ACTA ARITHMETICA
LXXIV.3 (1996)

On a problem of Eisenstein

by

Peter Stevenhagen (Amsterdam)

1. Introduction. In 1844, a list of 11 open problems composed by Eisenstein was published in Crelle's journal [7]. Among these problems, which are rather diverse in nature and precision, there are three that pertain to class groups of quadratic orders. Class groups of other orders were still unknown at that time, and Eisenstein's questions are couched in Gauss's language of quadratic forms. In various forms, they ask for "criteria" to recognize quadratic discriminants that yield class numbers divisible by an integer n, and to recognize for such discriminants the classes that are in the kernel or the image of the multiplication-by-n map. For $n = 2$, this is accomplished by Gauss's theory of genera and ambiguous forms. From our modern point of view, it is clear that, in the case of quadratic orders, one cannot hope for an immediate generalization of these results if one replaces $n = 2$ by $n = 3$, as is done by Eisenstein in his eighth problem. In fact, the behavior of the odd part of quadratic class groups is in many ways as intractable as it was in Eisenstein's days, and our knowledge of their "average behavior" is almost entirely conjectural [2].

The problem we will focus on in this paper is Eisenstein's fourth question, which can be seen as a weak version of the problem above for the case $n = 3$. In this question, we are asked to give a criterion to decide a priori whether the equation $x^2 - dy^2 = 4$ for a positive integer $d \equiv 5 \bmod 8$ is solvable in *odd* integers x and y. Note that the congruence condition on d is clearly necessary for the existence of such a solution. As Eisenstein indicates, this question is related to the 3-divisibility of the class number of the order $\mathcal{O}_{4d} = \mathbb{Z}[\sqrt{d}]$ of discriminant $4d$. Writing $\mathcal{O}_\Delta$ and $h(\Delta)$ for the quadratic order of discriminant Δ and its class number, respectively, we can formulate this in modern terms in the following way.

1991 *Mathematics Subject Classification*: 11R11, 11R16.
Key words and phrases: quadratic units, cubic fields.

1.1. Lemma. *The following are equivalent for a positive integer* $d \equiv 5 \bmod 8$:

(1) *the equation* $x^2 - dy^2 = 4$ *has no solutions in odd integers* x *and* y;
(2) *the fundamental unit* $\varepsilon_d \in \mathcal{O}_d$ *lies in the unit class of* $(\mathcal{O}_d/2\mathcal{O}_d)^*$;
(3) *the unit groups* $\mathcal{O}_{4d}^*$ *and* $\mathcal{O}_d^*$ *coincide*;
(4) $h(4d) = 3h(d)$.

Proof. All solutions to the Pell equation in (1) are of the form $x+y\sqrt{d} = \pm 2\varepsilon_d^k$ for some $k \in \mathbb{Z}$. If the fundamental unit ε_d has norm $N(\varepsilon_d) = -1$, only the even exponents k yield a solution, otherwise all values of k are allowed. The requirement that x and y be odd means that ε_d^k lies in $\mathcal{O}_d = \mathbb{Z}[(1+\sqrt{d})/2]$ but not in $\mathcal{O}_{4d} = \mathbb{Z}+2\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$, so there is no such solution if $\mathcal{O}_{4d}^*$ and $\mathcal{O}_d^*$ coincide.

As $\mathcal{O}_d/2\mathcal{O}_d$ is a field of 4 elements for $d \equiv 5 \bmod 8$, we see from the equality

$$\mathcal{O}_{4d}^* = \ker[\mathcal{O}_d^* \xrightarrow{\varphi_2} (\mathcal{O}_d/2\mathcal{O}_d)^* \cong \mathbb{F}_4^*] \tag{1.2}$$

that $\mathcal{O}_{4d}^*$ and $\mathcal{O}_d^*$ coincide if and only if the reduction map φ_2 maps ε_d to the unit class of $(\mathcal{O}_d/2\mathcal{O}_d)^*$. If this is not the case, φ_2 is surjective and $\mathcal{O}_{4d}^*$ has index 3 in $\mathcal{O}_d^*$. In this situation, $x + y\sqrt{d} = 2\varepsilon_d^2$ yields a solution in odd integers in (1). This shows that (1), (2) and (3) are equivalent.

