Journal of Research of the National Bureau of Standards Vol. 59, No. 4, October 1957 Research Paper 2798

A Numerical Study of Dedekind's Cubic Class Number Formula

Harvey Cohn [1]

In this paper an analytic formula of Dedekind is used to compute class numbers for a sample of pure cubic fields, employing the National Bureau of Standards electronic computer, the SEAC. The computation is one of major magnitude, and it illustrates the usefulness of combining integral and decimal arithmetic. The class numbers obtained are of much greater magnitude than those of pure cubic fields previously studied by means of hand computer methods.

1. Introduction

The discovery of fields with high class numbers [2] has become an end in itself [10].[3] There are generally two possible procedures: One is the *algebraic* method, consisting, operationally, of a certain sorting of values of polynomials according to factors; the second is the *analytic* method, based on zeta-function residues. The second method is of special interest when applicable, because of the scarcity of types of field for which a usable formula emerges.

In 1900, Dedekind applied both methods to the "pure" cubic field, or the field formed by adjoining $M^{1/3}$ to the rationals [4]. The largest class number h that Dedekind achieved was $h=9$ for $M=91$. In 1950, Cassels published a table of class numbers [1] with the larger $h=12$ for $M=43$, using the algebraic method. To achieve a substantially larger h it is necessary to take larger values of M. Furthermore, Dedekind's analytic formula is the simpler method to program for a machine for certain special M, namely, those that equal $(s^3+1)/c^3$ for s and c integers. A sample of 21 cases were run, yielding six class numbers h between 18 and 27, as well as other smaller ones (including the cases cited above).

As an incidental result the quadratic fields (whose relation to the pure cubic field is similar to the relation of rational numbers to the quadratic field) are studied in some numerical detail.

The computation uses a mixture of integral and decimal arithmetic like the earlier work with Gorn [3], but, here, more fortunately, round-off provides no difficulty, even far beyond the range covered. The work was begun about July 1956 and the runs were completed November 1956.

2. Dedekind's Formula

The first algebraic investigations of class number were made by Markoff [8], but the first explicit "closed" formula for class number was derived by Dedekind. The entire numerical study undertaken here stems from his formula, which we give without proof (in an equivalent form):

$$\epsilon^h=\frac{\Pi \mathrm{H}(\omega_N)^{1/6}}{\Pi \mathrm{H}(\omega_R)^{1/6}}. \tag{2.1}$$

Here h is the much desired class number of the real field $R(M^{1/3})$, and $\epsilon(>1)$ is the (often elusive) fundamental unit, which is discussed later. The function $\mathrm{H}(z)$ is defined for z a positive imaginary quantity ($\mathrm{Im}z>0$), as the (positive) function

$$\mathrm{H}(z)=\eta(z)\eta(-\bar{z})[i(\bar{z}-z)]^{1/2}, \tag{2.2}$$

where $\eta(z)$ is the (analytic) Dedekind eta-function [6].

$$\eta(z)=\exp(\pi iz/12)\prod_{n=1}^{\infty}(1-\exp 2\pi izn), \tag{2.3}$$

and $\bar{z}$ denotes the complex conjugate of z. The symbols ω_N, ω_R, are rather complicated and are treated in the next section, but more immediately relevant to the cubic field itself is the following fact: If M is decomposed by positive a, b, c, so that

$$M=ab^2c^3, \tag{2.4}$$

(so that a and b are free of quadratic factors), then $R(M^{1/3})$ is generated equally well by $(ab^2)^{1/3}$ or $(a^2b)^{1/3}$. Hence the number pair (a,b) of relatively prime integers (not both 1) uniquely determines a field $K_{a,b}=R(M^{1/3})$. For this field the conductor k is defined as

$$\left.\begin{aligned} k&=ab \qquad a^2-b^2\equiv 0 \pmod 9\\ k&=3ab \qquad a^2-b^2\not\equiv 0 \pmod 9.\end{aligned}\right\} \tag{2.5}$$

As a final definition,

$$D=-3k^2 \tag{2.6}$$

is called the discriminant. Its significance lies in the fact that the algebraic integers, in particular the fundamental unit ϵ, together with the algebraic conjugates ϵ', $\bar{\epsilon}'$ (the complex conjugates) satisfy

$$D\leq|(\epsilon-\epsilon')(\epsilon'-\bar{\epsilon}')(\epsilon-\bar{\epsilon}')|^2. \tag{2.7}$$

[1] Present address, Department of Mathematics, Washington University, St. Louis, Mo.

[2] A general background in algebraic number theory, including quadratic forms is assumed (see [7]).

[3] Figures in brackets indicate the literature references at the end of this paper.

