MATHEMATICS OF COMPUTATION
Volume 65, Number 215
July 1996, Pages 1327–1337

DENSITY COMPUTATIONS FOR REAL QUADRATIC UNITS

WIEB BOSMA AND PETER STEVENHAGEN

ABSTRACT. In order to study the density of the set of positive integers d for which the negative Pell equation $x^2 - dy^2 = -1$ is solvable in integers, we compute the norm of the fundamental unit in certain well-chosen families of real quadratic orders. A fast algorithm that computes 2-class groups rather than units is used. It is random polynomial-time in $\log d$ as the factorization of d is a natural part of the input for the values of d we encounter.

The data obtained provide convincing numerical evidence for the density heuristics for the negative Pell equation proposed by the second author. In particular, an irrational proportion $P = 1 - \prod_{j\geq 1 \text{ odd}}(1 - 2^{-j}) \approx .58$ of the real quadratic fields without discriminantal prime divisors congruent to 3 mod 4 should have a fundamental unit of norm -1.

1. INTRODUCTION

This paper is devoted to a numerical study of the solvability in integers of the negative Pell equation

$$x^2 - dy^2 = -1 \tag{1.1}$$

when d ranges over the set of nonsquare positive integers. Euler showed in 1759 that the equation with right-hand side $+1$ always has infinitely many solutions, and that the smallest nontrivial solution can be found from the continued fraction expansion of $\sqrt{d}$. He also showed that (1.1) is solvable if and only if the period of this expansion is odd. If this is the case, there are again infinitely many solutions, and the smallest of them can be found from the expansion. Euler's result settles the solvability question for every specific d, but it does not tell us at all *how often* we should expect (1.1) to be solvable. This basic problem, which was raised in the present form by Nagell [8], appears to be of a very different nature.

An obvious necessary condition for solvability of (1.1) is that -1 is a square modulo d, i.e., that d is not divisible by 4 or by a prime $p \equiv 3 \bmod 4$. Let us write $\mathcal{S}$ for the set of integers $d \geq 1$ that satisfy this condition. Then $\mathcal{S}$ consists of the integers that can be written as the sum of two coprime squares, and its distribution is well known. We have [10]

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

Received by the editor February 24, 1995.
1991 *Mathematics Subject Classification.* Primary 11R11, 11Y40, 11R45; Secondary 11E16.
Key words and phrases. Real quadratic class groups, negative Pell equation, density theorems.

We will study how often the necessary condition $d \in \mathcal{S}$ is sufficient for solvability of (1.1). More precisely, we will investigate whether the subset $\mathcal{S}^- \subset \mathcal{S}$ of integers d for which $x^2 - dy^2 = -1$ has integral solutions possesses a natural density inside $\mathcal{S}$, i.e., whether the limit

$$Q = \lim_{X \to \infty} \frac{\#\{d \in \mathcal{S}^- : d \leq X\}}{\#\{d \in \mathcal{S} : d \leq X\}} \tag{1.2}$$

exists. If it exists, we of course want to know the value of Q as well.

The analysis of the density (1.2) is the subject of two papers [11, 12] by the second author. The main results given there are conjectural as they involve unproved hypotheses on the distribution of the infinite Frobenius element in real quadratic class groups. They predict that the limit value Q exists, and that the convergence to the limit value Q is very slow. More precisely, we will not find the value of the quotient in (1.2) to be close to Q unless $\log\log X$, the order of magnitude of the average number of prime factors of a number of size X, is large. As it is not feasible to check a number of values d of double exponential order of magnitude, our numerical investigation has to proceed by indirect means.

Whatever way one chooses to proceed, one needs a fast algorithm to check whether (1.1) is solvable for a given integer $d \in \mathcal{S}$. This is clearly equivalent to the determination of the norm of the fundamental unit η_d of the quadratic order $\mathbf{Z}[\sqrt{d}]$ of discriminant $4d$. As for every $\epsilon > 0$, the regulator $\log|\eta_d|$ exceeds $d^{\frac{1}{2}-\epsilon}$ for infinitely many d, one cannot expect to be able to write down η_d for large values of d. For the same reason, it is not feasible for large d to decide the solvability of (1.1) by computing the length of the period of the continued fraction of $\sqrt{d}$. Fortunately, it is possible to compute the norm of η_d without computing η_d or the continued fraction of $\sqrt{d}$. One observes that computing the sign of the norm is equivalent to deciding whether the class of the ideal generated by $\sqrt{d}$ in the strict class group of the quadratic order of discriminant $4d$, which has order at most two, is in fact the trivial class. One can find this order by computing the 2-Sylow subgroup of the class group, and it was shown by Lagarias [5, 6] that if the factorization of d is part of the input, this leads to an algorithm to determine the solvability of (1.1) that is random polynomial-time in $\log d$. We have implemented a modified version of this algorithm in the computer algebra system Magma, and we will briefly indicate in the next section how it works. As is pointed out in [7], the basic ideas of the algorithm go back to Rédei.

