ACTA ARITHMETICA
LX.4 (1992)

The imaginary quadratic fields of class number 4

by

STEVEN ARNO (Bowie, Md.)

1. Introduction. In this paper we prove that the classical list of 54 imaginary quadratic fields of class number 4 is complete. In so doing we solve another classical problem rooted in the work of Gauss concerning the unique representation of an integer as the sum of three squares.

We point out that although Baker [2, 3] and Stark [18, 19] succeeded in solving the class number 1 and 2 problems, their methods did not extend to the higher cases. It was not until the work of Goldfeld, Gross, and Zagier [12, 13] that a general method was developed. This new method, however, does not allow one to solve the even class number problems without a good deal of further work. In this regard, we note that Oesterlé [17] finished the class number 3 problem, while the class number 8 problem still appears to be intractable.

Our paper is organized as follows. Section 2 discusses the problem of unique representation of an integer as a sum of three squares and its relation to the class number 4 problem. This topic has been dealt with by many authors, and we refer the reader to [4] for a more historical perspective. In Section 3 we discuss the powerful methods of Goldfeld, Gross, and Zagier by which one shows that if $d > c$, for an explicitly given constant c, then the class number $h(-d)$ is greater than 4. In our case the constant c is on the order of $e^{100\,000}$. The discriminants less than c cannot be handled in a uniform way, and we are therefore forced to consider several cases. In Section 4 we define the notions of "small" and "large" sets of minima of reduced forms of discriminant $-d$, and show that the work of Stark [19] can be used to handle discriminants corresponding to "small" sets in the approximate range $10^{14} < d < c$. Section 5 shows that the methods of Montgomery and Weinberger [15] are well suited to the d in this range which correspond to "large" sets. We then show, in Section 6, that in the case of class number 4 there are no exceptional sets. Together Sections 4, 5, and 6 constitute a single unit covering discriminants in the approximate range $10^{14} < d < c$. Finally, in Section 7 we discuss a sieve which can be used to find the discriminants of class number 4 with $d < 10^{14}$. Similar sieve techniques were developed by Lehmer, Lehmer and Shanks in [14].

Acknowledgements. I would like to thank Peter Sarnak for suggesting this problem to me and Duncan Buell for his careful reading of the manuscript. I would also like to thank the people at NASA Ames Research Center for the use of their CRAY X-MP Supercomputer, and especially David Bailey for his help and kindness.

2. Representation as a sum of 3 squares. Given a positive integer n, we denote by $P_3(n)$ the number of solutions of

$$x^2 + y^2 + z^2 = n \tag{1}$$

with $0 \le x \le y \le z$. The cases $n \equiv 0 \pmod 4$ and $n \equiv 7 \pmod 8$ are of no interest since $P_3(n) = P_3(n/4)$ in the former, and $P_3(n) = 0$ in the latter. For the remaining cases, i.e. $n \equiv 1, 2, 3, 5, 6 \pmod 8$, Legendre showed that (1) always has a solution such that $(x, y, z) = 1$.

Gauss conjectured that for $n \equiv 1, 2, 3, 5, 6 \pmod 8$ the function $P_3(n) \to \infty$ as $n \to \infty$, and Heilbronn confirmed the conjecture in the 1930's. It then became natural to ask for a complete listing of the n for which $P_3(n) = k$, $k > 0$. However, even for $k = 1$ the problem proved quite difficult.

The basic method for attacking this problem is via a famous theorem of Gauss which relates the quantity $P_3(n)$ to the quantity $h(-d)$, where $h(-d)$ denotes the number of equivalence classes of binary quadratic forms of discriminant $-d$, and $d = n$ or $4n$.

In order to state Gauss' theorem we first replace $P_3(n)$ by the related and simpler function $r_3(n)$, where $r_3(n)$ denotes the number of solutions of (1) without restrictions on the signs or relative sizes of x, y, and z. We may assume that n is squarefree, since otherwise $P_3(n) > 1$ trivially. It is then clear that for $n > 3$ and some integer k

$$r_3(n) = 24k \quad \text{and} \quad r_3(n) \le 48P_3(n)\,. \tag{2}$$

Theorem 1 (Gauss). *If $n > 4$ is squarefree and $n \equiv 3 \pmod 8$, then*

$$r_3(n) = 24h(-n)\,;$$

If $n > 4$ is squarefree and $n \equiv 1, 2, 5, 6 \pmod 8$, then

$$r_3(n) = 12h(-4n)\,.$$

We see from (2) that for $n \equiv 3 \pmod 8$

$$P_3(n) \ge h(-n)/2\,;$$

while for $n \equiv 1, 2, 5, 6 \pmod 8$

$$P_3(n) \geq h(-4n)/4\,.$$

It follows that if we find all d for which $h(-d) \leq 4$, we will as a corollary have found all n such that $P_3(n) = 1$. Further, since (2) shows us that $r_3(n)$ is a multiple of 24, Gauss' theorem implies that if n is squarefree, $n > 3$, and $n \equiv 1, 2, 5, 6 \pmod 8$, then $h(-d)$ is even. Hence only the d such that $h(-d) = 1, 2$, or 4, need to be found.

