A Numerical Study of the Relative Class Numbers of Real Quadratic Integral Domains

By Harvey Cohn

1. Introduction. In a classic paper in 1856 Dirichlet gave some applications of a formula for the ratio of the class number of a quadratic integral domain in a real field to the class number of the whole integral domain (of all quadratic integers in that field), with the principal objective of showing that this ratio takes many values (such as 1) infinitely often for the real case, in support of a conjecture of Gauss.

The object of this paper is first of all to give Dirichlet's results briefly, together with some theorems and illustrations immediately deducible from them (in order to restrict the computation to cases in which the theory is of more help). We shall, of course, offer various tables of relative class numbers, such data being our main object. We emphasize quadratic integral domains of *prime power* conductor under the whole integral domain (of all quadratic integers of the field).

We ask, in particular, when the relative class number is divisible by 2 and 4, and find simple linear congruence conditions. When we ask which prime conductors have relative class numbers divisible by 3, we find such primes are essentially the splitting primes of certain cubic fields and therefore representable by quadratic forms, according to the classic work of Dedekind [3]. This is basically an application of class-field theory and perhaps the tables emerging would be of some experimental use. The classic background is amplified in [7], [5], and [2].

Here it might be appropriate to remark that the tables given below have a "natural" limit of diminishing returns owing to the fact that the relevant portions of classical algebraic number theory were developed long ago with relatively little data, and it would be desirable to see the theory profit from more data before great feats of computer endurance are attempted.

2. Notation and Terminology. We follow the convention that Latin letters generally denote rational integers and Greek letters denote algebraic integers. The following symbols and terms appear throughout the work:

m is a square-free integer > 1.

$R(m^{1/2})$ is the *field* generated by $m^{1/2}$.

d is the *discriminant* of the field generated by $m^{1/2}$; $d = m$ if $m \equiv 1 \pmod 4$, $d = 4m$ if $m \not\equiv 1 \pmod 4$.

c is the indicator of the type of field, $c = 2$ if $m \equiv 1 \pmod 4$, $c = 1$ if $m \not\equiv 1 \pmod 4$. Thus $d = 4m/c^2$.

$\mathfrak{O}$ is the set of all algebraic integers of $R(m^{1/2})$. It consists of $\omega = (x + ym^{1/2})/c$ for which x and y are rational integers subject only to the condition $x \equiv y \pmod c$.

Received August 18, 1961. This research was supported in part by a National Science Foundation grant. Computer service on GEORGE was donated by the Argonne National Laboratories of the U. S. Atomic Energy Commission through the cooperation of Dr. William F. Miller, Director of the Applied Mathematics Division.

$F(\omega)$ is the function defined by $y = F(\omega)$ in the above definition.

$\mathfrak{O}_f$ is an arbitrary integral domain (ring with unity) in $R(m^{1/2})$, given uniquely for any integer $f > 0$. It consists of the subset of algebraic integers ω in $\mathfrak{O}$ for which $f \mid F(\omega)$. Here f is called the *conductor*. It is the index of $\mathfrak{O}_f$ in $\mathfrak{O}$, and $\mathfrak{O}_1 = \mathfrak{O}$.

f^2d is the *ring-discriminant* of $\mathfrak{O}_f$. Its purpose is that any given $D(>1)$ which is $\equiv 0$ or $1 \pmod 4$ can be written uniquely as f^2d for some f and d. Thus f^2d completely determines $R(m^{1/2})$ and $\mathfrak{O}_f$ in $R(m^{1/2})$.

$h(f^2d)$ is the class number (of ideals prime to f) in $\mathfrak{O}_f$.

$H(f)$ is the relative class number $= h(f^2d)/h(d)$, (used when the value of d, or the field, is understood in context).

ϵ is the fundamental unit, written $\epsilon = (a + bm^{1/2})/c$. Here $a > 0$, $b > 0$ and $a \equiv b \pmod c$.

e is the norm of the fundamental unit, actually ± 1, $N(\epsilon) = e = (a^2 - mb^2)/c^2$.

$\psi(f)$ is the value of $f\Pi(1 - (d/q)/q)$ extended over primes q which divide f. Here (d/q) is the Kronecker residue symbol, (thus $(d/2) = (2/d)$).

$\phi(f)$ is the minimum exponent t (>1) for which $\epsilon^t \varepsilon \mathfrak{O}_f$ or for which $f \mid F(\epsilon^t)$. It can be shown directly that $\phi(f) \mid \psi(f)$. By classical methods of primitive root theory, if $f \mid F(\epsilon^u)$, then $\phi(f) \mid u$.

Other symbols appear only locally and can best be defined as they arise.

3. Dirichlet's Theorems. The starting point is the following theorem, in principle due to Gauss: *For a given field* $R(m^{1/2})$, (*with* $m > 0$),

$$H(f) = \psi(f)/\phi(f). \tag{3.1}$$

If $m < 0$, the formula is modified so that, for instance, with $f > 1$, $\phi(f)$ is replaced by half the number of units in $\mathfrak{O}$. (We do not need the modified formula for the machine part of the calculation, but for supporting computations in Section 7).