We start in §3 with the somewhat simpler case of *squarefree* integers $d \in \mathcal{S}$. These form a subset Σ of large natural density $\prod_{p \equiv 1(4) \text{ prime}}(1 - p^{-2}) \approx .95$ in $\mathcal{S}$. We call this the *fundamental case*, as the frequency of solvability for $d \in \Sigma$, i.e., the natural density of $\Sigma \cap \mathcal{S}^-$ in Σ, is nothing but the natural density of the set of real quadratic fields with fundamental unit of norm -1 inside the set of real quadratic fields containing elements of norm -1. The main conjecture in [11] is that this density exists and equals the irrational *Pell constant*

$$P = 1 - \prod_{j \geq 1 \text{ odd}} (1 - 2^{-j}) = .5805775582\ldots\ . \tag{1.3}$$

It is based on the heuristic argument that the 'probability' for the negative Pell equation to be solvable for $d \in \Sigma$ depends solely on the 4-*rank* of the strict class group of the order $\mathbf{Z}[\sqrt{d}]$.

Unlike the class group itself, this 4-rank can easily be determined from the prime factors of d by a theorem of Rédei. In fact, our algorithm to decide the solvability of (1.1) computes it in its first step. Rédei's theorem shows that integers $d \in \mathcal{S}$ giving rise to high 4-ranks are so rare that they will not be found by picking random elements in $\mathcal{S}$. On the other hand, it also shows that they can easily be constructed as products of primes that satisfy certain congruence conditions with respect to each other. In this way, we can produce large sets of d giving rise to certain 4-ranks, and such d come by construction in factored form, as required by the algorithm. As it happens, the conjectured densities for the solvability of (1.1) are very small for $d \in \mathcal{S}$ yielding high 4-ranks, so in this case the numerical testing of the conjecture necessitates the handling of large numbers of large discriminants. For this reason, it is essential to have a fast algorithm to decide the solvability of (1.1). Implementation of an Euler-type algorithm as in [1] would never have yielded the current data.

The final section describes similar computations for $d \in \mathcal{S}$ that are not squarefree. In this situation we study the norm of fundamental units in arbitrary real quadratic orders, and here the frequency for solvability is predicted to depend on the conductor of the order in the corresponding maximal order [12] as well.

The computations in both sections show that the underlying hypotheses of [11] and [12] are very much in accordance with our numerical data. This of course does not prove that the values P and Q are the limit values they are conjectured to be, but it shows that these conjectures are very plausible. Especially in the fundamental case, there are various proven results in the direction of these conjectures, for which we refer to the last section of [11].

2. Deciding the solvability of the negative Pell equation

Let $d \in \mathcal{S}$ be a nonsquare integer and $\mathcal{O}_D = \mathbf{Z}[\sqrt{d}]$ the quadratic order of discriminant $D = 4d$. It is elementary [11, Lemma 2.1] to check that the negative Pell equation is solvable for d if and only if the class F_∞ of $\sqrt{d} \cdot \mathcal{O}_D$ is the trivial element in the strict class group of $\mathcal{O}_D$. As is well known [3], the elements of this class group can be identified with the $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of the binary quadratic forms of discriminant D, and in this terminology (1.1) is solvable if and only if the *anti-principal form* $-X^2 + dY^2$ of discriminant D is $\mathrm{SL}_2(\mathbf{Z})$-equivalent to the principal form $X^2 - dY^2$. As F_∞ has order at most two in the strict class group of $\mathcal{O}_D$, we are done if we can find a *basis* for the 2-Sylow subgroup $\mathcal{C}_D$ of this class group and a representation of F_∞ on this basis. By a basis of $\mathcal{C}_D$, we mean a finite number of nonzero elements $x_i \in \mathcal{C}_D$ such that $\mathcal{C}_D$ is the direct product of the cyclic groups $\langle x_i \rangle$.

The algorithm we use in this paper computes, for *any* nonsquare factored discriminant $D \equiv 0, 1 \bmod 4$, a basis for the 2-Sylow subgroup $\mathcal{C}_D$ of the strict class group of the quadratic order of discriminant D. Moreover, it efficiently computes the representation with respect to this basis for any given element $x \in \mathcal{C}_D$. As the mathematical content of the algorithm is described in detail in [2], we will only give a very brief description here.