As mentioned above, the n corresponding to class numbers 1 and 2 were successfully dealt with by Baker and Stark.

3. The work of Goldfeld, Gross, and Zagier. By an elliptic curve E over $\mathbb{Q}$ we mean an equation of the form

$$y^2 = f_3(x)\,, \tag{3}$$

where $f_3(x)$ is a cubic polynomial over $\mathbb{Z}$ with distinct roots, and hence discriminant $\Delta \neq 0$. To E we associate an $\mathcal{L}$-function

$$\mathcal{L}_E(s) = \prod_{p\mid\Delta}(1 - t_p p^{-s})^{-1} \prod_{p\nmid\Delta}(1 - t_p p^{-s} + p^{1-2s})^{-1} = \sum_{n=1}^{\infty} a_n n^{-s}\,, \tag{4}$$

where $t_p = p - N_p$, and N_p is the number of solutions of (3) modulo p. There is a large class of curves, usually called Weil curves, for which it is known that $\mathcal{L}_E(s)$ is entire and satisfies a functional equation $s \to 2 - s$. The defining property of a Weil curve is that

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi iz} \tag{5}$$

should be a modular form of weight 2 on $\Gamma_0(N)$, where N is the conductor of E. We also associate an abelian group to E,

$$E_{\mathbb{Q}} = \{(x, y) \in \mathbb{Q} \oplus \mathbb{Q} \mid y^2 = f_3(x)\} \cup \{\infty\}\,, \tag{6}$$

the group of rational points on E. Mordell [16] showed in 1922 that

$$E_{\mathbb{Q}} = \mathbb{Z}^r \oplus \{\text{torsion subgroup}\}\,, \tag{7}$$

where $r \in \mathbb{Z}$ is the rank of $E_{\mathbb{Q}}$. The well known conjecture of Birch and Swinnerton-Dyer asserts that $\mathcal{L}_E(s)$ has a zero of order r at $s = 1$.

By Lemma 8 (see Section 7), $\chi(p) = \left(\dfrac{-d}{p}\right) = -1$ for all p with $p \nmid d$ and $p < (d/4)^{1/h}$. Therefore if d is large and h is small, χ will look like the completely multiplicative function $\lambda(n)$, defined by $\lambda(p) = -1$ $\forall p$. Hence, if E is a Weil curve, we would expect the functions

$$\mathcal{L}_E(s, \chi) = \sum \frac{a_n \chi(n)}{n^s}\,, \tag{8}$$

$$\mathcal{L}_E(s,\lambda) = \sum \frac{a_n\lambda(n)}{n^s} \tag{9}$$

to behave similarly. However, since $\mathcal{L}_E(s,\chi)$ is entire,

$$\Psi_\chi(s) = \mathcal{L}_E(s)\mathcal{L}_E(s,\chi) \tag{10}$$

satisfies $\operatorname{ord}(\Psi_\chi)_{s=1} \geq \operatorname{ord}(\mathcal{L}_E(s))_{s=1}$ (where $\operatorname{ord}(f)_{s=c}$ denotes the order of the zero of f at $s=c$), while

$$\Psi_\lambda(s) = \mathcal{L}_E(s)\mathcal{L}_E(s,\lambda) \tag{11}$$

always satisfies $\operatorname{ord}(\Psi_\lambda)_{s=1} = 1$.

Goldfeld [12] was able to exploit this idea and show that if there is a Weil curve whose associated $\mathcal{L}$-function has a zero of at least third order at $s=1$, then $h(-d) > c(\varepsilon)(\log d)^{1-\varepsilon}$ for some effectively computable constant $c(\varepsilon)$, $\varepsilon > 0$. Further, on the basis of the Birch and Swinnerton-Dyer conjecture one would expect such curves to exist since there are curves known to have rank ≥ 3. The details involved in Goldfeld's proof are long and complicated, but a very readable account has been given by Oesterlé [17].