3. Quadratic Field

Associated with the cubic field in question is the quadratic field generated by adjoining to the rationals the imaginary cube root of unity ρ given by (say) the positive imaginary root of

$$\rho^2+\rho+1=0. \tag{3.1}$$

For this the norm function N is defined by

$$N(p+q\rho)=(p+q\rho)(p+q\rho^2)=p^2-pq+q^2. \tag{3.2}$$

We finally associate with the field $K_{a,b}$ and its conductor k the triples of integers $\{A, B, C\}$, such that

$$AC=k \tag{3.3}$$

$$1\leqq B<A \tag{3.4}$$

$$(A,N(B+C\rho))=1. \tag{3.5}$$

For every such triple of integers we construct the quadratic form

$$Q(x,y)=N[Ax+(B+C\rho)y] \tag{3.6}$$

and consider any prime p, not dividing $3k^2$, represented by $Q(x,y)$ for integral x and y. Then $\{A,B,C\}$ is called a *residue* (or *nonresidue*) triple or $Q(x,y)$ is called a *residue* (or *nonresidue*) form according to whether or not the equation

$$x^3\equiv a^2b \pmod p \tag{3.7}$$

is solvable for an integer x. Then for each triple satisfying eq (3.3), (3.4), or (3.5) a form $Q(x,y)$ is defined with "root"

$$\omega=\frac{B+C\rho}{A}. \tag{3.8}$$

The root ω is an ω_R or an ω_N according as the residue or nonresidue character of the form. The product symbol in eq (2.1) should then be self-explanatory. It can be shown there are $3k''$ triples $\{A,B,C\}$ that generate an ω_R and $6k''$ that generate an ω_N (not all of the ω_R or ω_N being distinct), where $9k''$, the total number of triples, is given by

$$9k''=k\prod_{p|k}(1-(-3/p)/p). \tag{3.9}$$

Here $(-3/p)$ is the usual quadratic residue symbol,

$$(-3/p)=\begin{cases} 1 \text{ for } p\equiv 1 \pmod 3 \\ -1 \text{ for } p\equiv -1 \pmod 3 \\ 0 \text{ for } p\equiv 0 \pmod 3. \end{cases} \tag{3.10}$$

The properties of the quadratic form $Q(x,y)$ will eventually come into play. It might suffice for the time being to mention that the function $\mathrm{H}(\omega)$, according to a well-known property of the Dedekind eta-function, is invariant under a unimodular change of variables; thus a unimodular integral change of variables of $Q(x,y)$ will not affect $\mathrm{H}(\omega)$; neither will the change $\omega'=-\overline{\omega}$. Thus let $Q(x,y)$ be equivalent to the reduced form

$$Q^*(X,Y)=RX^2+SXY+TY^2. \tag{3.11}$$

Its root may be written

$$\omega^*=\frac{-S+ik\cdot 3^{1/2}}{R},$$

so that

$$0\leqq S/2<R\leqq(-D/3)^{1/2}=k \tag{3.12}$$

because, for all $9k''$ forms corresponding to conductor k,

$$D=-4RT+S^2=-3k^2. \tag{3.13}$$

We are now guaranteed by eq (3.12) a much more favorable scaling for the computation of $\mathrm{H}(\omega)$. Thus

$$\left.\begin{aligned}\log \mathrm{H}(\omega)&=-\pi k3^{1/2}/(12R)+\sum_{n=1}^{\infty}\log(1-2\kappa^n\cos Sn/R+\kappa^{2n})\\ \kappa&=\exp(-\pi k3^{1/2}/R),\end{aligned}\right\} \tag{3.14}$$

and $\kappa\leqq\exp(-\pi 3^{1/2})$, so that to the degree of round-off used here, it will develop that no more than five terms of the infinite sum (or product) are necessary, when the reduced form is used for $Q(x,y)$.

4. Units and Choice of Field

We henceforth confine ourselves to fields generated by $M^{1/3}$, where, for a positive or negative integer s,

$$M=s^3+1. \tag{4.1}$$

The advantage is that a very obvious unit is

$$\eta=|-s+M^{1/3}|^{-1}=|s^2+sM^{1/3}+M^{2/3}|, \tag{4.2}$$

where $M^{1/3}$ refers to the real root. A fundamental unit is clearly of the type $\eta^{1/m}$, and the value of m can be ascertained in the sample treated here, by means of well-known results of Dedekind supplemented by the lemma (compare [9]):