Now $\psi(f)$ is fairly easy to find, but the calculation of $\phi(f)$ is the part requiring the electronic computer. Dirichlet [4] showed, however, that if $f = p_1^{F_1} \cdots p_s^{F_s}$, where the primes p_i come from a given finite set, then the values of $H(f)$ also come from a finite set as the exponents F_i vary; in fact $H(f) = H_0$, a constant if each F_i is sufficiently large. An examination of Dirichlet's method leads to the rule that if p_i is odd and f_0 is such that $H(f_0) = H(f_0p_i)$ (while if one $p_i = 2$, f_0 satisfies $H(f_0) = H(4f_0)$), then $H(f) = H(f_0)$ if $f_0 \mid f$, (recalling the prime divisors of f are to be limited to the p_i).

From general principles it also follows that if $f \mid g$, then $H(f) \mid H(g)$.

The main step in understanding these results is to consider any f which contains all the odd primes p_i (and possibly 2^2) as divisors. Then $f \mid F(\epsilon^{\phi(f)})$, i.e., $\epsilon^{\phi(f)} = (x_f + y_fm^{1/2})/c$, where $f \mid y_f$. But, let f^* be the factor of y_f consisting of powers of the p_i. (Thus $f \mid f^*$ while $(y_f/f^*, f) = 1$.) Then for p_i odd, $F(\epsilon^{\phi(f)p_i}) = p_if^*g$, where $(g, f) = 1$, as we prove by using the binomial theorem, (in a manner reminiscent of the proof that a primitive root modulo p^2 is a primitive root modulo p^n, $n > 2$). For p_i even, special attention must be given the denominator $c = 2$, but this can be left to the reader, as well as the completion of the proof of the above results by induction.

If we restrict f to powers of a prime p then we find $H(p^{n+1}) = H(p^n)$ or $pH(p^n)$ $(n \geqq 1)$, but eventually $H(p^{n+1}) = H(p^n)$ then $H(p^m) = H(p^n)$ for all $m \geqq n$ when p is odd, while for $p = 2$, $H(2^{n+1}) = H(2^n)$ or $2H(2^n)$, $(n \geqq 1)$, but eventually $H(2^{n+2}) = H(2^n)$ where $H(2^m) = H(2^n)$ for all $n \geqq m$.

4. Simple Cases. We first consider those q which divide $6\,mb$. In these cases the values of $H(q^t)$ are easily seen by elementary hand calculations, and we often omit these from the tables to make room for more interesting values.

$\mathbf{f = 2^F}$

$$\text{Define } M(a,b,f) = \begin{cases} 1 & \text{if} \quad f = 1, \\ \min\,(2^B, f) & \text{if} \quad 2^A = 1, \qquad f \geqq 2, \\ \min\,(2^A, f/2) & \text{if} \quad 2^A > 1, \qquad f \geqq 2, \end{cases}$$

where $2^A \parallel a$, i.e., $2^A \mid a$ but $2^{A+1} \nmid a$, and likewise $2^B \parallel b$. Then if $d \equiv 0 \pmod 4$,

$$H(f) = M(a, b, f), \tag{4.1}$$

while if $d \equiv 1 \pmod 4$ and $2 \mid ab$,

$$H(f) = [2 + (d/2)]M(a/2, b/2, f/2), \tag{4.2}$$

and if $d \equiv 1 \pmod 4$ and $2 \nmid ab$ (whence $d \equiv 5 \pmod 8$),

$$H(f) = M([a^2 - 3e]/2, [a^2 - e]/2, f/2). \tag{4.3}$$

(Note that $([a + bm^{1/2}]/2)^3 = a[a^2 - 3e]/2 + b[a^2 - e]m^{1/2}/2)$.

$\mathbf{f = 3^F}$

Let $3^B \parallel b$, $3^A \parallel a$. If $3 \mid m$, let $3^G \parallel 3a^2 + mb^2$, then

$$H(f) = \begin{cases} \frac{1}{3}\min\,(f, 3^G) & \text{if} \quad 3^B = 1 \\ \min\,(f, 3^B) & \text{if} \quad 3^B > 1. \end{cases} \tag{4.4}$$

If, however, $3 \nmid m$, let $3^T \parallel a^2 + b^2m$, then

$$H(f) = \begin{cases} \frac{1}{3}\min\,(f, 3^T) & \text{if} \quad 3 \nmid ab, \\ \frac{1}{2}[1 - (d/3)/3]\min\,(f, 3^A) & \text{if} \quad 3 \mid a, \\ [1 - (d/3)/3]\min\,(f, 3^B) & \text{if} \quad 3 \mid b. \end{cases} \tag{4.5}$$

(Note that $f = 3^F$ is "special" because of consideration of 3^G. Compare $f = q^F$ below).

$\mathbf{f = q^F}$

Here let q be a prime $\neq 2, 3$ for which $q \mid mb$, and let $q^B \parallel b$. Then

$$H(f) = \min\,(f, q^B). \tag{4.6}$$

Thus in many cases where $q \mid m$ and $q \nmid 6b$, then $H(q^n) = 1$ for all n, giving the easiest illustration of Dirichlet's original objective; e.g., for $m = d = 5$, $H(5^n) = 1$ for all $n > 0$.