Given a Weil curve E, it is in general very difficult to obtain any information about $\operatorname{ord}(\mathcal{L}_E(s))_{s=1}$. However, a remarkable theorem of Gross and Zagier [13] allows one to show in certain cases that $\operatorname{ord}(\mathcal{L}_E(s))_{s=1} \geq 3$. Using curves found by Gross, Zagier, and Serre, Oesterlé [17] obtained the following theorem.

THEOREM 2. *If $h(-d) = 4$ and $(d, 5077) = 1$, then $d < e^{2700}$. If $h(-d) = 4$ and $(d, 5077) > 1$, then $d < e^{100\,000}$.*

4. "Small" sets. Let k be an imaginary quadratic field, and $\zeta_k(s)$ the zeta function of k. We have the following fundamental formula for $\zeta_k(s)$ (see [15, 20])

$$\zeta_k(s) = \zeta(2s)\Big(\sum a_i^{-s}\Big) + \frac{2^{2s-1}\pi^{1/2}\zeta(2s-1)\Gamma(s-1/2)(\sum a_i^{s-1})}{\Gamma(s)d^{s-1/2}} + R_{a_i}(s)\,, \tag{12}$$

where the summation extends over the reduced forms of discriminant $-d$, a_i is the minimum of a given form, and

$$R_a = \frac{2^{s+1/2}\pi^s}{a^{1/2}\Gamma(s)d^{s/2-1/4}} \sum_{n=1}^{\infty} n^{s-1/2}\sigma_{1-2s}(n)\cos\left(\frac{\pi n b}{a}\right) \times \int_0^\infty \theta^{s-3/2}e^{-\frac{\pi n d}{2a}(\theta+\theta^{-1})}\,d\theta\,, \tag{13}$$

for $\sigma_s(n) = \sum_{d\mid n} d^s$.

LEMMA 1. $|R_a(s)| \le \dfrac{10a^{1/2}e^{\frac{-\pi d^{1/2}}{2a}}}{\Gamma(s)(\pi d)^{1/2}}$ *on* $\sigma = \frac{1}{2}$.

Proof. Let $c = \pi n d^{1/2}/2a$. Since

$$\int\limits_0^\infty \theta^{-1}e^{-c(\theta+\theta^{-1})}\,d\theta = \int\limits_0^1 \theta^{-1}e^{-c(\theta+\theta^{-1})}\,d\theta + \int\limits_1^\infty \theta^{-1}e^{-c(\theta+\theta^{-1})}\,d\theta \tag{14}$$

$$= 2\int\limits_1^\infty \theta^{-1}e^{-c(\theta+\theta^{-1})}\,d\theta \tag{15}$$

$$\le 2\int\limits_1^\infty e^{-c\theta}\,d\theta \tag{16}$$

$$= \frac{2e^{-c}}{c}\,, \tag{17}$$

we have

$$|R_a(s)| \le \frac{8a^{1/2}}{\Gamma(s)(\pi d)^{1/2}}\sum_{n=1}^\infty \frac{\sigma_0(n)}{n}e^{-\pi n d^{1/2}/2a} \tag{18}$$
$$\le \frac{8a^{1/2}}{\Gamma(s)(\pi d)^{1/2}}\left(\frac{e^{-\pi d^{1/2}/2a}}{1-e^{-\pi d^{1/2}/2a}}\right),$$

from which the lemma follows.

Following Stark [18] we let $s_n = \frac{1}{2} + i\gamma_n$ be the nth zero of $\zeta(s)$ on $\sigma = 1/2$. For $s = s_n$ we may rewrite (12) as

$$\left(\frac{d}{4\pi^2}\right)^{i\gamma_n} = -A_1 - A_2\,, \tag{19}$$

where

$$A_1 = \frac{(\sum a_i^{-1/2+i\gamma_n})\zeta(1-2i\gamma_n)\Gamma(1/2-i\gamma_n)}{(\sum a_i^{-1/2-i\gamma_n})\zeta(1+2i\gamma_n)\Gamma(1/2+i\gamma_n)}\,, \tag{20}$$

$$A_2 = \left(\frac{d}{4\pi^2}\right)^{i\gamma_n}\frac{\sum R_{a_i}(s_n)}{(\sum a_i^{-1/2-i\gamma_n})\zeta(1+2i\gamma_n)}\,. \tag{21}$$

Since A_1 has modulus 1, we may rewrite (19) as

$$\left(\frac{d}{4\pi^2}\right)^{i\gamma_n} = -A_1(1-\Theta A_2)\,, \tag{22}$$

for some $|\Theta| = 1$. Defining α_n, $0 \le \alpha_n \le 2\pi$, by

$$\alpha_n = \pi - 2\arg(\zeta(2s_n)) - 2\arg(\Gamma(s_n)) \pmod{2\pi} \tag{23}$$

and taking arguments in (22) yields the following lemma:

Lemma 2. *There exists an integer x_n such that*

$$\gamma_n \log\left(\frac{d}{4\pi^2}\right) = \alpha_n + 2\pi x_n + \arg\Big(\sum a_i^{-1/2+i\gamma_n}\Big) + \arg(1+\Theta_n A_2)\,.$$

Choosing $n = 1$, $n = m$, and subtracting leads to

$$(24)\qquad \bigg| x_m - \frac{\gamma_m x_1}{\gamma_1} - \frac{1}{2\pi}\left(\frac{\gamma_m \alpha_1}{\gamma_1} - \alpha_m\right) - \frac{1}{\pi}\left(\frac{\gamma_m}{\gamma_1}\arg\Big(\sum a_i^{-1/2+i\gamma_1}\Big) - \arg\Big(\sum a_i^{-1/2+i\gamma_m}\Big)\right)\bigg| \le \mathrm{Er}\,,$$

where

$$(25)\qquad \mathrm{Er} = \frac{1}{2\pi}\left|\frac{\gamma_m}{\gamma_1}\arg(1+\Theta_1 A_2) - \arg(1+\Theta_m A_2)\right|.$$

It is important to notice some of the weaknesses inherent in the above expression since this will help to motivate the definitions which follow. First note that if $h(-d) = 4$ and n satisfies $1 \le n \le 11$, then Lemma 1 implies

$$(26)\qquad |A_2(s_n)| \le \frac{80((a_{\max})^{1/2} e^{\frac{\pi}{2}(53 - \frac{d^{1/2}}{a_{\max}})})}{\pi d^{1/2} |\sum a_i^{-1/2-i\gamma_n}|}\,.$$

We see from this inequality that our error term is strongly affected by the height of the zero s_n. Further, if any a_i is near $d^{1/2}$ then our error term will be large!

With the previous comments in mind, let $h(-d) = 4$, and let a_i, $i = 1,\ldots,4$, be the leading coefficients of reduced forms of discriminant $-d$. Recall that $a_1 = 1$.

Definition. We say that the set $\{a_i\}$ is *small* if $a_2 < 23$, $a_3 < 2470$, and $a_4 = a_2 a_3$.

Definition. We say that the set $\{a_i\}$ is *large* if $a_2 \ge 23$, or $a_3 \ge 2470$.

Definition. We say that the set $\{a_i\}$ is *bad* if it is neither small nor large, i.e. if $a_2 < 23$, and $a_3 < 2470$, but $a_4 \ne a_2 a_3$.

Lemma 3. *If the set $\{a_i\}$ is small*, $d > 10^{14}$, *and n satisfies* $1 \le n \le 11$, *then* $\mathrm{Er} < e^{-25}$.

Proof. This follows from (25), and (26) along with the elementary inequality $\arg(1+z) \le \pi z/3$ which is valid for $|z| < 1/2$.

We are now in a position to prove the main result of this section.

Theorem 3. *If the set $\{a_i\}$ is small*, *and* $10^{14} \le d \le e^{2800}$, *then* $h(-d) > 4$.

Proof. From (24) and Lemma 3 we know that the expression

$$\frac{\gamma_m x_1}{\gamma_1} - \frac{1}{2\pi}\left(\frac{\gamma_m \alpha_1}{\gamma_1} - \alpha_m\right) - \frac{1}{\pi}\left(\frac{\gamma_m}{\gamma_1}\arg\Big(\sum a_i^{-1/2+i\gamma_1}\Big) - \arg\Big(\sum a_i^{-1/2+i\gamma_m}\Big)\right) \tag{27}$$

is within e^{-25} of an integer, though we are forced to use a somewhat larger number to account for computational error. A computer check then shows that if the set $\{a_i\}$ is small, and $10 \le x_1 \le 7000$, then there is some n, $1 \le n \le 11$, for which the equation (24) does not hold. By Lemma 2,

$$4\pi^2 e^{2\pi x_1/\gamma_1 + 2} \ge d \ge e^{2\pi x_1/\gamma_1},$$

from which the theorem follows.

Comment. A list of the zeros we used can be found in Table 1.