LEMMA. In the notation of (2.5), if $k>10s$, then

$$\epsilon=\eta \text{ or } \eta^{1/2}. \tag{4.3}$$

PROOF. Let $\epsilon=\eta^{1/m}$ be the fundamental unit. Then ϵ, as an algebraic number, has a (root) discriminant not less than the discriminant D of $K_{a,b}$. Hence

$$D\leqq|\epsilon-\epsilon'|^2|\epsilon-\overline{\epsilon}'|^2|\epsilon'-\overline{\epsilon}'|^2,$$

where ϵ', $\bar{\epsilon}'$ are the complex conjugate roots belonging to the same equation as ϵ. But $|\epsilon'|=|\bar{\epsilon}'|=\epsilon^{-1/2}$, thus

$$D \leqq (\epsilon+\epsilon^{-1/2})^4(2\epsilon^{-1/2})^2 \leqq 4\epsilon^3(1+\epsilon^{-3/2})^4. \qquad (4.4)$$

But finally, $D=3k^2$, $\epsilon=\eta^{1/m}$, whereas η is approximately $3s^2$ from eq (4.2). Hence

$$3k^2 \leq 4(3s^2)^{3/m}(1+\eta^{-3/2m})^4(\eta/3s^2)^{3/m}. \qquad (4.5)$$

Taking the maximum on the right when $m \geqq 3$, we see that the corresponding factors in parentheses are as follows:

$$3k^2 \leqq 4(3s^2)\cdot 2^4(1+2^{1/3}+2^{2/3})/3, \qquad (4.6)$$

(the last factor being the one where $m=3$, $s=1$), the inequality (4.6) is contradicted when $k>10s$. Q.E.D.

The list of 21 cases is given in table 1 in order of increasing k. Those cases in which the fundamental unit was known to Dedekind or Cassels are denoted [4] by a "D" or "C", respectively. In the other cases, easily, $k>10s$. The possibility that $\eta=\epsilon^2$ is *excluded* by the fact that in these cases the class number, calculated by assuming $\eta=\epsilon$, will turn out to be *odd*.

5. Subroutines

The following number-theoretic subroutines were programed for this computation: One should bear in mind that the SEAC is a binary machine with a 44 bit word and sign bit. The numbers treated range arithmetically from $-4+2^{-42}$ to $4-2^{-42}$, i. e., the decimal point is fixed between the second and third high-order bit. Integers are held in the low end of the register (or scaled by 2^{-42}).

1. *Division of two integers* to produce integral quotient and integral remainder. (The built-in division operation produced only a "decimal" quotient.)

2. *The Euclidean algorithm*, or solution in X, Y of

$$sX+tY=(s,t). \qquad (5.1)$$

3. *Reduction of modules.*[5]

4. *Multiplication of modules.*[5]

5. *Generation of coefficients of* $Q(x,y)$ (from $\{A,B,C\}$ of eq (3.6)).

6. *Transformation of coefficients of* $Q(x,y)$ *under unimodular change of variables.*

7. *Reduction of* $Q(x,y)$ *to the properly or improperly equivalent reduced form* $Q^*(x,y)$ *subject to conditions* (3.12). To do this we first find the minimum value of $Q(x,y)$ by scanning all of the finite set of points for which $Q(x,y)<Q(1,0)=A^2$, or for which

$$[Ax+(B+C/2)y]^2+3C^2y^2/4<A^2. \qquad (5.2)$$

If the minimum value is $Q(x_0,y_0)=R$, then the Euclidean algorithm generates an integral unimodular transformation of coordinates, (or finds a_{12},a_{22}), so that $a_{22}x_0-a_{12}y_0=1$. Thus in the new coordinates,

$$\left.\begin{aligned} x_0X'+a_{12}Y'&=x \\ y_0X'+a_{22}Y'&=y \end{aligned}\right\} \qquad (5.3)$$

$Q(x,y)$ becomes

$$Q(X,Y)=RX'^2+S'X'Y'+T'Y'^2. \qquad (5.4)$$

Now to minimize the coefficient of $X'Y'$, all we need do is perform the transformation

$$\left.\begin{aligned} X'&=X+gY \\ Y'&=Y, \end{aligned}\right\} \qquad (5.5)$$

choosing $g=-[S'/2R]$, (the integral part), and we obtain $Q^*(X,Y)$ of eq (3.11) and (3.12).

8. *Determination of the residue character of a quadratic form.* This subroutine finds a small [6] prime p represented by $Q^*(X,Y)$ and not dividing D. (The procedure is similar to the search for the minimum of $Q(x,y)$ by eq (5.2).) Then the eq (3.7) is tested with $+x$ and $-x$, where x runs from 1 to $(p-1)/2$. If x passes through all these values without eq (3.7) being satisfied, then, and only then, Q is a nonresidue form.

9. *The built-in "base zero" operations.* These are standard fixed-point subroutines for input conversion to binary form and output conversion to decimal form, for logarithms, exponentials, sines, and cosines, among others.

6. First Run. Class Numbers

The subroutines listed earlier, taken together with the formulas and concomitant explanations, should indicate the basic program for computing h. It must be added that (binary) nonintegral quantities used, e. g., in logarithmic computations were scaled by 2^{-14}, and the final decimal values for $h \log_{10} \epsilon$ were expressed to six decimal places.