5. The Program. The basic sub-routine considers the input

$$m, a, b, f \tag{5.1}$$

from which $\phi(f)$, $\psi(f)$, and $H(f)$ are calculated. The machine forms by induction $\epsilon^t = [a(t) + b(t)m^{1/2}]/c$ stored as $a(t)$, $b(t)$ calculated modulo f^2. Then letting $t = 1, 2$, the machine records the earliest $t[= \phi(f)]$ for which $b(t) \equiv 0 \pmod f$. The machine next calculates $\psi(f)$ by examining the prime factors q of f sequentially. The machine finds (d/q) for $q \nmid 2d$ by actually testing the solvability in x of $x^2 \equiv d \pmod q$, while for $q \mid 2d$, (d/q) is determined directly from the rules. Finally, $H(f) = \psi(f)/\phi(f)$. The output for each input consists of

$$f, H(f), \psi(f), b(\phi(f))/f \pmod f. \tag{5.2}$$

The last value is desired for purposes of testing $F(\epsilon^{\phi(f)})$. For example, if

$$(b(\phi(f))/f, f) = 1,$$

then f is a suitable f_0 for Section 3.

The basic sub-routine was used in several ways.

In one run the basic sub-routine was set up to increment f by 1 automatically over a range $f_1 \leqq f \leqq f_2$ where f_1 and f_2 are given in addition to the initial data. For $m = 5$ the problem was run up to $f = 4400$ and for $m = 2$ and 3, it was run up to $f = 1000$.

In another variation, the values of f were incremented as before but were restricted to *primes* in the preassigned range. (We always use the letter p to denote a prime.) These main runs were made for $f = p$ an odd prime up to 997 for 38 values of m, namely

$$\text{Series A: } 2 \leqq \text{square free } m \not\equiv 1 \pmod 4 \leqq 42 \tag{5.2}$$

$$\text{Series B: } 5 \leqq \text{square free } m \equiv 1 \pmod 4 \leqq 97. \tag{5.3}$$

The problem was programmed for the GEORGE computer with only approximately 500 words of a 4096-word high-speed memory involved. The machine is internally binary with 40-bit word length and approximate speed of 50,000 two-address operations per second.

In all the runs, the output consisted of the input data (5.1) (as a heading) followed by the output data (5.2) listed "on-line" (parallel) with the computation. The input and output were in decimal (internally converted) and on paper tape originally (but the output was later transformed to magnetic tape just to speed up the printing process from flexowriter to line printer). The actual input and output times were negligible.

The running time for each case was about $f/50$ seconds. The calculations were run between December 1960 and May 1961.

6. Use of Some Cyclic Groups. Let m be given and let $p \nmid 2m$ be an arbitrary given prime. Define a group in which the elements $\mathfrak{a}_t$ are the following sets:

$$\mathfrak{a}_t = \{x + ym^{1/2}\}, \quad \text{where} \quad x \equiv ty \quad \text{and} \quad N(x + ym^{1/2}) \not\equiv 0 \pmod p, \tag{6.1}$$

and

(6.2) $\mathfrak{a}_\infty = \{x\}$, where $x \neq 0$.

The group operation is multiplication (mod p), easily shown to be independent of the representative. When $(m/p) = -1$, there are $p + 1$ of these elements, while when $(m/p) = +1$ there are $p - 1$ of these elements (by excluding two values of t for which $t^2 \equiv m \pmod{p}$). In general, we have a group $\mathfrak{A}_p$ with $p - (m/p) = \psi(p)$ elements, and with $\mathfrak{a}_\infty$ as the unit element.

We see that the group $\mathfrak{A}_p$ is cyclic. This is true where $(m/p) = -1$ since the group is a sub-group of the cyclic group of reduced residues of algebraic integers modulo p, (now an ideal prime). When $(m/p) = -1$ we rewrite $\mathfrak{a}_t = \mathfrak{a}[u]$ where

$$(6.3) \qquad \mathfrak{a}[u] = \{x(r(1 + u) + m^{1/2}(1 - u))\}.$$

Here r satisfies $r^2 \equiv m \pmod{p}$ and t and u are related by $t \equiv r(1 + u)/(1 - u)$ (mod p). We can verify $\mathfrak{a}[u]\mathfrak{a}[v] = \mathfrak{a}[uv]$, hence when $(m/p) = 1$, $\mathfrak{A}_p$ is isomorphic to the multiplicative (cyclic) residue group of rational integers modulo p.

The important result for us is the following: if $p \nmid 2m$ and if r is a given integer dividing $p - (m/p)$ a necessary and sufficient condition that $r \mid H(p)$ is that $c\epsilon$ belong to an $\mathfrak{a}_t$ which is an r-th power in $\mathfrak{A}_p$. This result follows from the cyclic structure of $\mathfrak{A}_p$ once we note that $(c\epsilon)^{\phi(p)} \equiv z \pmod{p}$ for z an integer, hence $(c\epsilon)^{\phi(p)}$ belongs to $\mathfrak{a}_\infty$ the unit element, while $\psi(p)$ is the order of the group.