For (4), we observe that the natural map between the class groups of the orders $\mathcal{O}_{4d}$ and $\mathcal{O}_d$ yields an exact sequence

$$0 \to (\mathcal{O}_d/2\mathcal{O}_d)^*/\varphi_2[\mathcal{O}_d^*] \to \mathrm{Cl}(\mathcal{O}_{4d}) \to \mathrm{Cl}(\mathcal{O}_d) \to 0. \tag{1.3}$$

We conclude that $h(4d)$ equals $h(d)$ if φ_2 is surjective, and that $h(4d)$ equals $3h(d)$ in the situation of (2). ∎

Even if we believe that there is no simple criterion that enables us to decide a priori whether the equivalent statements in Lemma 1.1 hold for a given integer $d \equiv 5 \bmod 8$, there are related questions one might hope to be able to solve. The most obvious question is probably the determination of the *size* of the set of d's for which the statements in Lemma 1.1 hold. In the fundamental case, i.e., when $d \equiv 5 \bmod 8$ is squarefree, extensive computations have been performed by Stephens and Williams [9]. Let us denote the set of positive squarefree integers congruent to 5 modulo 8 by $\mathcal{D}$ and write $\mathcal{E}$ for the *Eisenstein set* of integers $d \in \mathcal{D}$ that satisfy the equivalent conditions of Lemma 1.1. As the reduction map $\varphi_2 : \mathcal{O}_d^* \to \mathbb{F}_4^*$ in (1.2) maps ε_d into a group of order 3, the most natural conjecture would be the following.

1.4. Conjecture. *The Eisenstein set $\mathcal{E}$ has natural density* $1/3$ *in* $\mathcal{D}$.

It is unreasonable to expect Conjecture 1.4 to be true without the restriction to squarefree values of d. For non-fundamental values $d = f^2 d_0 \equiv 5 \bmod 8$ with d_0 squarefree, the fundamental unit ε_d is the kth power of ε_{d_0}, where k is the order of ε_{d_0} in $(\mathcal{O}_{d_0}/f\mathcal{O}_{d_0})^*/(\mathbb{Z}/f\mathbb{Z})^*$. It follows that ε_d is the unit element in $(\mathcal{O}_d/2\mathcal{O}_d)^* = (\mathcal{O}_{d_0}/2\mathcal{O}_{d_0})^*$ as soon as 3 divides k. In fact, starting from the assumption that in the fundamental case, one has "equidistribution" of ε_{d_0} over $(\mathcal{O}_{d_0}/f\mathcal{O}_{d_0})^*/(\mathbb{Z}/f\mathbb{Z})^*$ for each odd f, one can adapt the argument in [11] to derive a plausible conjectural density for the general case.

The "natural" conjectural densities for the behavior of quadratic units modulo a fixed conductor are often in close accordance with numerical data. In the case of Conjecture 1.4, Stephens and Williams found that for the values $d \in \mathcal{D}$ in the interval $[10^8, 10^9]$, a fraction $29725316/91189086 \approx .326$ lies in the Eisenstein set $\mathcal{E}$.

In relation with the conjectured densities for the solvability of the negative Pell equation [11], similar distribution phenomena for quadratic units were numerically studied in [1]. A close match of conjectural and numerical data was found.

Another famous example of a conjectured distribution is the behavior modulo 16 of the quadratic unit ε_p for prime numbers $p \equiv 1 \bmod 8$. The class number $h(-4p)$ of the *imaginary* quadratic field $\mathbb{Q}(\sqrt{-p})$ is divisible by 4 for such p, and ε_p lies in the unit class of $(\mathcal{O}_p/4\mathcal{O}_p)^*/\{\pm 1\}$. It can be shown that $h(-4p)$ is divisible by 8 exactly when ε_p is trivial in $(\mathcal{O}_p/8\mathcal{O}_p)^*/\{\pm 1\}$, and divisible by 16 exactly when $p\varepsilon_p$ is trivial in $(\mathcal{O}_p/16\mathcal{O}_p)^*/\{\pm 1\}$, cf. [12, 13]. One can show that the set $\mathcal{P}$ of primes for which 8 divides $h(-4p)$ has density $1/2$ inside the set of primes congruent to 1 modulo 8. However, neither the set of primes p for which $h(-4p)$ is divisible by 16 nor its complement in $\mathcal{P}$ is known to be infinite. Numerically, $h(-4p)$ appears to be divisible by 16 for $1/2$ of the primes in $\mathcal{P}$, cf. [3].