5. "Large" sets. Let $(d,k) = 1$, and $\chi_1(n) = \left(\frac{-d}{n}\right)$. Also let χ be a real, primitive character modulo k. Analogous to the formula (12) for $\zeta(s)\mathcal{L}(s,\chi)$ we have the following fundamental formula for $\mathcal{L}(s,\chi)\mathcal{L}(s,\chi\chi_1)$ (see [15]):

$$it\mathcal{L}(\tfrac12 + it, \chi)\mathcal{L}(\tfrac12 + it, \chi\chi_1)\Gamma(\tfrac12 + it)\left(\frac{kd^{1/2}}{2\pi}\right)^{it} = M(t)\sin(\vartheta(t)) + \Theta t E(t), \tag{28}$$

where $|\Theta| \le 1$, and for $P_k(s) = \prod_{p|k}(1 - p^{-2s})$ and $A(s) = \sum_i \chi(a_i)a_i^{-s}$ we have

$$M(t) = |2t\zeta(1+2it)\Gamma(\tfrac12 + it)P_k(1+2it)A(\tfrac12 + it)|, \tag{29}$$

$$\vartheta(t) = \arg\left(i\zeta(1+2it)\Gamma(\tfrac12 + it)P_k(1+2it)A(\tfrac12 + it)\left(\frac{kd^{1/2}}{2\pi}\right)^{it}\right) \tag{30}$$

and

$$E(t) = 4\pi k^{-1}\sum_{\mathcal{Q}_i} a_i^{-1/2}\sum_{n=1}^{\infty} K_0\left(\frac{\pi n d^{1/2}}{ak}\right)\sum_{y|n}\Big|\sum_{j=1}^{k}\chi(\mathcal{Q}_i(j,y)e^{2\pi ijn/ky})\Big|. \tag{31}$$

(Here $\mathcal{Q}_i$ represents a reduced form of discriminant $-d$ and leading coefficient a_i, and for $\mathrm{Re}\,(x) > 0$, and $\nu \in \mathbb{C}$

$$K_\nu(x) = \tfrac12\int_1^{\infty} e^{-\frac{x}{2}(u+u^{-1})}(u^{\nu-1} + u^{-\nu-1})\,du \tag{32}$$

is the modified Bessel function of the second kind.)

The following three lemmas were proved by Montgomery and Weinberger in [15].

Lemma 4. *If* $0 \le t \le 1/20$, *then*

$$M(t) \ge \tfrac{7}{4} \prod_{p|k} (1-p^{-1}) |A(\tfrac{1}{2}+it)| ;$$

If $0 \le t \le 1/4$, *then*

$$M(t) \ge \tfrac{11}{7} \prod_{p|k} (1-p^{-1}) |A(\tfrac{1}{2}+it)| .$$

Lemma 5. *We have*

$$\vartheta(t) = t\biggl(C + \log\biggl(\frac{kd^{1/2}}{8\pi}\biggr)\biggr) + 3\Theta t^3 + \Theta t\biggl(a(k) + 2\sum_{p|k} \frac{\log p}{p-1}\biggr),$$

where $C = 0.5771\ldots$ *is Euler's constant, and* $a(k) = |\frac{A'}{A}(\frac{1}{2}+it)|$.

Lemma 6. *If* $0 \le t \le 1/4$, *then*

$$E(t) \le \frac{8}{3^{1/4}\pi^{1/2}} d^{-1/4} k^{1/2} \log k \prod_{p|k} (2+3p^{-3/2}) \Bigl(\sum_i e^{-\pi d^{1/2}/2a_i k}\Bigr).$$

Following [15] we choose t such that $\mathcal{L}(\frac{1}{2}+it,\chi) = 0$, and rewrite (28) as

$$|\sin(\vartheta(t))| \le r , \tag{33}$$

where

$$r = t \left| \frac{E(t)}{M(t)} \right| . \tag{34}$$

Setting $\vartheta(t) = n\pi + \delta$, and applying Lemma 5 we arrive at

$$\frac{2}{t}\left(-|S(t)| - \varepsilon(r) + n\pi + t\log\frac{e^C k}{8\pi}\right) \le \log d \le \frac{2}{t}\left(|S(t)| + \varepsilon(r) + n\pi + t\log\frac{e^C k}{8\pi}\right) , \tag{35}$$

where

$$|S(t)| \le 3t^3 + t\biggl(a(k) + 2\sum_{p|k}\frac{\log p}{p-1}\biggr),$$

and $|\delta| \le \varepsilon(r)$ for some function ε of r.

This expression shows us that d must lie in certain intervals. It is important to note that if $a(k)$ is large our intervals will be large, and the expression above will lose its utility. This explains why this method is best suited to "large" sets.

In the early ranges, i.e. around 10^{14} through 10^{20}, our error terms are still somewhat large, and there is some degree of subtlety in handling these cases. Therefore we supply the reader with several details pertaining to these ranges even though this makes our exposition less pleasant. We will need the following theorem of Gauss.