For illustration, we start with $r = 2$, and take $p \nmid 2mb$. Set

$$a + bm^{1/2} = (x + ym^{1/2})k, \quad \text{or,}$$

$$(6.4) \qquad \begin{cases} a \equiv k(x^2 + y^2m) \\ b \equiv 2kxy. \end{cases}$$

This system is solvable, for $k \neq 0$, if and only if the equation

$$(6.5) \qquad bx^2 - 2axy + bmy^2 \equiv 0 \bmod p$$

is solvable, with $(x, y) \neq (0, 0)$. The discriminant is $4c^2e$. Hence if $N(\epsilon) = e = -1$, then $2 \mid H(p)$, for $p \nmid 2mb$.

Thus for some cases, e.g., where $N(\epsilon) = +1$, the only possible f for which $H(f) = 1$ must come from primes in the special cases in Section 4 above. (We recall that if $f \mid g$, then $H(f) \mid H(g)$). Thus for $m = 3$, the only f for which $H(f) = 1$ are now seen to be $f = 3^t$ and $f = 2 \cdot 3^t$.

We next consider the sub-group of $\mathfrak{A}_p$, called $\mathfrak{B}_p$, all of whose elements have norms which are quadratic residues of p. Thus $\mathfrak{a}_\infty$ is necessarily in $\mathfrak{B}_p$, while $\mathfrak{a}_t$ is in $\mathfrak{B}_p$ if and only if $([t^2 - m]/p) = +1$. It is easily seen that the norms of representatives in $\mathfrak{a}_t$ are not all residues, by results on successions of residues and non-residues. Thus $\mathfrak{B}_p$ has only order $(p - (m/p))/2$, since it must then be of index 2. Now if we normalize the representative of $\mathfrak{a}_t$ in (6.1) belonging to $\mathfrak{B}_p$ to be plus or minus an element of norm 1, we can say that if $e = 1$, then ϵ represents a perfect square in $\mathfrak{B}_p$ if and only if for some integers x and y

$$(6.6) \qquad \pm c^2\epsilon \equiv (x + ym^{1/2})^2 \pmod{p}.$$

But the condition for a perfect square in $\mathfrak{B}_p$ is precisely the condition that $\pm\epsilon$ represents a perfect fourth power in $\mathfrak{A}_p$, or $4 \mid H(p)$. Expanding (6.6), we discover we must be able to solve simultaneously

$$\text{(6.7)}\qquad \begin{cases} \pm ca \equiv x^2 + my^2 \\ \pm cb \equiv 2xy \end{cases} \pmod p.$$

An elementary calculation reveals this system is solvable if and only if (with signs $s_1, s_2 = \pm 1$),

$$\text{(6.8)}\qquad \begin{cases} x^2 + my^2 \equiv s_1 ca \\ x^2 - my^2 \equiv s_2 c \end{cases} \pmod p.$$

For this it is necessary and sufficient that $2c(s_1 a + s_2)$ and $2mc(s_1 a - s_2)$ be perfect squares modulo p. With some manipulation, we find, *if* $N(\epsilon) = e = +1$ *and* $p \nmid 2mb$, *then a necessary and sufficient condition that* $4 \mid H(p)$ *is that*

$$\text{(6.9)}\qquad (-1/p) = (m/p) = ([2a/c - 2]/p).$$

We can often simplify the result (6.9) to take the form

$$\text{(6.10)}\qquad (-S/p) = (Q/p) = (R/p),$$

for smaller values of Q and R shown in the columns 10 and 11 of Table I with $S = 1$, except for $m = 15$ and 35, where $S = 2$. When $e = -1$, there are still many occurrences of $H(p) = 4$ (the smallest such value is listed in column 11).

7. Divisibility by 3. A more interesting case is $r = 3$. This can occur (for $p \nmid 6mb$) only when $3 \mid \psi(p)$ or $(-3m/p) = 1$. We ask, when can we solve $c\epsilon \equiv k(x + ym^{1/2})^3 \pmod p$ or

$$\text{(7.1)}\qquad \begin{cases} a \equiv k[x^3 + 3xy^2m] \\ b \equiv k[3x^2y + y^3m] \end{cases} \pmod p,$$

for $xy \not\equiv 0$? Eliminating k, we see this leads to the solvability of $\lambda(x/y) \equiv 0 \bmod p$ where λ is a polynomial defining a root of a cubic field,

$$\text{(7.2)}\qquad \lambda(\xi) = b\xi^3 - 3a\xi^2 + 3b\xi m - am = 0.$$

Hence $3 \mid H(p)$ (for $p \nmid 6m$) if and only if p is a splitting prime for the field $R(\xi)$. In fact, *p must split into three distinct prime ideals* since $(-3m/p) = 1$, and the discriminant D_3 of the cubic can be shown to differ from $-3m$ by a rational square. The reader is referred to Hasse's work [6] for details on the method.