The basic procedure is to generate the $9k''$ triples $\{A,B,C\}$ in lexicographic order. For each triple we compute the corresponding forms Q and (reduced) Q^*, and finally we form (and accumulate) the contributions (3.14), resulting in the following data (in decimal form):

Input: "Case number", a, b, k, D

Output: For a nonresidue form, eq (3.11),

$$R,S$$

[4] See headnote to table 1.

[5] See section 7.

[6] No effort was made to secure the smallest p, although this seems to have happened accidentally in the few cases spot checked. The smallest prime would have required much more programing, although the effect might have proved rewarding.

For a residue form, eq (3.7), (3.11),

$$x,p,R,S$$

Final output,

$$h \log \epsilon,\ h \log_{10} \epsilon.$$

For simplicity, R and S, which are never negative, were packed into one word, likewise x (with sign removed) and p. To identify a residue form, the x, p combination was printed first, with a minus sign. The residue and nonresidue forms are omitted from the final tabulation to save space. The division $h=h \log_{10}\epsilon/\log_{10}\epsilon$ was performed by hand, resulting in integral h to five significant figures (see table 1). The data from tables of Dedekind and Cassels are denoted by "D" and "C", respectively.

During the actual runs, the program was read in on wire, and the parameters were read in on teletype tape in trios of "case number", a, b. (Here the case number was packed with identifying information to check the tape position.) The output was on teletype printer.

The program exhausted almost 900 of the 1,024 electrostatic memory spaces.

The running time varied from 3 minutes for case I to 14 hours for case XXI. A subroutine permitted the current $\{A,B,C\}$ and cumulative sum of $\pm\log$ $H(\omega)$ to be dumped every half hour or so for rerun purposes. Almost no time went into input-output, by comparison. The vast bulk of the time went toward the testing of the residue characters, i. e., toward the solution or nonsolution of eq (3.7). The problem was brought to a close at case XXI largely because time was beginning to become prohibitive.

The SEAC has no overflow stops at all, not even for 0/0, and no automatic error checks. As a substitute for both, a test was made to see if the discriminant of each quadratic form checks with $-3k^2$. In the range covered, no overflow would have occurred, barring machine errors.

7. Group Structure of Modules

A good deal of insight into the machinery of Dedekind's formula is gained by considering the composition structure of the group of quadratic forms in the "order" of discriminant $-3k^2$. Once again, rather than summarize a well-known and lengthy theory, we shall consider the modules only in relation to the present computation.

The notation

$$\mathfrak{M}=[A_1+B_1\rho, \ldots, A_t+B_t\rho] \tag{7.1}$$

denotes the aggregate of integers in $R(\rho)$

$$\xi=\Sigma n_i(A_i+B_i\rho),$$

where n_i are integers. Such a set is called a *module*. Every module has a *reduced basis* like $[A,\ B+C\rho]$ identified with the triple $\{A,B,C\}$ of section 3. Here *A is taken as the minimum positive rational integer in $\mathfrak{M}$*, and $B+C\rho$ is defined by the conditions that C is the *minimum positive coefficient of ρ, whereas B is the minimum positive integer in a module element in which the coefficient of ρ is C.* The enumeration of triples $\{A,B,C\}$ enumerates modules, of course, whereas $Q(x,y)$ is the norm of an arbitrary element of the module. Clearly

TABLE 1

"D" and "C" denote units or class numbers appearing in Dedekind's and Cassel's works, respectively.