From the factorization of D, one obtains an $\mathbf{F}_2$-basis X for the group of quadratic characters $\chi : \mathcal{C} = \mathcal{C}_D \to \mathbf{F}_2$ with image in the field $\mathbf{F}_2$ of two elements. Such χ are quadratic Dirichlet characters of conductor dividing D. If the elements of $\mathcal{C}$ are represented by binary quadratic forms, the value of χ on the class of a form F is

the value taken by χ on the integers coprime to D that are represented by F. The basis X consists of characters of prime power conductor.

In addition, the factorization of D provides us with a set of so-called ambiguous forms, whose classes generate the 2-torsion subgroup $\mathcal{C}[2]$ of $\mathcal{C}$. We do not in general know the relation between these generators, and in fact the whole purpose of our computation is to decide whether the class $F_\infty \in \mathcal{C}[2]$ of the antiprincipal form is the trivial class. If we select one ambiguous form F_p for each prime divisor p of D (and two for $p = 2$ when 32 divides D), we obtain a set S of 2-torsion generators that has exactly one nontrivial relation. More precisely, we have a natural surjection $\mathbf{F}_2^S \to \mathcal{C}[2]$ with an unknown 1-dimensional kernel. Even though we cannot see which ambiguous form in $\mathbf{F}_2^S$ is in the trivial class, the character pairing

$$\mathbf{F}_2^S \times \mathbf{F}_2^X \to \mathbf{F}_2 \tag{2.1}$$

tells us which ambiguous forms are in $2\mathcal{C}$. The pairing (2.1) is completely explicit: for $\chi \in X$ of q-power conductor, with $q \neq p$ an odd prime, the value $\chi(F_p)$ equals the Legendre symbol $\left(\frac{p}{q}\right)$ with values taken in $\mathbf{F}_2$. Rédei's theorem is the simple group-theoretic fact that the 4-rank of $\mathcal{C}$ equals the cardinality of X minus the rank of the $\mathbf{F}_2$-matrix

$$M_D = (\chi(F_p))_{\chi \in X, F_p \in S}. \tag{2.2}$$

What enables our algorithm to find the full 2-class group $\mathcal{C}$ is the observation of Gauss [4, art. 286] that if the class F of a form in $\mathcal{C}$ is in $2\mathcal{C}$, then one can find a form whose class in $\mathcal{C}$ is a 'square root' of F, i.e., twice its class equals F. This square root is usually not unique, and Gauss's algorithm, which employs a reduction procedure for ternary quadratic forms, does not necessarily yield a form in the trivial class if F is the trivial class in $\mathcal{C}$.

The construction of a basis for the 2-class group $\mathcal{C}$ proceeds recursively and is essentially a matter of linear algebra over $\mathbf{F}_2$. From the pairing (2.1) one readily computes a subset $B \subset S$ that yields a basis for $\mathcal{C}[2]/(\mathcal{C}[2] \cap 2\mathcal{C})$. One can then change the remaining elements of S by $\mathbf{F}_2$-linear combinations of forms in B to ensure that their classes in $\mathcal{C}$ are 'squares'. Using Gauss's algorithm, one now computes a square root of each of these forms. This yields a set S' of forms whose classes generate the 2-torsion subgroup of $\mathcal{C}/\mathcal{C}[2]$. As the group of quadratic characters on $\mathcal{C}/\mathcal{C}[2]$ is the annihilator of $\mathbf{F}_2^S$ under the pairing (2.1), we can easily compute an $\mathbf{F}_2$-basis for this group. This brings us back to the original situation in which $\mathcal{C}$ has been replaced by the smaller group $\mathcal{C}/\mathcal{C}[2]$. A basis of $\mathcal{C}$ is obtained as the union of B and a basis of $\mathcal{C}/\mathcal{C}[2]$. In order to represent an element $x \in \mathcal{C}$ with respect to this basis, we compute the unique $\mathbf{F}_2$-linear combination b of forms in B for which the class of $x - b$ is in $2\mathcal{C}$ and a form a whose class is a square root of $x - b$ in $\mathcal{C}$. Then we have $x = b + 2a$, and it suffices to write a with respect to the basis of $\mathcal{C}/\mathcal{C}[2]$.

In our situation, we want to decide whether the element F_∞ is the trivial element, so we write it with respect to the basis of $\mathcal{C}$ that is being computed recursively. As soon as we discover during the computation that F_∞ does require a basis element in its representation, we know it is nontrivial and we stop. This implies that in many cases, we only have to perform part of the computation of $\mathcal{C}_{4d}$ in order to decide the solvability of (1.1) for d. Especially in the fundamental case in the next section, where we test many d for which (1.1) is not solvable, this leads to a considerable reduction of the running time of the algorithm.