Finding the field discriminant of $R(\xi)$ is rather lengthy but since the methods are so well-known we can merely outline the steps. The module $[1, b\xi, am/\xi]$ consists only of integers of $R(\xi)$ and its discriminant is $-108mc^4$ by a direct calculation. Since only perfect squares could be superfluous factors of the discriminant, we need examine the basis elements to see if $r + sb\xi + tam/\xi$ can be divisible by 2 (or 3) without r, s, and t being simultaneously divisible by 2 (or 3). We find the *only* possibilities are the following cases which we leave for the reader to verify:

Case i. $3 \mid m$ and $3 \mid b$; then $3 \mid b\xi$ and $3 \mid (am/\xi)$
Case ii. $3 \nmid m$ and $9 \mid a$ (or b); then $3 \mid b\xi$ (or $3 \mid (am/\xi)$)
Case iii. $3 \nmid mab$ and $am \equiv \pm b \pmod 9$; then $3 \mid (b\xi + e_1e_2am/\xi - e_2)$

where $e_1 = \pm 1 \equiv am$, $e_2 = \pm 1 \equiv b \pmod 3$

Case iv. $c = 2$; then $2 \mid b\xi$, $4 \mid (b\xi + am/\xi)$.

These calculations were made partly on the basis of possible ideal factorizations of (2) and (3) and partly as a direct consequence of the following equation for $\mu = (b\xi + am/\xi)e$:

$$\begin{aligned}\mu^3 - 3b(1-m)\mu^2 + 3(b^2-a^2)(1-m)\mu \\ + [a^3(6m+2) + a^2b(m^2-12m+3) \\ - ab^2(2m+6m^2) + b^3(9m^2-1)] = 0.\end{aligned} \tag{7.3}$$

The occurrences of cases (i–iii) are noted in column 7 of Table I.

We finally obtain

$$d_3f_3^2 = D_3 = -108m/s^2c^2, \tag{7.4}$$

where

$$\begin{cases} s = 9 & \text{if } 3 \mid m, 3 \mid b, \\ s = 3 & \text{if } 3 \nmid m, 9 \mid ab, \quad \text{or if } \quad 3 \nmid mab, am \equiv \pm b \pmod 9, \\ s = 1 & \text{otherwise.} \end{cases} \tag{7.5}$$

We then consider the set of $h(d_3f_3^2)$ primitive reduced quadratic forms of discriminant D_3. Those which are perfect cubes under composition represent precisely all primes $p(\nmid 6m)$ for which $3 \mid H(p)$.

A supporting computation was made by Mr. Roy Lippmann on an IBM 650 to calculate all primitive reduced forms from D_3. The square-free kernel m_3 is shown in Table I, together with $h(D_3)$ and the conductor f_3. The $h(D_3)$ primitive forms (A, B, C) which are cubes under composition were most easily identified by finding some "convenient" small prime $(p \nmid 6m)$ represented by the form and checking $H(p)$, (see [1]). The coefficients A and B of forms and representative primes p and $H(p)$ are listed in Table III.

Now in every case, it so happens that $3 \parallel h(d_3f_3^2)$, hence there are $h(d_3f_3^2)/3$ forms which are perfect cubes. Also, the ambiguous forms are always perfect cubes, but in general they are not the complete set. The non-ambiguous forms, naturally, are written two at a time by means of $\pm B$.

8. Irregular Primes. We finally note that there are many odd primes p, for which, for some fixed $i > 0$,

$$H(p^n) = H(p) \min(p^{n-1}, p^i). \tag{8.1}$$

We call these primes irregular and we call i the *index of irregularity*. When $p \nmid 6mb$ such cases are explained by some combinational curiosities much less transparent than those occurring in Section 3. They are listed because the occurrence of prime divisors of f in the relative class number is of some theoretical value.

These values were found by scanning the outputs (5.2) as f ran over the odd primes p for cases where $b \equiv 0 \pmod p$. The 53 individual cases which emerged were tested by rerunning these cases, using $f = p^2$. The values of $b/f \not\equiv 0 \pmod f$ indicated primes of index 1, while those where $b/f \equiv 0$ while $b/fp \not\equiv 0 \pmod f$ indicated primes p of index 2. No odd primes of higher index emerged from the experiment.

9. Summary of Calculations. The problem ran some 40 hours and generated some 300 pages of tables, obviously too much to reproduce! We therefore attempt a qualitative résume.

From the output, we would readily believe that when $e = -1$ there are infinitely many odd primes for which $H(p) = 1$, while when $e = 1$ there are infinely many primes for which $H(p) = 2$. Indeed, even in the case $e = 1$, we know (from Section 4) that if $p \mid m$ and $p \nmid 6b$ then $H(p) = 1$. In either case, except for scattered irregular primes in Table IV, $H(p) = H(p^n)$.

A frequency count is surprising in its uniformity. When $e = -1$, we examine the 167 odd primes < 1000 and find $H(p) = 1$ in 39–43 per cent of these primes as m varies, while when $e = +1$ the corresponding case $H(p) = 2$ occurs for 56–63 per cent of these primes as m varies. If we define $P(m, n; x)$ as the proportion of primes $\leqq x$ for which $H(p) = n$ (in reference to $R(m^{1/2})$) we find a reasonably steady value for $P(5, 1; x)$. For instance, $P(5, 1; 500) = 42$ per cent, $P(5, 1; 1000) = 41$ per cent, $P(5, 1; 2000) = 39$ per cent, $P(5, 1; 4000) = 37$ per cent.

Continuing with $m = 5$, $H(p)$ (as far as we might imagine) "should" take all prime values but it seems to take large values "rather slowly." The earliest p for some larger primes are $H(911) = 13$, $H(1087) = 17$, $H(3079) = 19$, $H(1103) = 23$. For $p < 4400$, $H(p)$ takes no larger prime! Thus an "asymptotic" study of the values of $H(p)$ can be expected to be astronomical in size (perhaps larger than for studies of classical prime number distributions).