Case	s	$\|M\|$	a	b	c	$\log_{10}\eta$	ϵ		k	k''	$h \log_{10}\epsilon$	h		Generator	D
I	1	2	2	1	1	0. 585159	η	D	6	1	0. 585159	1	D	$2^{1/3}$	−108
II	2	9	1	3	1	1. 096455	η	D	9	1	1. 096455	1	D	$3^{1/3}$	−243
III	3	28	7	2	1	1. 436650	$\eta^{1/2}$	D	14	2	2. 154975	3	D	$28^{1/3}$	−588
IV	−18	5831	17	1	7	2. 987641	η	D	17	2	2. 987641	1	D	$17^{1/3}$	−867
V	8	513	19	1	3	2. 283584	$\eta^{1/2}$	D	19	2	3. 425376	3	D	$19^{1/3}$	−1083
VI	−2	7	7	1	1	1. 060137	η	D	21	2	3. 180412	3	D	$7^{1/3}$	−1323
VII	−3	26	26	1	1	1. 425922	η	D	26	4	4. 277770	3	C	$26^{1/3}$	−2028
VIII	19	6860	5	2	7	3. 034650	$\eta^{1/2}$	D	30	6	4. 551974	3	D	$20^{1/3}$	−2700
IX	−10	999	37	1	3	2. 476964	η	D	37	4	7. 430929	3	C	$37^{1/3}$	−4107
X	−4	63	7	3	1	1. 678966	η	D	63	6	10. 073793	6	D	$63^{1/3}$	−11907
XI	−9	728	91	1	2	2. 385408	η		91	8	21. 468668	9	D	$91^{1/3}$	−24843
XII	23	12168	1	39	2	3. 200589	η	D	117	12	19. 203533	6	C	$39^{1/3}$	−41067
XIII	5	126	14	3	1	1. 876216	η		126	18	16. 885942	9		$126^{1/3}$	−47628
XIV	7	344	43	1	2	2. 167739	η	D	129	14	26. 012867	12	C	$43^{1/3}$	−49923
XV	−5	124	31	2	1	1. 873900	η		186	30	16. 865096	9		$124^{1/3}$	−103788
XVI	4	65	65	1	1	1. 683490	η	D	195	24	30. 302812	18		$65^{1/3}$	−114075
XVII	−6	215	215	1	1	2. 032753	η		215	28	42. 687799	21		$215^{1/3}$	−138675
XVIII	6	217	217	1	1	2. 034093	η		217	20	54. 920504	27		$217^{1/3}$	−141267
XIX	−7	342	38	3	1	2. 166895	η		342	54	58. 506160	27		$342^{1/3}$	−350892
XX	15	3376	422	1	2	2. 829347	η		422	70	59. 416280	21		$422^{1/3}$	−534252
XXI	17	4914	182	1	3	2. 938049	η		546	72	79. 327311	27		$182^{1/3}$	−894348

$$\rho\mathfrak{M}=\rho[A,\ B+C\rho]=[\rho A,\ -C+(B-C)\rho]$$

is another module leading to the same $Q(x,y)$, as $N(\rho)=1$, so is $\rho^2\mathfrak{M}$. Thus the triples $\{A,B,C\}$ or the reduced modules $[A,\ B+C\rho]$, with $AC=k$, come in "threes," leading to the same form $Q(x,y)$.

Dedekind considered the multiplicative group formed by the modules under multiplication of basis elements:

$$[A,\ B_1+C_1\rho][A_2,\ B_2+C_2\rho]=$$
$$[A_1A_2,\ A_1B_2+A_1C_2\rho,\ A_2B_1+A_2C_1\rho,\ (B_1B_2-C_1C_2)+$$
$$(B_1C_2+B_2C_1-C_1C_2)\rho]. \quad (7.2)$$

It can be shown that the product module can be reduced to the form $[A_3,\ B_3+C_3\rho]$ where $A_3C_3=k$, (provided $A_1C_1=A_2C_2=k$). This process is closely analogous to the composition of forms, or, of course the multiplication of ideals.

For the purpose of performing this multiplication of modules we need two subroutines mentioned earlier (numbers 3 and 4 of section 5).

3. *Reduction of modules*, (from $[A_1,\ B_1+C_1\rho,\ B_2+C_2\rho]$ to the reduced form $[A,\ B+C\rho]$).

4. *Multiplication of modules.* This is the repeated application of the earlier subroutine for the reduction of product (7.2) to $[A,\ B+C\rho]$.

The notation "residue" (or "nonresidue") module can now be introduced to correspond to "residue" (or "nonresidue") form. Dedekind has shown that the set of residue modules forms a subgroup of index three among the set of all modules. Thus the nonresidue modules can be partitioned into co-sets so that all modules are of type

$$\mathfrak{R},\ \mathfrak{R}\mathfrak{N}_1,\ \mathfrak{R}\mathfrak{N}_1^2,$$

where $\mathfrak{R}$ is a *variable* residue and $\mathfrak{N}_1$ is a fixed nonresidue module. In the notation $\mathrm{H}(\mathfrak{M})$ for $\mathrm{H}(B+C\rho/A)$, we can write in accordance with (2.1)

$$\epsilon^h=\frac{\Pi\mathrm{H}(\mathfrak{R}\mathfrak{N}_1)}{\Pi\mathrm{H}(\mathfrak{R})}. \quad (7.3)$$

Now if we take precautions that once $\mathfrak{R}$ appears, $\rho\mathfrak{R}$ and $\rho_2\mathfrak{R}$ shall *not* appear, we have only k'' factors in numerator or denominator.

Now (7.3) is very close to Dedekind's original formula. (Dedekind used quadratic forms and not modules to generate the products in (7.3).)