Even though we are still unable to prove anything non-trivial in most of these distribution problems for quadratic units, there are a few positive exceptions. It is the purpose of this paper to show that Conjecture 1.4 is not entirely untractable. More precisely, we will show the following.

1.5. Theorem. *The upper density of the Eisenstein set $\mathcal{E}$ in $\mathcal{D}$ satisfies*

$$\limsup_{x\to\infty} \frac{\#\{d \in \mathcal{E} : d \le x\}}{\#\{d \in \mathcal{D} : d \le x\}} \le \frac{1}{2}.$$

I have not been able to prove a positive lower bound for the lower density of $\mathcal{E}$ in $\mathcal{D}$. As it is elementary to show that $\mathcal{D}$ satisfies $\lim_{x\to\infty} x^{-1}\#\{d \in \mathcal{D} : d \le x\} = \pi^{-2}$, one would need to show that $\#\{d \in \mathcal{E} : d \le x\}$ grows

linearly with x. We can, however, prove the following weaker result. Even though it is not an optimal result, it does show that $\mathcal{E}$ is infinite.

1.6. THEOREM. *The Eisenstein set $\mathcal{E}$ satisfies*

$$\#\{d \in \mathcal{E} : d \le x\} \gg x^{1/2}.$$

The proofs of Theorems 1.5 and 1.6, which can be found in Section 3, are based on the class field theoretic interpretation of the exact sequence (1.3), which allows us to construct elements of the Eisenstein set from suitable cubic number fields, and a method of Davenport and Heilbronn to count cubic number fields [5, 6]. As we use the method of Davenport and Heilbronn rather than their theorems, we have collected the various results on the counting of cubic fields that form the basis of our proof in a separate section. When combined with the main result (Theorem 3.3) of Section 3, they readily yield 1.5 and 1.6.

2. Counting cubic number fields. Let K be a cubic number field, i.e., a cubic extension of the rational number field $\mathbb{Q}$. Then we can associate a binary cubic form $F_K \in \mathbb{Z}[X,Y]$ with K by writing its ring of integers on a $\mathbb{Z}$-basis as $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\mu + \mathbb{Z}\nu$ and putting

$$\begin{aligned} F_K(X,Y) &= |\Delta_K|^{-1/2}|\Delta(\mu X + \nu Y)|^{1/2} \\ &= |\Delta_K|^{-1/2}\Big|\prod_{\sigma\neq\tau}(\sigma(\mu)-\tau(\mu))X + (\sigma(\nu)-\tau(\nu))Y\Big|^{1/2}. \end{aligned}$$

Here Δ_K is the discriminant of K, and σ and τ range over the distinct embeddings of K into $\overline{\mathbb{Q}}$. As is shown in [5], the form F_K is an irreducible primitive binary cubic form of discriminant Δ_K in $\mathbb{Z}[X,Y]$. It is only determined up to sign by the choice of μ and ν, but the induced "fundamental mapping" from the set of $\mathbb{Q}$-isomorphism classes of cubic fields to the set Φ of $\mathrm{GL}_2(\mathbb{Z})$-orbits of irreducible integral primitive binary cubic forms is injective. A precise description of the classes of the *field forms* that make up the image of this mapping is given in [6]. These are the classes that lie for each rational prime p in a subset $U_p \subset \Phi$ consisting of classes of forms whose reduction modulo $p^2\mathbb{Z}$ is of a certain type. The growth of the number of equivalence classes of binary forms of discriminant in either $[-x,0]$ or $[0,x]$ for $x \to \infty$ had already been determined by Davenport in the early fifties, and Davenport and Heilbronn combine this with a sieving argument to obtain an asymptotic estimate for the number of non-isomorphic cubic fields with discriminant in $[-x,0]$ or $[0,x]$. In the current paper, we will only need to count cubic fields K of discriminant $4d$, where $d \in \mathcal{D}$ is a squarefree positive integer congruent to 5 modulo 8. Once we have the alternative description of such K furnished by the following lemma, this can be done by a slight modification of the original argument of Davenport and Heilbronn.

2.1. Lemma. *Let K be a totally real cubic field. Then 2 is the only rational prime that is totally ramified in $K/\mathbb{Q}$ if and only if the discriminant Δ_K of K satisfies $\Delta_K/4 \in \mathcal{D}$.*

Proof. We use some generalities on cubic fields that may be found in [8]. For K a cubic number field, we can write the discriminant as $\Delta_K = f^2 d$ for some fundamental quadratic discriminant d. Note that d is positive exactly when K is totally real. A rational prime p is totally ramified in K if and only if p divides f, so 2 is the only totally ramified prime in $K/\mathbb{Q}$ if $\Delta_K/4$ lies in $\mathcal{D}$.