Table II is given to point out some relative class numbers which are small prime powers, $H(p) = 3$ is in Table III, and $H(p) = 2$ or 4 comes from columns 10 and 11 of Table I. Despite the uniformity of the earlier frequency count, some values of m seem to be more "amenable" to given values of $H(p)$ than others. This seeming paradox might again be a manifestation of the fact that "$p < 1000$" is a miniscule range of values!

As far as *congruence* properties of $H(p)$ are concerned, Sections 6 and 7 provide us with much more guidance. For example, by the uniform density of primes in linear congruence classes for a fixed modulus, when $e = -1$, $H(p) \equiv 0 \pmod 4$ only one-third as often as $H(p) \not\equiv 0 \pmod 4$.

In a similar manner, using known results on the distribution of primes represented by quadratic forms [8], we can see that if k_3 of the $h(D_3)$ forms are perfect cubes, then $k_3/2h(D_3)$ is the proportion of primes for which $H(p) \equiv 0 \pmod 3$, at least by "Dirichlet density." Actual frequency counts show the proportion to be reassuringly close to $1/6$; (with $k_3 = h(D_3)/3$ in the cases treated here).

The congruence properties $H(p) \equiv 0 \pmod 5$, however, provide too few instances in the range $p < 1000$, to make a frequency count meaningful.

The conditions on p which make $H(p) \equiv 0 \pmod 4$ when $e = -1$, are more provocative. The percentage of such $p(<1000)$ varies from 4 per cent (when $m = 37$) to 12 per cent (when $m = 89$). There seems to be no simple explanation (e.g., in terms of linear or quadratic forms). As a matter of curiosity, when $m = 5$, $H(p) \equiv 0 \pmod 4$ for

$$p = 61, 89, 109, 149, 269, 389, 401, 521, 661, 701, 761, 769, 809, 821, 829;$$

when $m = 37$, this holds for

$$p = 53, 101, 181, 293, 349, 397, 593;$$

Table I

Summary of Calculation

Columns 1–5 are explained in Section 2, Columns 6–9 in Section 7, Columns 10–11 in Section 6.

1	2	3	4	5	6	7	8	9	10	11†
m	a	b	e	$h(d)$	m_3	f_3	$h(d_3)$	$h(d_3f_3^2)$	Q	R or p_4
(Series A: $m \not\equiv 1 \pmod 4$, $c = 1$, $d = 4m$, $d_3 = 4m_3$.)										
2	1	1	−1	1	−6	3	2	6	···	41
3	2	1	+1	1	−1	9	1	6	2	3
6	5	2	+1	1	−2	9	1	6	2	−3
7	8	3	+1	1	−21	3	4	12	−2	7
10	3	1	−1	2	−30	3	4	12	···	157
11	10	3	+1	1	−44	3	4	12	2	11
14	15	4	+1	1	−56	3	4	12	−2	7
15	4	1	+1	2	−5	9	2	12	3*	−5*
19	170	39	+1	1	−57	3	4	24	2	19
22	197	42	+1	1	−66	3	8	24	2	−11
23	24	5	+1	1	−69	3	8	24	−2	23
26	5	1	−1	2	−78	3	4	12	···	37
30	11	2	+1	2	−10	9	2	24	5	−6
31	1,520	273	+1	1	−93	3	4	12	−2	31
34	35	6	+1	2	−102	3	4	12	−2	17
35	6	1	+1	2	−105	3	8	24	5*	−7*
38	37	6	+1	1	−114	3	8	24	2	−19
39	25	4	+1	2	−13	9	2	24	3	−13
42	13	2	+1	2	−14	9	4	24	6	−7
(Series B: $m \equiv 1 \pmod 4$, $c = 2$, $d = m$, $d_3 = m_3$.)										
5	1	1	−1	1	−15	3	2	6	···	61
13	3	1	−1	1	−39	3	4	12	···	29
17	8	2	−1	1	−51	3	2	6	···	13
21	5	1	+1	1	−7	9	1	12	3	−7
29	5	1	−1	1	−87	1 (iii)	6	6	···	13
33	46	8	+1	1	−11	9	1	6	−3	11
37	12	2	−1	1	−111	3	8	24	···	53
41	64	10	−1	1	−123	3	2	6	···	5
53	7	1	−1	1	−159	3	10	30	···	17
57	302	40	+1	1	−19	9	1	12	3	−19
61	39	5	−1	1	−183	3	8	24	···	59
65	16	2	−1	2	−195	3	4	12	···	29
69	25	3	+1	1	−23	1 (i)	3	3	−3	23
73	2,136	250	−1	1	−219	3	4	12	···	37
77	9	1	+1	1	−231	1 (ii)	12	12	7	−11
85	9	1	−1	2	−255	1 (ii)	12	12	···	101
89	1,000	106	−1	1	−267	3	2	6	···	73
93	29	3	+1	1	−31	1	3	3	3	−31
97	11,208	1,138	−1	1	−291	3 (i)	4	12	···	53

* Here $S = 2$. (See Section 6).