8. Ambiguous Forms and Modules

To appreciate the relation between modules and forms we must realize that not only do $\mathfrak{M}$, $\rho\mathfrak{M}$, $\rho^2\mathfrak{M}$ correspond to the same form but $\mathfrak{M}$ and $\overline{\mathfrak{M}}$ can correspond to the same form. Here $\mathfrak{M}$, the conjugate module is defined by

$$\left.\begin{aligned}\mathfrak{M}&=[A,\ B+C\rho]\\ \mathfrak{M}&=[A,\ B+C\rho^2].\end{aligned}\right\} \quad (8.1)$$

The difficulty really arises when $\mathfrak{M}=\overline{\mathfrak{M}}$, (or $\rho\mathfrak{M}=\overline{\mathfrak{M}}$, etc.). (The second possibility is really no different as it implies $\rho^2\mathfrak{M}$ is then its own conjugate.) These are the *ambiguous* forms of classical number theory. Generally $\mathfrak{M}\overline{\mathfrak{M}}=[1,\ k\rho]$ the unit element, or principal ideal so that if $\mathfrak{M}=\overline{\mathfrak{M}}$, $\mathfrak{M}^2$ is a unit element and $\mathfrak{M}$ must belong to any subgroup of index three. In other words the self-conjugate modules are all *residue* modules.

To give an ample illustration let us take case VI, $s=-4$, $k=21$, and list the $9k''=18$ modules in lexicographic order, as does the computing machine, but with the interrelations in question clearly indicated.

LIST OF MODULES FOR $k=21$

$[1,\ 21\rho]=\mathfrak{M}_0$	$[7,\ 5+3\rho]=\mathfrak{M}_3$	$[21,\ 7+\rho]=\rho\mathfrak{M}_1$
$[3,\ 7\rho]=\mathfrak{M}_1$	$[7,\ 6+3\rho]=\overline{\mathfrak{M}}_2$	$[21,\ 9+\rho]=\rho\mathfrak{M}_3$
$[3,\ 1+7\rho]=\overline{\mathfrak{M}}_1$	$[21,\ \rho]=\rho\mathfrak{M}_0$	$[21,\ 13+\rho]=\rho^2\mathfrak{M}_3$
$[7,\ 3\rho]=\rho\overline{\mathfrak{M}}_1$	$[21,\ 1+\rho]=\rho^2\mathfrak{M}_0$	$[21,\ 15+\rho]=\rho^2\overline{\mathfrak{M}}_1$
$[7,\ 3+3\rho]=\rho^2\mathfrak{M}_1$	$[21,\ 4+\rho]=\rho^2\overline{\mathfrak{M}}_2$	$[21,\ 16+\rho]=\rho^2\mathfrak{M}_2$
$[7,\ 4+3\rho]=\mathfrak{M}_2$	$[21,\ 6+\rho]=\rho\overline{\mathfrak{M}}_2$	$[21,\ 18+\rho]=\rho\mathfrak{M}_2$.

These modules form a group with identity element $\mathfrak{M}_0$. Rather than construct the whole group table we might identify $\mathfrak{M}_i,\rho\mathfrak{M}_i,\rho^2\mathfrak{M}_i$ as one element, and it is easy to see that the group reduces to an abelian group of order 6 given by

$$\mathfrak{M}_0,\ \mathfrak{M}_1,\ \mathfrak{M}_3,\ \overline{\mathfrak{M}}_1=\mathfrak{M}_1^2,\ \mathfrak{M}_2=\mathfrak{M}_1\mathfrak{M}_3,\ \overline{\mathfrak{M}}_2=\mathfrak{M}_1^2\mathfrak{M}_3 \quad (8.2)$$

with the generators $\mathfrak{M}_1$, $\mathfrak{M}_3$ satisfying

$$\mathfrak{M}_0=\mathfrak{M}_1^3=\mathfrak{M}_3^2. \quad (8.3)$$

We see $\mathfrak{M}_0$, $\mathfrak{M}_3$ are the residue subgroup, for clearly, $\mathfrak{M}_0=\overline{\mathfrak{M}}_0$, $\mathfrak{M}_3=\overline{\mathfrak{M}}_3$.

The corresponding quadratic forms, (grouped after Dedekind with their "negatives"), are [7]

$$\left.\begin{aligned}\mathfrak{M}_0:&\quad x^2\pm xy+331y^2=Q_0(x,y)\\ \mathfrak{M}_1:&\quad 9x^2\pm 3xy+37y^2=Q_1(x,y)\\ \mathfrak{M}_2:&\quad 13x^2\pm 9xy+27y^2=Q_2(x,y)\\ \mathfrak{M}_3:&\quad 19x^2\pm 11xy+19y^2=Q_3(x,y).\end{aligned}\right\} \quad (8.4)$$

Forms for $\mathfrak{M}_0$ and $\mathfrak{M}_3$ are ambiguous (or self-conjugate). Note that $ab^2=7$, so that for the primes given

$$\begin{cases}331=Q_0(0,1), & 10^3\equiv 7\ (\mathrm{mod}\ 331)\\ 19=Q_3(1,0), & 4^3=7\ (\mathrm{mod}\ 19)\end{cases}$$

[7] The negative of $Q(x,y)$ is found by replacing S by $-S$ or, effectively, by keeping R and D fixed and replacing S by $2R-S$.