THEOREM 4. *Let N denote the number of primes dividing d. Then $2^{N-1}|h(-d)$.*

As a corollary we see that if $h(-d) \le 4$ then d is divisible by at most three primes.

We assume in cases 1 through 3 that the sets $\{a_i\}$ are large, and use the zeros found in Table 2.

Case 1. We choose $k = 2683$, and assume that $(k, d) = 1$. In this case

$$r \le \frac{280.62|\sum e^{-\pi d^{1/2}/2a_i 2683}|}{d^{1/4}|A|}\,.$$

If $a_2 \ge 23$, then

$$\frac{1}{|A|} < 1.8\,, \qquad \left|\frac{A'}{A}\right| < 2.76\,, \qquad \left|\sum\right| < 3.001\,.$$

If $a_2 < 23$, and $a_3 \ge 2470$, then

$$\frac{1}{|A|} < 3.961\,, \qquad \left|\frac{A'}{A}\right| < 4.22\,, \qquad \left|\sum\right| < 2.002\,.$$

It follows that if $d > 1.5 \times 10^{14}$, $r \le .64$, $\varepsilon(r) \le .7$, and from (35) we conclude that there are no d such that $h(-d) = 4$ in the interval $29 \le \log d \le 33$.

Case 2. We choose $k = 2683$ again, and assume $(k, d) = 1$, and $d \ge e^{33}$. We now have $r \le .582$, and $\varepsilon(r) \le .63$. Hence there are no d such that $h(-d) = 4$ in the interval $28 \le \log d \le 33.9$.

Continuing this process, we assume that $d \ge e^{33.9}$. It follows that $\varepsilon(r) \le .49$. Hence there are no d such that $h(-d) = 4$ in the interval $26 \le \log d \le 35.7$.

If $d \ge e^{35.7}$, then $\varepsilon(r) \le .31$. Hence there are no d such that $h(-d) = 4$ in the interval $24 \le \log d \le 38$.

If $d > e^{38}$, then $\varepsilon(r) \le .17$, and we conclude that there are no d such that $h(-d) = 4$ in the interval $22 \le \log d \le 39.8$.

Finally, if $d \ge e^{39.8}$, then $\varepsilon(r) \le .17$, and we conclude that there are no d such that $h(-d) = 4$ in the interval $21 \le \log d \le 40.5$.

We have now proven the following proposition:

Proposition 1. *If the set* $\{a_i\}$ *is large*, $1.5 \times 10^{14} \le d \le e^{40.5}$, *and* $h(-d) = 4$, *then* 2683 *divides* d.

Case 3. Assume $d > e^{40.5}$.

If $(17923, d) = 1$, then $\varepsilon(r) < .13$, and there are no d such that $h(-d) = 4$ in the interval $32 \le \log d \le 200$.

If $(28963, d) = 1$, then $\varepsilon(r) \le .19$, and there are no d such that $h(-d) = 4$ in the interval $36 \le \log d \le 196$.

If $(37427, d) = 1$, then $\varepsilon(r) \le .12$, and there are no d such that $h(-d) = 4$ in the interval $38 \le \log d \le 331$.

We record the results of case 3 in the following proposition:

Proposition 2. *If the set* $\{a_i\}$ *is large*, *and* $e^{40.5} \le d \le 10^{196}$, *then* $h(-d) > 4$.

At this point our error terms are all small, and there is no difficulty in continuing along the lines of the previous cases via computer. We arrive at

Proposition 3. *If the set* $\{a_i\}$ *is large*, *and* $10^{196} \le d \le 10^{2800}$, *then* $h(-d) > 4$.

Proposition 4. *If* $(5077, d) > 1$ *and* $e^{2700} \le d \le e^{100\,000}$, *then* $h(-d) > 4$.

Comment. The assumptions in Proposition 4 imply that the set $\{a_i\}$ is large. Further, since $(5077, d) > 1$, we only need to find two k's relatively prime to each other and to 5077 for each gap between 2700 and 100000. (In the previous cases we needed three such k's.)

6. "Bad" sets. If our discriminant corresponds to a "bad" set, the previous methods will fail. Fortunately, we can show that for sufficiently large d of class number 4, there are no "bad" sets.

Lemma 7 (Gauss). *If* $a > 0$, $a \le d^{1/2}/2$, $a \mid d$, *and* a *is squarefree*, *then there is exactly one reduced form of discriminant* $-d$ *with minimum* a.

The proof of Gauss' lemma can be found in [10].