Conversely, suppose that 2 is the only totally ramified prime in $K/\mathbb{Q}$. Then all primes $p \neq 2$ that ramify in $K/\mathbb{Q}$ divide d but not f, so they divide Δ_K at most once. (This also follows from the fact that they have a single tamely ramified extension of ramification index 2 in K.) The extension $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ is an abelian extension of degree 3 that is totally and tamely ramified at the primes over 2, and unramified at all other primes. Class field theory tells us that the Galois group of this extension is a quotient of the ray class group of $\mathbb{Q}(\sqrt{d})$ of conductor 2. The natural image of $(\mathcal{O}_d/2\mathcal{O}_d)^*$ in this ray class group is the subgroup generated by inertia above 2. We deduce that $(\mathcal{O}_d/2\mathcal{O}_d)^*$ maps surjectively to the Galois group of $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$. It follows that 2 is inert in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, so d is squarefree and congruent to 5 mod 8. Moreover, the integer f, which is the conductor of the extension $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$, is equal to 2. This gives $\Delta_K/4 \in \mathcal{D}$. ∎

2.2. Proposition. *Let $\mathcal{K}$ be the set of isomorphism classes of cubic fields K for which the discriminant satisfies $\Delta_K/4 \in \mathcal{D}$. Then*

$$\lim_{x\to\infty} x^{-1}\#\{K \in \mathcal{K} : \Delta_K/4 \leq x\} = 1/(3\pi^2).$$

Proof. In [6], the growth of the set of isomorphism classes of cubic fields that are not totally ramified at any rational prime is studied in detail. The forms corresponding to these fields are characterized by the fact that their discriminants occur as discriminants of quadratic fields, i.e., they are not divisible by p^2 for $p \geq 3$, and either odd or congruent to 8 or 12 mod 16. In the notation of [6], this can be translated by saying that such forms lie in V_p for all primes p. The number of isomorphism classes of such fields of positive discriminant $< x$ grows asymptotically like $x/(2\pi^2)$ (see [6, Prop. 3]). For our current set of fields, Lemma 2.1 tells us that we have to replace the local condition at the prime 2 by a different one: we are looking at forms F that have a triple root modulo 2 and discriminant congruent to 4 modulo 8. In the notation of [6], this means that locally at 2, we want forms that lie in the class U_2 of the field forms but not in the class V_2 of forms corresponding to fields that are not totally ramified at 2. We can now deduce from [6, Lemmas 4 and 5] that we have to replace the local factor 3/5 at the prime 2 (corresponding

to V_2) by a factor $1/10$ (corresponding to $U_2 \setminus V_2$) in order to find the growth rate of the set $\mathcal{K}$: it contains asymptotically $\frac{5}{3} \cdot \frac{1}{10} \cdot x/(2\pi^2) = x/(12\pi^2)$ isomorphism classes of cubic fields K of discriminant $\Delta_K < x$. If we count up to $4x$, we get the constant of the proposition. ∎

A cubic field K of discriminant d is not totally ramified at any rational prime if and only if the cubic extension $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ is an unramified cyclic extension. This observation enables Davenport and Heilbronn to count the average number of unramified cubic cyclic extensions $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ for quadratic fields $\mathbb{Q}(\sqrt{d})$. For given fundamental discriminant d, it is easy to see that there are $(h_3^*(d)-1)/2$ such extensions of $\mathbb{Q}(\sqrt{d})$ that are pairwise non-isomorphic. Here $h_3^*(d)$ denotes the order of the 3-torsion subgroup $\mathrm{Cl}(\mathcal{O}_d)[3]$ of $\mathrm{Cl}(\mathcal{O}_d)$. By counting the number of cubic forms that have no total ramification at any prime p (i.e., forms that lie in V_p for all p), it is shown [6, Theorem 3] that for d ranging over the set of discriminants of real quadratic fields, the average value of $h_3^*(d)$ equals $4/3$. We need to adapt this result to our smaller set of discriminants $\mathcal{D}$.