3. The fundamental case

In this section, we study the density problem (1.2) for the subset $\Sigma \subset \mathcal{S}$ of squarefree integers in $\mathcal{S}$. It is conjectured in [11] that the limit

$$P = \lim_{X \to \infty} \frac{\#\{d \in \Sigma \cap \mathcal{S}^- : d \leq X\}}{\#\{d \in \Sigma : d \leq X\}} \tag{3.1}$$

exists and is equal to the value given in (1.3). If d ranges over the elements of Σ, then the fields $\mathbf{Q}(\sqrt{d})$ range over the real quadratic fields K for which, by the Hasse principle, -1 is in the norm image $N_{K/\mathbf{Q}}K^*$. Thus, P is the natural density of the set of real quadratic fields having a unit of negative norm inside the set of real quadratic fields containing elements of norm -1. The ordering in this case is by 'radicand' d rather than by discriminant Δ_K (which equals d for odd d and $4d$ for even $d \in \Sigma$), but this is of no importance, as even and odd d are conjectured to yield the same density P. We will see this numerically later in this section.

As stated in the introduction, it is not possible to check (3.1) numerically by computing the value of the quotient for large values of X. The conjectural value (1.3) of the limit is based on the fact that the average number of prime factors of d tends to infinity with d. However, this number grows asymptotically only like $\log\log d$, so it is never large for tractable d. For this reason, we do not check the conjecture directly but focus on the underlying heuristic argument instead. This argument states that the probability for the negative Pell equation to be solvable for $d \in \Sigma$ depends solely on the 4-rank of the strict class group of the quadratic field $\mathbf{Q}(\sqrt{d})$. More precisely, let us denote for $e \geq 0$ by $\Sigma(e) \subset \Sigma$ the set of $d \in \Sigma$ for which the 4-rank of the narrow class group $\mathcal{C}$ of $\mathbf{Q}(\sqrt{d})$ equals e. Then the main conjecture in [11] is the following.

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

This conjecture is a theorem for $e = 0$, but an open problem for all $e \geq 1$. It can in principle be checked numerically by considering all $d \in \Sigma$ in a given large interval, as is done in [11] for those d for which the discriminant of $\mathbf{Q}(\sqrt{d})$ is in one of the intervals $[1, 2 \cdot 10^7]$ and $[10^{10}, 10^{10} + 2 \cdot 10^7]$. However, it then turns out that about 99.9% of all tested d have 4-rank $e \leq 2$, so we only get a numerical confirmation of our conjecture for small e. Moreover, testing a density $(2^{e+1}-1)^{-1}$ for large e involves testing a large number of d in order to make it possible to obtain an approximation of this small probability.

Our algorithm is sufficiently efficient to handle large numbers of (factored) discriminants, so we only have to come up with many $d \in \Sigma$ for which $\mathcal{C}$ has some fixed 4-rank e. Fortunately, this is an easy task, as Rédei's theorem tells us that the 4-rank of $\mathcal{C}$ can be read off from the *Rédei matrix* (2.2). If we generate $\mathcal{C}[2]$ with the classes of the 'prime forms' $\{F_p\}_{p|d}$ and the quadratic characters on $\mathcal{C}$ by Legendre symbols $\chi_q = \left(\frac{\cdot}{q}\right)$ for odd primes q dividing d, the matrix M_D consists of Legendre symbols $\chi_q(p)$ with values in $\mathbf{F}_2$. If p and q coincide, one can compute the corresponding entry from the fact that the rows of M_D add up to zero.

The simplest way to produce a discriminant $d \in \Sigma$ of 4-rank e is to take the product of $e+1$ primes that are not congruent to 3 mod 4 and all squares modulo each other. As we need very many d of this kind, especially for the higher values

of e, we have done the following. For each of the 22 primes $p < 200$ that are not congruent to 3 mod 4, we computed prime numbers $p_1 < p_2 < \cdots < p_{20}$ by taking $p_1 = p$ and $p_k > p_{k-1}$ the smallest prime congruent to 1 mod 4 such that all p_i with $i < k$ are squares modulo p_k. In all cases, this yields sequences with $10^7 < p_{20} < 10^8$. Out of such a sequence, we can construct $\binom{20}{e+1}$ values of d for which $C(4d)$ has 4-rank e. For the values $2 \leq e \leq 9$ we considered, these numbers increase with e as follows.