Proposition 5. *The set of "bad" sets for discriminants* $d > 1.5 \times 10^{14}$ *and class number* 4 *is empty.*

Proof. Choose $a \ne 1$, and let $p \mid a$. Since $b^2 - 4ac = -d$, $\left(\frac{-d}{p}\right) = 0$, or 1. As $a < 2470$ (since we have assumed it is a bad set), and $d > 1.5 \times 10^{14}$, we see from Lemma 8 of Section 7 that $\left(\frac{-d}{p}\right) = 0$, so that $p \mid d$. By Lemma 7 there is a unique form with minimum a. If there is another prime q dividing any $a_i < 2470$, then our 4 minima must be 1, p, q, and pq. If there is no such q, then either $a_3 \geq 2470$, and our set is "large", or $a_3 = p^m$ for some $m \in \mathbb{Z}$. For a fundamental discriminant this is impossible.

Comment. As mentioned above, Sections 4, 5, and 6 form a single unit which together show that no medium sized discriminant can have class number 4. It is remarkable that these methods are so complementary.

7. Discriminants less than 10^{14}.

The basic strategy we will use to handle the case of small discriminants is given by

LEMMA 8. *If* $\chi(p) = 1$, *then* $p > (d/4)^{1/h}$.

Proof. Since $\chi(p) = 1$, the prime p splits in $\mathbb{Q}(\sqrt{-d})$, $p = P_1P_2$, with $P_1 \neq P_2$. Thus $P_1^h = \langle a \rangle$, where $\langle a \rangle$ is a principal ideal, and $a \notin \mathbb{Z}$. It follows that $p^h = N(P_1^h) = N(\langle a \rangle) > d/4$.

To help clarify things we will assume that $10^{12} \leq d \leq 10^{14}$. Our method then proceeds as follows. By Lemma 8, if $h(-d) = 4$, then $\chi(p) = -1$, or 0 for all primes in the range $3 \leq p \leq 700$. We split the primes in this range into two sets:

$$A = \{p \mid 3 \leq p \leq 41\} \quad \text{and} \quad B = \{p \mid 43 \leq p \leq 700\}\,.$$

Notice that $k = \prod_{p \in A} p > 1.5 \times 10^{14}$. Using the Chinese remainder theorem we can construct all numbers $n < k$ for which $\left(\frac{-n}{p}\right) = -1$ or 0 for all $p \in A$. The number of numbers constructed in this way is

$$k_1 = \prod_{p \in A} \left(\frac{p-1}{2} + 1\right).$$

Since k_1 is much smaller than k, we have some hope that a machine can check these numbers one-by-one.

Needless to say, one needs a fast check even for k_1 numbers. This is the purpose of the set B. For each n that we construct, we check $\left(\frac{-n}{p}\right)$ for $p \in B$ to see whether it satisfies the above mentioned conditions. This, as will be explained below, can be expected to eliminate most numbers. Those that remain can then be checked directly.

Some justification for this approach lies in the conjecture of Vinogradov that the least prime quadratic residue to the modulus q is $O(q^{\varepsilon})$ for all $\varepsilon > 0$. Under the assumption of the extended Riemann hypothesis Ankeny achieved the bound $O(\log^2 q)$, and his proof suggests that the correct bound is $O(\log q)$. If this is the case, then it is reasonable to expect very few numbers to reach the end of our sieve.

A detailed description of the code and the various checks that were used to insure its accuracy are not included in this paper for obvious reasons.

We mention, however, one check that was particularly useful. If n was constructed correctly, $\left(\frac{-n}{p}\right) \neq 1$ for any prime $p \in A$. By running n through a sieve of the first 20 primes in the set B, we produce numbers with an unusual quadratic behavior. A separate program was written to determine the values of the Legendre symbol for the n we developed in this way. The first four n we tested were:

$$46255062048195\,, \quad 135723858044775\,,$$
$$73689407691900\,, \quad 9399159144375\,.$$

By means of this method we proved

Theorem 5. *Let $k = \mathbb{Q}(\sqrt{-n})$. If n is squarefree, and $10^4 \le n \le 1.5 \times 10^{14}$, then the class number of k is greater than* 4.

Theorem 6. *Let $k = \mathbb{Q}(\sqrt{-n})$. If n is squarefree, $(n, 2683) > 1$, and $10^{14} \le n \le 10^{18}$, then the class number of k is greater than* 4.