2.3. Proposition. *The average value of $h_3^*(d)$ for $d \in \mathcal{D}$ equals*

$$\lim_{x\to\infty} \frac{\sum_{d\in\mathcal{D}:d\le x} h_3^*(d)}{\sum_{d\in\mathcal{D}:d\le x} 1} = \frac{4}{3}.$$

Proof. There are asymptotically $\prod_{p>2 \text{ prime}}(1-p^{-2})x = 8x/\pi^2$ integers $d < x$ that are not divisible by the square of any odd prime, and these integers are equidistributed over the residue classes modulo 16. The real quadratic field discriminants are those d that lie in the six residue classes $1, 5, 8, 9, 12, 13 \bmod 16$, so there are asymptotically $\frac{6}{16} \cdot 8x/\pi^2 = 3x/\pi^2$ real quadratic field discriminants $d < x$. If we restrict to discriminants in $d \in \mathcal{D}$, which are congruent to 5 modulo 8, only 2 residue classes out of 6 are allowed, so we lose a factor 3 and find a main term x/π^2.

On the side of the field forms F_K that have no total ramification at any rational prime in $K/\mathbb{Q}$, we have to impose the additional restriction at 2 that the discriminant be congruent to $5 \bmod 8$. This is a straightforward computation. We know from [6, Lemma 4] that the density factor at $p = 2$ of the forms which have no total ramification at 2 (i.e., they lie in V_2) equals $(p^2-1)/(p^2+1) = 3/5$. An elementary counting argument for forms modulo p [6, Lemma 1] shows that the density factor at $p = 2$ of the forms with discriminant coprime to p equals $(p^2-p)/(p^2+1) = 2/5$. Such discriminants have $\Delta \equiv 1 \bmod 4$, and we want to show that $\Delta \equiv 1 \bmod 8$ and $\Delta \equiv 5 \bmod 8$ both contribute $1/5$. If this is the case, we see that we have to replace the local factor $3/5$ at 2 by $1/5$, so there is a factor 3 disappearing both on the cubic form side and on the quadratic field side. The average value of $h_3^*(d)$ then remains unchanged.

We see from the explicit form of the discriminant

$$\Delta(aX^3+bX^2Y+cXY^2+dY^3) = b^2c^2+18abcd-27a^2d^2-4(b^3c+d^3a)$$

of a cubic form and its reduction $\Delta \equiv b^2c^2+a^2d^2 \equiv 1 \bmod 2$ that Δ is odd if and only if exactly one of the terms ad and bc is odd. For such Δ we have

$$\Delta \equiv \begin{cases} 1 \bmod 8 & \text{if } ad \text{ is odd,} \\ 5 \bmod 8 & \text{if } ad \text{ is even,} \end{cases}$$

so we get the same contribution from the residue classes $1 \bmod 8$ and $5 \bmod 8$. ∎

2.4. Corollary. *The lower density of the discriminants $d \in \mathcal{D}$ for which 3 does not divide $h(d)$ satisfies*

$$\liminf_{x\to\infty} \frac{\#\{d \in \mathcal{D} : d \le x \text{ and } 3 \nmid h(d)\}}{\#\{d \in \mathcal{D} : d \le x\}} \ge \frac{5}{6}.$$

Proof. Let α be this lower density. Then the subset of discriminants $d \in \mathcal{D}$ with $h_3^*(d) \ge 3$ has upper density $\ge 1-\alpha$, so we find $\alpha+3(1-\alpha) \le 4/3$. This immediately yields $\alpha \ge 5/6$. ∎

3. Densities for Eisenstein's problem. In order to apply the counting of cubic fields performed in the previous section to Eisenstein's problem as formulated in Conjecture 1.4, we take the set $\mathcal{K}$ of isomorphism classes of cubic fields from Proposition 2.2 and consider the map

$$\Psi : \mathcal{K} \to \mathcal{D}, \qquad K \mapsto \Delta_K/4.$$

Theorems 1.5 and 1.6 are based on the study of the map Ψ. The image of Ψ is closely related to the behavior of the exact sequence of finite abelian groups

$$0 \to (\mathcal{O}_d/2\mathcal{O}_d)^*/\varphi_2[\mathcal{O}_d^*] \to \mathrm{Cl}(\mathcal{O}_{4d}) \to \mathrm{Cl}(\mathcal{O}_d) \to 0 \tag{3.1}$$

that we encountered as (1.3) in the proof of Lemma 1.1. We will employ the class field theoretic interpretation of (3.1) as an exact sequence of Galois groups

$$0 \to \mathrm{Gal}(R_2/H) \to \mathrm{Gal}(R_2/\mathbb{Q}(\sqrt{d})) \to \mathrm{Gal}(H/\mathbb{Q}(\sqrt{d})) \to 0. \tag{3.2}$$