e	2	3	4	5	6	7	8	9
$\#d$	1140	4845	15504	38760	77520	125970	167960	184756

The large numbers for the higher e-values are necessary, as we expect to find only 1 out of $2^{e+1} - 1$ values of d with 4-rank e to be in $\mathcal{S}^-$, so the expected number $N_e = \binom{20}{e+1}/(2^{e+1} - 1)$ of such d per sequence should not become too small to be 'measurable' with some accuracy. Note that the case $e = 9$ involves a 2-class group computation for $22 \cdot \binom{20}{10} = 4064632$ discriminants that mostly have 40 to 50 decimal digits. Moreover, these are large 2-class groups in the sense that their 4-rank is by construction very high. Even with our fast algorithm, this is still a rather formidable computing task. However, it can easily be run on parallel machines. In our case, we used about 50 Sun workstations at the University of Amsterdam. The results are presented in Table 3.3.

3.3. TABLE. Solvability of the negative Pell equation for high 4-ranks

p	$e = 2$	3	4	5	6	7	8	9
5	179	323	539	587	600	512	315	170
8	172	277	493	596	599	493	315	168
13	176	317	497	632	626	516	333	177
17	180	347	486	611	584	485	325	187
29	148	304	491	607	601	533	327	171
37	158	322	501	601	608	506	368	194
41	161	362	510	685	582	533	370	171
53	148	320	471	598	600	476	304	192
61	163	333	440	591	624	518	318	163
73	187	309	526	629	615	511	353	156
89	165	351	530	619	590	504	299	172
97	164	325	505	605	598	472	326	178
101	172	297	507	608	611	527	352	197
109	165	295	502	620	622	487	349	179
113	145	314	508	569	620	494	325	179
137	165	303	519	630	604	475	320	187
149	146	348	460	680	583	502	312	173
157	173	364	460	629	611	461	361	187
173	158	340	496	618	620	481	307	184
181	156	325	514	634	617	489	311	173
193	148	326	493	591	609	482	323	203
197	167	314	486	604	588	489	336	178
A_e	163.45	323.45	497.00	615.64	605.09	497.55	329.50	179.05
N_e	162.86	323.00	500.13	615.24	610.39	494.00	328.69	180.60
	+.37%	+.14%	−.63%	+.06%	−.87%	+.72%	+.25%	−.86%

The first column has the prime $p = p_1$ that is used to generate the sequence of 20

'cosquare primes'. The other columns have the value e of the 4-rank on the first line, then the number of d-values in $\Sigma(e)^-$ for each of the 22 sequences, and on the bottom lines the average number A_e of d-values in $\Sigma(e)^-$ per sequence, the expected number N_e defined above and the percentage by which A_e deviates from N_e. We see that deviations of 10% from the predicted values are not uncommon in single rows, but that the overall behavior is remarkably close to what conjecture 3.2 predicts: the deviation of A_e from N_e is less than 1%.

We note also that the *even* values of d, which occur on the line $p = 8$ and were excluded from consideration in [9], behave in no way different from the odd values.

For still higher 4-ranks, the testing rapidly becomes unattractive, as the expected density $(2^{e+1} - 1)^{-1}$ decreases exponentially. Moreover, our basic setup using 20 cosquare primes becomes inappropriate as $\binom{20}{e+1}$ decreases for $e > 9$. We did perform the computations for $e = 10$. The expected number N_e is then as small as 82.05, and the computed values ranged from 67 to 103. They lead to a value $A_e = 86.18$, which deviates only +5.03% from its expected value. We found $N_{11} = 30.76$ too small to be worth trying.

One may object against our approach of testing Conjecture 3.2 that the values of d we consider are rather special in the sense that M_{4d} is the zero matrix for these d, so the 4-rank of $\mathcal{C}(4d)$ is equal to the 2-rank. We have therefore conducted a similar experiment for discriminants that do not have this property, i.e., we have constructed discriminants for which the 4-rank of $\mathcal{C}(4d)$ is fairly high and smaller than the 2-rank. To obtain such discriminants, we took, from each of the 22 sequences of 'cosquare primes' constructed above, the set A of the first 10 primes and computed a set B of 10 other primes congruent to 1 mod 4 that are squares modulo each prime in A without paying attention to the quadratic character of the primes in B modulo each other. If we now form $d = d_1 d_2$ by multiplying a product d_1 of t_1 primes in A and a product d_2 of t_2 primes in B, the rank r of the Rédei matrix M_{4d} is equal to the rank of its submatrix M_{d_2}. Thus, the class group $\mathcal{C}(4d)$ will have 2-rank $t_1 + t_2 - 1$ and 4-rank $t_1 + t_2 - 1 - r \geq t_1$. As we have not imposed any restrictions on the relative quadratic behavior of the primes in B, the rank r of M_{d_2}, which is in our situation the difference between the 2-rank and the 4-rank of $\mathcal{C}(4d)$, will in most cases be positive, and often not far from the maximal value $t_2 - 1$. For varying choices of t_1 and t_2, one can thus obtain large families of values of d of the required type.