† When $e = -1$, Column 11 has the earliest prime p_4 for which $H(p_4) = 4$. (See Section 6).

Table II

Some Special Values of p for Which $n \mid H(p)$

The table gives the minimum odd prime $p(<1000)$ for which $H(p) = n$, (or $H(p) = 2n$, if n is odd and $e = N(\epsilon) = +1$). If no such p occurs, the table lists p_r the earliest prime (<1000) for which $H(p)/n$ (or $H(p)/2n$) gives the minimum quotient r.

m	$n = 8$	16	32	9	27	5	25	7	11
				Series A					
2	137	353	...	269_2	...	79	...	643	199
3*	313	193	...	181	...	71	...	...	...
6*	409	97	...	89	971_2	311	...	743	109
7*	71	751	127	179	271	131	...	197	617_4
10	241	449	...	271	...	19	...	419	131
11*	97	881	449	719	...	409	199	421	...
14*	71	79	...	251	...	29	...	97	...
15*	31	...	...	163	487	61	...	71	...
19*	73	...	...	991	269	31	...	13	397
22*	353	401	641	883	593	271	701	127	131_2
23*	41	47	...	521	...	59	...	631	...
26	641	881	...	...	...	139	...	337_2	...
30*	23	383	...	739	...	439	349	211	...
31*	7	193	...	883_7	...	19	449	13	...
34*	23	911_3	...	163	...	59	...	83	433_4
35*	47	449	223	71	...	89	...	701	...
38*	137	769	...	37	701	431	...	127	...
39*	673	79	...	827	...	151	...	911	857
42*	103	673_7	...	809	431	491	...	433	...
				Series B					
5	89	...	...	919	...	211	...	307	967
13	233	...	...	827	...	59	...	211	109
17	281	...	...	127	...	79	...	...	...
21*	199	337	...	...	...	101	...	433	263
29	233	673	...	971	...	619	...	601_2	461_6
33*	71	47	...	433_2	379	139	...	239	331
37	...	...	...	73_2	...	71	...	167	...
41	769_2	769	...	307	...	199	...	491	593_2
53	929_2	929	449	433_4	...	379	...	113_2	659
57*	487	127	...	197	...	271	...	43	...
61	937	977	...	271	487	59	...	463	...
65	601	...	353	467	431	211	...	...	43
69*	71	239	...	307	...	79	...	97	...
73	857	...	...	107	...	379	...	333_2	67
77*	127	113	...	...	...	101	...	71	...
85	...	...	...	71	...	331	...	139	947
89	809	641	929	631	...	59	...	503	967
93*	463	79	...	379	811_3	251	...	29	947
97	113_2	113	673	107	...	151	...	463	...

(* Denotes values of m for which $N(\epsilon) = 1$).

Table III

Quadratic Forms Which are Perfect Cubes

These are the forms (A, B, C) of discriminant $B^2 - 4AC = d_3 f_3^2$ which represent those primes $p(\nmid 6m)$ for which $3 \mid H(p)$, where p is "conveniently" small.

m	$d_3 f_3^2$	A	B	p	$H(p)$	A	B	p	$H(p)$
				Series A					
2	−216	1	0	79	3	2	0	29	6
3	−324	1	0	97	12	2	2	41	6
6	−648	1	0	163	6	2	0	83	12
7	−756	1	0	193	12	7	0	139	6
		2	2	107	6	14	14	17	6
10	−1080	1	0	271	9	2	0	137	6
		5	0	59	3	10	0	37	12
11	−1188	1	0	313	24	11	0	71	6
		2	2	149	6	19	16	19	6
14	−1512	1	0	379	42	2	0	191	24
		7	0	61	6	14	0	41	6
15	−1620	1	0	409	12	5	0	101	6
		2	2	227	12	10	10	43	6
19	−2052	1	0	577	36	19	0	103	6
		2	2	257	6	23	8	23	6
22	−2376	1	0	619	6	2	0	347	12
		11	0	227	12	22	0	331	6
		7	±2	7	6	14	±12	47	6
23	−2484	1	0	877	6	23	0	131	6
		2	2	311	24	25	4	349	6
		5	±4	5	6	10	±6	67	6
26	−2808	1	0	727	3	2	0	353	6
		13	0	67	3	26	0	53	6
30	−3240	1	0	811	30	2	0	503	12
		5	0	167	12	10	0	241	60
		11	±4	11	6	22	±4	37	6
31	−3348	1	0	853	6	27	0	139	6
		2	2	419	30	29	4	29	6
34	−3672	1	0	919	6	2	0	461	6
		17	0	71	24	27	0	61	6
35	−3780	1	0	1009	12	5	0	269	6
		7	0	163	6	27	0	167	12
		2	2	557	6	31	8	31	6
		10	10	97	6	14	14	71	18
38	−4104	1	0	1051	6	2	0	521	6
		19	0	73	24	27	0	179	36
		23	±6	23	6	31	±22	31	6
39	−4212	1	0	1069	12	13	0	337	..
		2	2	587	6	26	26	47	6
		17	±2	17	6	31	±2	31	6
42	−4536	1	0	1303	6	2	0	569	6
		7	0	337	84	14	0	137	6
		13	±12	13	6	26	±12	59	12

