this residue class, which is of course only determined up to sign and taking the inverse residue class in $(\mathcal{O}/\mathfrak{p})^*$, is 'equidistributed over $(\mathcal{O}/\mathfrak{p})^*$' if all these rings are identified with $(\mathbf{Z}/p\mathbf{Z})^*$. In certain situations similar to ours such assumptions have been proved, and numerical evidence for it exists in others. We refer to [10] for equidistribution results when d ranges over the primes congruent to 1 mod 4 and $\mathfrak{p}$ is a power of the prime over 2. In [9] there are numerical data related to a problem of Eisenstein, which deals with the case that d is a squarefree number congruent to 5 mod 8 and $\mathfrak{p}$ is the prime $2\mathcal{O}$. For such d, the ring $\mathcal{O}/2\mathcal{O}$ is the field of 4 elements, and ε_d turns out to be the unit element in the group $(\mathcal{O}/2\mathcal{O})^* \cong \mathbf{Z}/3\mathbf{Z}$ in approximately 1 out of 3 cases. It is shown in [12] that ε_d is in the unit class for infinitely many d, and that the upper density of the set of such d inside the set of all squarefree $d \equiv 5 \bmod 8$ is at most 1/2. Unfortunately, the general case of our assumption does not appear to be easily accessible at the moment.

4. Generalizations

The approach we have given to examine the distribution of the class of a fixed prime over the class group in a family of quadratic fields can readily be extended to more general situations.

Already in the real quadratic case, one can focus attention on the precise relation in the class group that exists between the classes of the ramifying primes rather than restricting one's attention to the question whether $F_\infty = 0$ is that relation. For a description of the equidistribution phenomenon that should then be expected we refer to [11].

For abelian fields of higher degree, say of prime degree p, the p-part of the class group can be studied in a way that is highly similar to the study of the 2-class group in the quadratic case. One then studies the p-class group as a module over the complete cyclotomic ring $R = \mathbf{Z}_p[\zeta_p]$. In this situation, there is again an essentially unique relation between the classes of the ramifying primes whose form can be examined. Its distribution should depend on the $\mathfrak{m}^2$-rank of the class group, where $\mathfrak{m}$ is the maximal ideal of R. We leave it to the reader to extend the heuristics from the quadratic case to this more general situation. Unlike in the quadratic case, there is to my knowledge no numerical material available that could be used to see whether such heuristics give a description that is matched by the behavior of small examples.

REFERENCES

[1] B. D. Beach and H. C. Williams, *A numerical investigation of the Diophantine equation $x^2 - dy^2 = -1$*, Proc. 3rd Southeastern Conf. on Combinatorics, Graph Theory and Computing, 1972, pp. 37–52.

[2] W. Bosma and P. Stevenhagen, *Density computations for real quadratic units*, Math. Comp., to appear (1995).

[3] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number Theory Noordwijkerhout 1983 (H. Jager, ed.), Springer LNM 1068, 1984.

[4] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1938.

[5] T. Nagell, *Über die Lösbarkeit der Gleichung $x^2 - Dy^2 = -1$*, Arkiv för Mat., Astr., o. Fysik **23** (1932), no. B/6, 1–5.

[6] L. Rédei, *Über die Pellsche Gleichung $t^2 - du^2 = -1$*, J. reine angew. Math. **173** (1935), 193-221.

[7] L. Rédei, *Über einige Mittelwertfragen im quadratischen Zahlkörper*, J. reine angew. Math. **174** (1936), 131–148.

[8] 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.

[9] A. J. Stephens and H. C. Williams, *Some computational results on a problem of Eisenstein*, Théorie des Nombres - Number Theory (J. W. M. de Koninck and C. Levesque, eds.), de Gruyter, 1992, pp. 869–886.

[10] P. Stevenhagen, *On the 2-power divisibility of certain quadratic class numbers*, J. of Number Theory **43** (1993), no. (1), 1–19.

[11] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Exp. Math. **2** (1993), no. (2), 121–136.

[12] P. Stevenhagen, *On a problem of Eisenstein*, Acta Arith., (to appear, 1995).

Peter STEVENHAGEN
Faculteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam, Pays-Bas
e-mail: psh@fwi.uva.nl