TABLE 2

Case	Test value		Form			
			Residue		Nonresidue	
	$\|x\|$	p	R	S	R'	S'
I	4	31	1	0	4	2
II	16	61	1	1	7	3
III	11	151	1	0	4	2
	6	61	3	0	12	18
IV	3	223	1	1	7	13
	11	73	3	3	13	15
V	31	271	1	1	7	3
	26	97	3	3	13	23
VI	10	331	1	1	9	15
	4	19	[a] 19	27	13	17
VII	49	523	1	0	4	6
	17	181	3	0	12	6
	4	19	19	10	21	24
	4	19	19	28	7	10
VIII	14	691	1	0	4	2
	22	127	25	0	13	2
	1	19	19	6	25	20
	1	19	19	32	9	6
	1	7	7	10	25	40
	1	7	7	4	27	36
IX	304	1, 033	1	1	7	11
	104	349	3	3	21	39
	1	19	19	23	31	27
	1	19	19	15	13	25
X	305	3, 019	1	1	9	15
	21	73	49	49	19	33
	9	37	37	9	49	63
	9	37	37	65	43	45
	1	31	31	11	49	7
	1	31	31	51	13	1
XI	747	6, 211	1	1	49	7
	17	139	49	49	49	77
	8	67	67	125	37	13
	11	79	[a] 79	147	43	21
	8	67	67	9	57	3
	454	2, 089	3	3	61	17
	4	31	31	53	19	3
	4	31	31	9	73	59
XII	3,364	10, 267	1	1	9	15
	2	139	81	63	81	9
	2	139	81	99	81	45
	6	193	63	39	7	11
	6	193	63	87	63	3
	15	103	[a] 103	37	49	17
	1	19	19	31	67	65
	3	43	43	27	79	31
	4	31	31	47	73	55
	4	31	31	15	37	59
	3	43	43	59	61	13
	1	19	19	7	97	35

[a] Signifies quadratic form whose negative belongs to a conjugate module.

Case	Test value		Form			
			Residue		Nonresidue	
	$\|x\|$	p	R	S	R'	S'
XIII	352	11, 923	1	0	4	2
	18	331	36	66	36	30
	18	331	36	6	9	6
	71	439	49	0	73	48
	43	163	81	72	79	82
	43	163	81	90	43	82
	2	67	67	70	81	36
	2	67	67	64	49	70
	12	103	103	24	49	84
	12	103	103	182	61	108
	13	109	109	130	37	18
	13	109	109	88	81	18
	4	31	31	22	117	102
	4	31	31	40	97	22
	4	19	19	10	76	10
	11	241	52	54	13	2
	11	241	52	50	52	102
	4	19	19	28	76	66
XV	93	25, 921	1	0	4	6
	87	751	36	66	9	12
	87	751	36	6	36	42
	17	1, 069	27	0	108	54
	109	499	52	2	13	2
	55	997	63	6	103	200
	64	397	76	22	76	98
	56	601	148	206	148	58
	56	601	148	90	37	16
	64	397	76	130	19	16
	55	997	63	120	163	80
	109	499	52	102	52	50
	3	97	97	180	157	254
	12	463	117	102	61	20
	3	151	151	292	43	10
	7	73	73	96	91	50
	163	1, 447	91	76	79	106
	13	211	133	92	109	78
	31	193	171	174	49	22
	23	241	108	18	27	18
	115	937	28	34	7	6
	115	937	28	22	28	50
	23	241	108	98	108	90
	31	193	171	168	133	22
	13	211	133	174	63	78
	163	1, 447	91	106	117	24
	7	73	73	50	139	242
	3	151	151	10	172	162
	12	463	117	132	127	142
	3	97	97	14	67	120
XVI	838	28, 549	1	1	9	3
	253	1, 297	25	25	133	191
	11	211	169	169	61	103
	111	409	169	273	31	37
	111	409	169	65	109	131
	43	157	157	165	25	35
	7	139	139	105	169	143
	7	139	139	173	25	5
	43	157	157	149	127	239
	2	19	19	1	169	299
	2	19	19	37	171	75
	6	151	151	9	169	221
	18	79	79	157	49	61
	18	79	79	1	169	247
	6	151	151	293	175	215
	12	163	163	5	37	25
	2	73	73	103	175	145
	48	463	63	75	63	33
	4	43	43	45	103	7
	342	1, 063	27	27	27	45
	4	43	43	41	133	37
	48	463	63	51	7	9
	2	73	73	43	67	115
	12	163	163	321	97	71

in accordance with eq (3.7). In the "general" situation, of course, the residue modules will not all be ambiguous.