TABLE III—*Continued*

m	$d_3f_3^2$	A	B	p	$H(p)$	A	B	p	$H(p)$
				Series B					
5	-135	1	1	139	3	5	5	47	3
13	-351	1	1	367	3	10	10	79	3
		8	±1	11	3	. .	. . .	. . .	. .
17	-459	1	1	127	9	11	5	11	3
21	-567	1	1	571	6	7	7	109	12
		8	±3	23	6	. .	. . .	. . .	. .
29	-87	1	1	103	3	3	3	41	6
33	-891	1	1	223	6	11	11	23	12
37	-999	1	1	1063	3	16	5	619	3
		2	±1	131	3	4	±3	73	18
		8	±5	89	6	. .	. . .	. . .	. .
41	-1107	1	1	277	12	17	7	71	3
53	-1431	1	1	1447	3	20	13	239	3
		7	±5	7	3	18	±15	23	3
		10	±3	43	3	8	±3	83	3
57	-1539	1	1	397	36	19	19	139	6
		5	±1	5	6	. .	. . .	. . .	. .
61	-1647	1	1	1663	3	22	17	271	9
		18	±3	23	3	8	±7	53	6
		13	±11	13	6	. .	. . .	. . .	. .
65	-1755	1	1	439	3	23	19	23	3
		5	5	89	18	13	13	37	6
69	-23	1	1	101	6	. .	. . .	. . .	. .
73	-1971	1	1	499	3	25	23	79	3
		5	±3	5	6	. .	. . .	. . .	. .
77	-231	1	1	331	6	3	3	89	18
		8	5	233	6	7	7	61	6
85	-255	1	1	271	15	8	1	83	21
		3	3	97	12	5	5	131	3
89	-2403	1	1	601	12	27	27	83	3
93	-31	1	1	47	6	. .	. . .	. . .	. .
97	-2619	1	1	661	12	27	27	31	3
		23	±7	23	3	. .	. . .	. . .	. .

and when $m = 89$, this holds for

$$p = 53, 73, 109, 157, 233, 257, 269, 449, 461, 509, 601, 613, 641, 733, 757, 809, 821, 929, 937, 977.$$

Curiously enough, when $m = 37$ all $p(<1000)$ for which $H(p) \equiv 0 \pmod 4$ satisfy $H(p) = 4$; from Table II, this value of m seems most "resistant to variety" in the values of $H(p)$.

TABLE IV

Irregular (Odd) Primes < 1000

For values of m in Table I. Primes of index 2 are marked with (*), unmarked primes are of index 1. (See Section 8.)

m	p	$H(p)$	m	p	$H(p)$
	Series A			Series B	
2	13	2	13	241	2
2	31	1	29	3*	1
3	103	2	29	11	1
6	3	1	33	3	1
6	7	2	33	29	2
10	191	5	33	37	4
10	643	1	37	7	1
15	3	1	37	89	6
15	181	2	37	257	6
19	79	2	41	29*	2
22	43	4	41	53	2
22	73	2	53	5	2
23	7	2	57	59	2
23	733	2	69	5	2
31	157	2	69	17*	2
34	37	2	73	5*	6
34	547	26	73	7	1
35	23	2	73	41	2
38	5	2	85	3	1
39	5	2	89	5*	2
39	7	2	89	7	1
39	37	2	89	13	2
42	3*	1	89	59	5
42	5	2	93	13	2
42	43	2	97	17	2
42	71	2			

It is our hope that additional motivation might be suggested by these data before the next electronic tour de force is attempted.

Department of Mathematics
University of Arizona
Tucson, Arizona, and

Applied Mathematics Division
Argonne National Laboratory
Argonne, Illinois

1. H. COHN, "A numerical study of Dedekind's cubic class number formula," *J. Res. Nat. Bur. Standards*, v. 59, 1957, p. 265-271. (A similar composition problem is treated on a computer here.)

2. E. C. Dade, O. Taussky, & H. Zassenhaus, "On the semi-group of ideal classes in an order of an algebraic number field," *Bull. Amer. Math. Soc.*, v. 67, 1961, p. 305–308. (The ideals which divide *f*, normally excluded from class number considerations, are treated theoretically and with the aid of computers.)

3. R. Dedekind, "Über die Anzahl der Idealklassen in reinen kübischer Zahlkörpern," *J. Reine Angew. Math.*, v. 121, 1900, p. 40–123.

4. P. G. L. Dirichlet, "Une propriete des formes quadratiques a determinant positive," *J. Math. Pures Appl.* Ser II, v. 1, 1856, p. 76–79.

5. R. Fueter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, v. 1, II Leipzig-Berlin, 1924. (This work gives the classic application of relative class structures concisely.)

6. H. Hasse, "Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage," *Math Z.* v. 31, 1929, p. 565–582. (Reference centers primarily on the top line of the table on p. 568.)

7. H. Weber, *Lehrbuch der Algebra*, v. II, III, Braunschweig, 1894, 1908.

8. H. Weber, "Beweiss des Satzes dass jede eigentliche primitive quadratische Form unendlich viele Primzahlen darstellen fähig ist," *Math. Ann*, v. 20, 1882, p. 301–329.