Here H denotes the Hilbert class field of $\mathbb{Q}(\sqrt{d})$, and R_2 the ring class field corresponding to the quadratic order of discriminant $4d$. We can also view R_2 as the ray class field of conductor 2 of $\mathbb{Q}(\sqrt{d})$, since for conductor $f = 2$ the group $(\mathbb{Z}/f\mathbb{Z})^* = 1$ is simply too small to make a difference between the ray class field and the ring class field of conductor f possible.

We recall that for any conductor $f \in \mathbb{Z}_{>0}$, the ring class field of conductor f can be characterized [4, Theorem 9.18] as the maximal subfield of the ray class field of conductor f that is dihedral over $\mathbb{Q}$. This means that we have $\mathrm{Gal}(R_2/\mathbb{Q}) = \mathrm{Gal}(R_2/\mathbb{Q}(\sqrt{d})) \rtimes \mathbb{Z}/2\mathbb{Z}$, where the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$ acts by inversion on $\mathrm{Gal}(R_2/\mathbb{Q}(\sqrt{d}))$.

3.3. Theorem. *The map Ψ satisfies the following properties.*

(1) *The image of Ψ lies in the Eisenstein set $\mathcal{E}$; it consists of those $d \in \mathcal{E}$ for which the sequence* (3.1) *is split.*

(2) *If $d \in \mathcal{D}$ lies in the image of Ψ, then $\Psi^{-1}(d)$ has $h_3^*(d)$ elements.*

Proof. Let $d \in \mathcal{D}$ be a discriminant that is in the image of Ψ. Then there exists a cubic field K of discriminant $4d$, and the field $K(\sqrt{d})$ is a cyclic cubic extension of conductor 2 of $\mathbb{Q}(\sqrt{d})$ that is dihedral over $\mathbb{Q}$. This implies that the ring class field R_2 of conductor 2 of $\mathbb{Q}(\sqrt{d})$ has degree at least 3 over the Hilbert class field H, so we have $h(4d) = 3h(d)$, and d is in the Eisenstein set by (4) of Lemma 1.1. Moreover, the canonical map $\mathrm{Gal}(R_2/\mathbb{Q}(\sqrt{d})) \to \mathrm{Gal}(K(\sqrt{d})/\mathbb{Q}(\sqrt{d}))$ provides a splitting of the Galois group version (3.2) of (3.1).

Conversely, if d is in the Eisenstein set and (3.2) is split, there exists a cyclic cubic extension $F/\mathbb{Q}(\sqrt{d})$ of conductor 2 inside the ring class field extension $R_2/\mathbb{Q}(\sqrt{d})$ of conductor 2. As F is dihedral over $\mathbb{Q}$, it is of the form $F = K(\sqrt{d})$ for some cubic field K of discriminant $\Delta_K = 4d$. Thus d is in the image of Ψ, and we have proved (1).

Let now d be in the image of Ψ. Then the argument above shows that the isomorphism classes of cubic fields in $\Psi^{-1}(d)$ correspond to the cyclic cubic extensions F of conductor 2 of $\mathbb{Q}(\sqrt{d})$ that are contained in the ring class field R_2 of conductor 2 of $\mathbb{Q}(\sqrt{d})$. There are $(h_3^*(4d)-1)/2$ cubic subextensions of $R_2/\mathbb{Q}(\sqrt{d})$, and $(h_3^*(d)-1)/2$ of them are unramified over $\mathbb{Q}(\sqrt{d})$. We have $h_3^*(4d) = 3h_3^*(d)$ because $h(4d)$ equals $3h(d)$ and (3.1) is split. Subtracting yields $(3h_3^*(d)-1)/2-(h_3^*(d)-1)/2 = h_3^*(d)$ isomorphism classes in $\Psi^{-1}(d)$. Note that this answer reflects the fact if the classes of K_1 and K_2 are in $\Psi^{-1}(d)$, then the extension $K_1(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ arises from $K_2(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ by twisting with an unramified cyclic cubic extension $C/\mathbb{Q}(\sqrt{d})$. ∎

Proof of Theorem 1.5. Let $\mathcal{D}'$ denote the set of discriminants $d \in \mathcal{D}$ for which the sequence (1.3) is split. If $d \in \mathcal{D}$ is a discriminant for which 3 does not divide $h(d)$, then d is clearly in $\mathcal{D}'$. It follows from Corollary 2.4 that the lower density of $\mathcal{D}'$ in $\mathcal{D}$ is at least $5/6$.