Theorem 7. *Let $k = \mathbb{Q}(\sqrt{-n})$ and $-d$ the discriminant of k. If n is squarefree, $n \le 10^4$, and $h(-d) = 4$, then n is one of the following numbers*:

$$14, 17, 21, 30, 33, 34, 39, 42, 46, 55, 57, 70, 73, 78, 82, 85, 93, 97, 102, 130, 133\,,$$
$$142, 155, 177, 190, 193, 195, 203, 219, 253, 259, 291, 323, 355, 435, 483, 555\,,$$
$$595, 627, 667, 715, 723, 763, 795, 955, 1003, 1027, 1227, 1243, 1387\,,$$
$$1411, 1435, 1507, 1555\,.$$

Comment. The fact that no exceptional fields were discovered is not surprising. Several authors [6, 14] have already searched up through 10^6 without finding an exception, and it is well known that a large exception would contradict the generalized Riemann hypothesis [12].

8. Conclusion.

We can now solve the problem of unique representation as a sum of three squares. Indeed, from our work in sections three through seven, we know that the list of fields presented in Theorem 7 is the complete list of imaginary quadratic fields with class number 4. We then derive (as in [4])

Theorem 8. *For $n \not\equiv 0 \pmod 4$, $P_3(n) = 1$ if and only if n is one of the following numbers*:

$$1, 2, 3, 5, 6, 10, 11, 13, 14, 21, 22, 30, 35, 37, 42, 43, 46, 58, 67, 70\,,$$
$$78, 91, 93, 115, 133, 142, 163, 190, 235, 253, 403, 427\,.$$

Table 1

n	γ	$\lvert\zeta(2s_n)\rvert$
1	14.134725	1.9488
2	21.022040	.8310
3	25.010858	.5342
4	30.424876	.5148
5	32.935062	.8130
6	37.586178	.9383
7	40.918719	1.9220
8	43.327073	.9778
9	48.005151	.5426
10	49.773832	1.4281
11	52.970321	.6885

Table 2

k	γ
163	0.202901
427	0.249925
2683	0.156679
17923	0.030986
28963	0.033774
30895	0.018494
37427	0.019505
115147	0.003158
123204	0.010650
139011	0.012930
145412	0.017312
151419	0.021347
188995	0.026513

Note. These tables are taken from the papers of Stark [18], and Montgomery and Weinberger [15]. Details pertaining to the methods of calculation can be found there.

References

[1] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) 55 (1952), 65–72.

[2] A. Baker, *A remark on the class number of quadratic fields*, Bull. London Math. Soc. 1 (1966), 98–102.

[3] —, *Imaginary quadratic fields of class number* 2, Ann. of Math. 94 (1971), 139–152.

[4] P. T. Bateman and E. Grosswald, *Positive integers expressible as a sum of* 3 *squares in essentially only one way*, J. Number Theory 19 (1984), 301–308.

[5] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York 1966.

[6] D. A. Buell, *Small class numbers and extreme values of L-functions of quadratic fields*, Math. Comp. 31 (1977), 786–796.

[7] P. Chowla and A. Selberg, *On Epstein's zeta function*, J. Reine Angew. Math. 227 (1967), 86–110.

[8] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Graduate Texts in Math. 74, Springer, New York 1980.

[9] C. B. Haselgrove and J. C. P. Miller, *Tables of the Riemann Zeta Function*, Royal Society Math. Tables, Vol. 6, Cambridge 1960.

[10] H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. 25 (1934), 150–160.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, Yale Univ. Press, 1966.

[12] D. M. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa (4) 3 (1976), 623–663.

[13] B. Gross et D. Zagier, *Points de Heegner et derivées de fonctions L*, C. R. Acad. Sci. Paris 297 (1983), 85–87.

[14] D. H. Lehmer, E. Lehmer, and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. 24 (1970), 433–451.

[15] H. L. Montgomery and P. J. Weinberger, *Notes on small class numbers*, Acta Arith. 24 (1974), 529–542.

[16] L. J. Mordell, *On the rational solutions of the indeterminate equations of the* 3*rd and* 4*rth degrees*, Proc. Cambridge Philos. Soc. 21 (1922), 179–192.

[17] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Sém. Bourbaki, 1983–1984, exp. 631.

[18] H. M. Stark, *A complete determination of the complex quadratic fields of class number* 1, Michigan Math. J. 14 (1967), 1–27.

[19] —, *On complex quadratic fields with class number two*, Math. Comp. 29 (1975), 289–302.

[20] —, *L-functions and character sums for quadratic forms (II)*, Acta Arith. 15 (1969), 307–317.

[21] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford Univ. Press, London 1951.

THE SUPERCOMPUTING RESEARCH CENTER
17100 SCIENCE DRIVE
BOWIE, MARYLAND 20715
U.S.A.

Received on 17.8.1990
and in revised form on 26.3.1991 (2076)