In our numerical experiment, we varied t_1 in the range $3, 4, \ldots, 9$ and fixed $t_2 = 4$. This yields $22 \cdot \sum_{i=3}^{9} \binom{10}{i} = 21274$ values of d_1, each to be multiplied with $\binom{10}{4} = 210$ values of d_2 constructed from the corresponding set of primes B; in total this makes 4 467 540 values of d. The 2-rank $e_2 = t_1 + t_2 - 1 = t_1 + 3$ of the corresponding class groups ranges from 6 to 12, and the difference r between 2- and 4-rank from 0 to 3. There are $22 \cdot \binom{10}{4} = 4620$ values of d_2 that occur, and as the corresponding Rédei matrices M_{d_2} are expected to behave like 'random symmetric 4×4-matrices' over the field of 2-elements, one expects the distribution over the possible r-values 3–2–1–0 to be close to 2021–2021–505–72, cf. [11]. The actual distribution in our example was 2106–1987–455–72.

The following table presents the outcome of our experiment. We leave out the data for discriminants with $M_{4d} = 0$, since they were tested in the preceding experiment, and there are only few of them among our current data. In each row the value of $r \in \{3, 2, 1\}$ is fixed, and in each column the 2-rank e_2. The entry

corresponding to a pair (r, e_2) lists the number of $d \in \mathcal{S}^-$ that was found and below that the number that is predicted by our conjecture. Note that the 4-rank for such an entry is $e_2 - r \in \{3, 4, \ldots, 11\}$, so we have constant 4-rank along diagonal lines ($\nearrow$) in the table. In smaller type, the total number of d's that were tested for this entry is indicated. Again, we see that the deviation from the expected values is relatively small as soon as this expected value is sufficiently large to be accurately 'measurable'. This convinces us of the correctness of the basic Conjecture 3.2.

3.4. TABLE. Solvability of the negative Pell equation for d with $M_{4d} \neq 0$

r	$e_2 = 6$	7	8	9	10	11	12
3	16680 16848 252720	14214 14266 442260	8244 8424 530712	3400 3482 442260	968 991 252720	211 185 94770	14 21 21060
2	7625 7692 238440	6568 6623 417270	3795 3943 500724	1613 1636 417270	473 467 238440	71 87 89415	7 10 19870
1	873 867 54600	791 752 95550	459 450 114660	190 187 95550	61 53 54600	4 10 20475	2 1 4550

4. The nonfundamental case

As we mentioned in the introduction, the squarefree values of d form a set Σ of large natural density

$$B = \prod_{p \equiv 1(4) \text{ prime}} (1 - p^{-2}) \approx .95$$

in $\mathcal{S}$. An arbitrary element in $\mathcal{S}$ can uniquely be written as $f^2 d$ with $d \in \Sigma$ squarefree and $f \in \mathbf{Z}_{>0}$ a product of primes congruent to 1 mod 4. We therefore have $\mathcal{S} = \bigcup_{f \in \mathcal{F}} \mathcal{S}_f$ with $\mathcal{S}_f = \{f^2 d : d \in \Sigma\}$ and f ranging over the set $\mathcal{F}$ of odd positive integers without prime factors congruent to 3 mod 4. It is elementary to show that $\mathcal{S}_f$ has natural density $f^{-2}B$ in $\mathcal{S}$, in accordance with the identity $\sum_{f \in \mathcal{F}} f^{-2} = B^{-1}$. We can find the natural density Q of $\mathcal{S}^-$ in $\mathcal{S}$ defined in (1.2) from the natural densities of $\mathcal{S}_f \cap \mathcal{S}^-$ in $\mathcal{S}$ for each $f \in \mathcal{F}$. For the main term coming from $f = 1$ the conjectural density equals $P \cdot B$, with B as above and P the Pell constant from (1.3). This has been checked numerically in the previous section. It is conjectured in [12] that the natural density of $\mathcal{S}_f \cap \mathcal{S}^-$ in $\mathcal{S}$ for arbitrary $f \in \mathcal{F}$ equals $\psi(f) \cdot P \cdot B$, where ψ is the multiplicative function defined by $\psi(f) = \prod_{p|f \text{ prime}} \psi(p)$ and

$$\psi(p) = \frac{2 + (1 + 2^{1-v_p})p}{2(p+1)} \tag{4.1}$$

for $p \equiv 1 \bmod 4$ a prime number with exactly v_p factors 2 in $p-1$. Setting $\psi(f) = 0$

for $f \in \mathbf{Z} \setminus \mathcal{F}$, we obtain the value

$$Q = \Big(\sum_{f \geq 1} \frac{\psi(f)}{f^2}\Big) \cdot P \cdot B$$
$$= P \cdot \prod_{\substack{p \text{ prime} \\ p \equiv 1 \bmod 4}} \big(1 + \frac{\psi(p)}{p^2 - 1}\big)\big(1 - \frac{1}{p^2}\big) \approx .57339$$

for the density of $\mathcal{S}^-$ in $\mathcal{S}$.