9. Second Run. Residue Group

A second run was undertaken to simulate more closely Dedekind's original method, which consisted of using the structure of the residue group. The advantage in so doing is clear if we think of the fact that most of the computing time goes toward testing eq (3.7) for a solution. The amount of work can be cut to about a sixth [8] if we agree to keep the quadratic forms in storage so as to never test the same form twice. Because the memory had been almost exhausted by the program, magnetic tape was used for storage of forms.

The second run proceeded as follows. The machine generated the modules, testing each in turn until it came to (say) $\mathfrak{N}_1$, the first nonresidue module, which it put into memory. (Only the internal memory had been used thus far.) Once the machine reached this point it returned to the *beginning* of the list of modules and did two things "simultaneously": First of all, it tested each module whose quadratic form was not on the tape and loaded on the tape [9] every form that had been tested. Second, the machine took the residue module (say) $\mathfrak{N}$ that had not been previously tested (and loaded on tape) and formed $\mathfrak{N}_1\mathfrak{N}$ loading both quadratic forms on tape, while it accumulated $\log \mathrm{H}(\mathfrak{N}_1\mathfrak{N}) - \log \mathrm{H}(\mathfrak{N})$.

The second run led to an interesting array of quadratic forms which we see in table 2. Here R,S refer to coefficients of the residue quadratic form and R',S' refer to the corresponding nonresidue quadratic form which is formed by multiplying by the module $\mathfrak{N}_1$ as explained earlier.

Unfortunately, here overflow was a serious problem in the multiplication of modules, and only cases I through XVI, excluding XIV, went to completion. The forms for which $S=R$ or zero obviously correspond to self-conjugate modules.[10] The other self-conjugate modules are marked by "[a]", and can be spotted by the fact that the residue quadratic form and its negative do *not* both appear in table 2 (see footnote 9).

[8] Unfortunately tape motion produced too much delay (as much as 1 min per search) to permit these benefits to be fully realized.

[9] Here, whenever $\overline{\mathfrak{M}}=\mathfrak{M}$, $\rho\mathfrak{M}$, or $\rho^2\mathfrak{M}$, one should load both the Q for $\mathfrak{M}$ and the negative Q (for $\overline{\mathfrak{M}}$) on the tape to prevent both Q and its negative from appearing as residue forms. This fact had been overlooked and had to be corrected by an undesirable manual intervention in the computation.

[10] See footnote to table 2.

10. Concluding Prospects

The computation consummated here represents one phase of what really amounts to a larger task. The computation of units should also be programed, possibly after Voronoi's algorithm [5], so that h can be found even when M does not have the fortuitous form s^3+1. The storage of the previously tested forms in a larger high-speed memory would, of course, have speeded up computations, but the testing of congruence (3.7) leaves much to be desired in the direction of efficiency. To carry the groupings of modules and forms on to larger k, a double precision multiplication of modules would have to be provided. Lastly, it would be desirable to find the class structure algebraically [2], which is not altogether beyond the capacity of the SEAC.

The class structures, as well as the group structures, of the modules shall be the subject of further theoretical investigations.

The author thanks Olga Taussky for her aid and encouragement.

11. References

[1] J. W. S. Cassels, The rational solutions of the diophantine equations $Y^2=X^3-D$, Acta Math. **82,** 244 (1950).
[2] H. Cohn, Some experiments in ideal factorization on the MIDAC, J. Assoc. Comput. Mach. **2,** 111 (1955).
[3] H. Cohn and S. Gorn, A computation of cyclic cubic units, J. Research NBS **59,** 155 (1957) RP2783.
[4] R. Dedekind, Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern, Journ. für die reine und ang. Math. **121,** 40 (1900)
[5] B. N. Delauney and D. K. Fadeev, Theory of irrationals of third degree (in Russian), Travaux de l'Institut Stekloff XI (1940).
[6] R. Fueter, Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen, vol. I (Teubner, Leipzig, 1924).
[7] E. Hecke, Theorie der algebraischen Zahlen (Akad. Verlag, Leipzig, 1923).
[8] A. Markoff, Sur les nombres entiers dependents d'une racine cubique d'un nombre entier. Mém. de l'Acad. Imp. des Sciences de St. Pétersbourg, VII 38 (1892).
[9] T. Nagell, Über die Einheiten in reinen kubischen Zahlkörpern. Videnskap. Skrift. I, Mat. Kl., 11 (1923).
[10] O. Taussky, Some computational problems in algebraic number theory, numerical analysis, Proc. Symp. Appl. Math. Vol. 6. Amer. Math. Soc. 1956, 187–193.

Washington, March 14, 1957.