By Theorem 3.3(1), the intersection $\mathcal{E}' = \mathcal{D}' \cap \mathcal{E}$ of discriminants d in the Eisenstein set for which the sequence (1.3) is split is exactly the image of the map Ψ. By Proposition 2.2, the set $\mathcal{K}$ contains asymptotically $x/(3\pi^2)$ isomorphism classes of cubic fields K with $\Delta_K/4 < x$. As $\mathcal{D}$ itself contains

asymptotically x/π^2 discriminants $d < x$, we find that the upper density of $\mathcal{E}' = \Psi[\mathcal{K}]$ in $\mathcal{D}$ is at most $1/3$. It follows that the lower density of the set $\mathcal{D}' \setminus \mathcal{E}' = \mathcal{D}' \setminus \mathcal{E}$ in $\mathcal{D}$ is at least $5/6 - 1/3 = 1/2$. As $\mathcal{D} \setminus \mathcal{E}$ contains $\mathcal{D}' \setminus \mathcal{E}$, the complement $\mathcal{D} \setminus \mathcal{E}$ of the Eisenstein set in $\mathcal{D}$ also has lower density at least $1/2$. It follows that the upper density of the Eisenstein set itself in $\mathcal{D}$ is bounded by $1/2$. ∎

Proof of Theorem 1.6. As the Eisenstein set $\mathcal{E}$ contains the set $\mathcal{E}' = \Psi[\mathcal{K}]$, it suffices to show that the cardinality of the Ψ-image of $\mathcal{K}_x = \{K \in \mathcal{K} : \Delta_K/4 < x\}$ grows at least like a positive constant times $x^{1/2}$ with x. If d is in $\Psi[\mathcal{K}_x]$, there are exactly $h_3^*(d)$ elements in $\mathcal{K}_x$ that map to d. Standard estimates for real quadratic class numbers show that for $d < x$, we have $h_3^*(d) \le h(d) \le x^{1/2}$. As no more than $x^{1/2}$ isomorphism classes of cubic fields from $\mathcal{K}_x$ map to the same discriminant, we see from the size of $\mathcal{K}_x$ itself given in Proposition 2.2 that, asymptotically, $\#\Psi[\mathcal{K}_x]$ has at least $x^{1/2}/(3\pi^2)$ elements. ∎

References

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

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

[3] H. Cohn and J. C. Lagarias, *On the existence of fields governing the* 2*-invariants of the class groups of* $\mathbb{Q}(\sqrt{dp})$ *as* p *varies*, Math. Comp. 41 (1983), 711–730.

[4] D. A. Cox, *Primes of the Form* $x^2 + ny^2$, Wiley-Interscience, 1989.

[5] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, *I*, Bull. London Math. Soc. 1 (1969), 345–348.

[6] —, —, *On the density of discriminants of cubic fields*, *II*, Proc. Roy. Soc. London A 322 (1971), 405–420.

[7] G. Eisenstein, *Aufgaben*, J. Reine Angew. Math. 27 (1844), 86–88; see also: Mathematische Werke, Band I, Chelsea, 111–113.

[8] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischen Grundlage*, Math. Z. 31 (1930), 565–582.

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

[10] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Experiment. Math. 2 (1993), 121–136.

[11] —, *A density conjecture for the negative Pell equation*, in: Computational Algebra and Number Theory, Sydney 1992, Kluwer, 1995, 187–200.

[12] —, *Divisibility by* 2*-powers of certain quadratic class numbers*, J. Number Theory 43 (1993), 1–19.

[13] K. S. Williams, *On the class number of* $\mathbb{Q}(\sqrt{-p})$ *modulo* 16, *for* $p \equiv 1 \bmod 8$ *a prime*, Acta Arith. 39 (1981), 381–398.

FACULTEIT WISKUNDE EN INFORMATICA
UNIVERSITEIT VAN AMSTERDAM
PLANTAGE MUIDERGRACHT 24
1018 TV AMSTERDAM, THE NETHERLANDS
E-mail: PSH@FWI.UVA.NL

Received on 18.4.1995
and in revised form on 29.5.1995 (2777)