As in the fundamental case, we cannot check the conjectural value of Q by a direct computation. However, it is perfectly feasible to check the numerical adequacy of the constant $\psi(f)$ for any value of $f \in \mathcal{F}$. We can restrict to *squarefree* values of f, since $f^2 d$ with $f \in \mathbf{Z}$ and $d \in \Sigma$ is in $\mathcal{S}^-$ if and only if $f_0^2 d$ is in $\mathcal{S}^-$ for the largest squarefree factor f_0 of f, cf. [12]. The value of $\psi(f)$ for $f \in \mathcal{F}$ is based on two heuristic assumptions.

4.2. **Assumption.** *For every conductor $f \in \mathcal{F}$, the discriminants in Σ and Σ^- have the same distribution over the residue classes of $\mathbf{Z}/f\mathbf{Z}$.*

This assumption reflects the fact that for squarefree d, no relation is known to exist between the solvability of (1.1) and the congruence class of d modulo a prime $p \equiv 1 \bmod 4$. All we need for the conjecture in [12] is that for $d \in \Sigma^-$, the values of the Legendre symbol $\left(\frac{d}{p}\right)$ are independent for $p \in \mathcal{F}$, and the values 1, -1 and 0 occur with relative frequencies $p/(2p+2)$, $p/(2p+2)$ and $1/(p+1)$. This density statement is easily seen to be true for the set of *all* squarefree integers, and it also holds for the set Σ by a theorem of Rieger [10]. In order to check it numerically for the subset $\Sigma^- \subset \Sigma$, we have determined for all $d \in \Sigma$ considered in [11], i.e., those d for which the associated discriminant is contained in one of the intervals $[1, 2 \cdot 10^7]$ and $[10^{10}, 10^{10} + 2 \cdot 10^7]$, the values of the Legendre symbols $\left(\frac{d}{p}\right)$ for a few small $p \in \mathcal{F}$. There are 1696777 values of d for the first interval and 1420163 for the second.

4.3. TABLE. Distribution of Legendre symbols for d in Σ and Σ^-

$\left(\frac{d}{p}\right)$	$p = 5$	13	17	41	101	257
1	.4167 .4132 .4144 .4250 .4253	.4643 .4615 .4625 .4668 .4674	.4722 .4697 .4706 .4741 .4749	.4881 .4866 .4872 .4891 .4897	.4951 .4942 .4941 .4956 .4947	.4981 .4976 .4978 .4981 .4974
-1	.4167 .4132 .4142 .4253 .4245	.4643 .4615 .4623 .4668 .4667	.4722 .4699 .4705 .4751 .4747	.4881 .4866 .4870 .4891 .4890	.4951 .4943 .4950 .4951 .4962	.4981 .4977 .4978 .4980 .4988
0	.1667 .1735 .1714 .1497 .1502	.0714 .0770 .0753 .0663 .0659	.0556 .0604 .0589 .0508 .0504	.0238 .0268 .0258 .0217 .0213	.0098 .0114 .0109 .0093 .0090	.0039 .0047 .0044 .0039 .0037

Table 4.3 shows the relative frequencies for each p. The first line of each entry is the *proven* asymptotic fraction of $d \in \Sigma$ with indicated value of $\left(\frac{d}{p}\right)$. Within the accuracy of the table, this coincides with the computed fraction for the set of

all squarefree d in these intervals. The second line of the entry has the computed fractions for $d \in \Sigma$ in each of the two selected intervals, and the third line the same fractions for $d \in \Sigma^-$. We see that the distributions for the sets Σ^- and Σ do not differ substantially. We also tested for possible dependencies between values of $\left(\frac{d}{p}\right)$ for our six primes p for $d \in \Sigma^-$. They are known to be independent for $d \in \Sigma$, and we found no indication that the situation is different for Σ^-.

If $p \in \mathcal{F}$ is prime, Assumption 4.2 implies that a fraction $(2+p)/(2p+2)$ of all $d \in \Sigma^-$ has Legendre symbol $\left(\frac{d}{p}\right) \neq 1$ and a fraction $p/(2p+2)$ has $\left(\frac{d}{p}\right) = 1$. For $d \in \Sigma^-$ satisfying $\left(\frac{d}{p}\right) \neq 1$, we always have $p^2 d \in \mathcal{S}^-$. In the other case however, when we have $\left(\frac{d}{p}\right) = 1$, we need a second heuristic assumption, which is an equidistribution assumption on fundamental units of real quadratic fields modulo a fixed conductor that is explained in [12]. For the basic case of a prime conductor it is the following.

4.4. **Assumption.** *Let $p \in \mathcal{F}$ be a prime number with v_p factors 2 in $p-1$. Then $\{d \in \Sigma^- : p^2 d \in \mathcal{S}^-\}$ has natural density 2^{-v_p} in Σ^-.*

Under the natural asumption that these frequencies are again independent modulo different p, we obtain the value in (4.1) for $\psi(f)$ since an elementary argument [12, Lemma 3.1] shows that we have $f^2 d \in \mathcal{S}^-$ for $d \in \Sigma^-$ if and only if $p^2 d$ is in $\mathcal{S}^-$ for all prime divisors $p|f$.

In order to test Assumption 4.4, we determined for the values $d \in \Sigma^-$ from each of the intervals used in compiling Table 4.2 and a few well-chosen $p \in \mathcal{F}$ the number of discriminants d that have $p^2 d \in \mathcal{S}^-$ among those that satisfy $\left(\frac{d}{p}\right) = 1$. Table 4.5 shows the fractions obtained.

4.5. TABLE. Fraction of $d \in \Sigma^-$ with $\left(\frac{d}{p}\right) = 1$ and $p^2 d \in \mathcal{S}^-$

p	v_p	fraction	value	$2^{v_p-1} \cdot$ value
5	2	286619/573486 231540/462884	.49978 .50021	.99956 1.00042
41	3	164790/659959 133209/533024	.24970 .24991	.99879 .99965
17	4	79531/639735 64876/516857	.12432 .12552	.99455 1.00416
97	5	41242/667995 33793/538960	.06174 .06270	.98784 1.00321
193	6	20902/649973 16949/541603	.03116 .03129	1.02906 1.00141
257	8	5243/672114 4248/541435	.00780 .00785	.99850 1.00426
65537	16	24/674073 10/544213	.00004 .00002	1.16669 .60212

The final column lists the value $2^{v_p-1} \cdot$ (fraction), which is conjecturally close to 1. The behavior of the fractions in Table 4.5 is again as good as we may reasonably

expect. This convinces us of the correctness of the conjectural values of $\psi(f)$ for all $f \geq 1$, and consequently of the validity of the conjectures in [12].

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. MR **50:**231
2. W. Bosma and P. Stevenhagen, *On the computation of quadratic 2-class groups*, University of Amsterdam mathematical preprint series, report 95–04, 1995.
3. H. Cohen, *A course in computational algebraic number theory*, Springer Graduate Texts in Math., vol. 138, Berlin and New York, 1993. MR **94i:**11105
4. C. F. Gauss, *Disquisitiones Arithmeticae*, Gerhard Fleischer, Leipzig, 1801.
5. J. C. Lagarias, *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, J. Algorithms **1** (1980), 142–186. MR **83e:**90112
6. J. C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. **260** (1980), no. 2, 485–508. MR **81g:**10029
7. P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math. **307/8** (1979), 373–398. MR **81f:**12005
8. 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.
9. L. Rédei, *Über einige Mittelwertfragen im quadratischen Zahlkörper*, J. Reine Angew. Math. **174** (1936), 131–148.
10. 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. MR **30:**4734
11. P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Exp. Math. **2** (1993), no. 2, 121–136. MR **94k:**11120
12. P. Stevenhagen, *A density conjecture for the negative Pell equation*, Computational Algebra and Number Theory, Mathematics and its Applications, vol. 325, Kluwer Academic Publishers, 1995, pp. 187–200.

School of Mathematics and Statistics, University of Sydney, Sydney NSW 2006, Australia

E-mail address: wieb@maths.su.oz.au

Faculteit Wiskunde en Informatica, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands

E-mail address: psh@fwi.uva.nl

References

[6] **On the Computational Complexity of Determining the Solvability or Unsolvability of the Equation X2 - DY2 = -1**

J. C. Lagarias

Transactions of the American Mathematical Society, Vol. 260, No. 2. (Aug., 1980), pp. 485-508.

Stable URL:

http://links.jstor.org/sici?sici=0002-9947%28198008%29260%3A2%3C485%3AOTCCOD%3E2.0.CO%3B2-H