On Gauss's Class Number Problems

By Daniel Shanks

Abstract. Let h be the class number of binary quadratic forms (in Gauss's formulation). All negative determinants having some $h = 6n \pm 1$ can be determined constructively: for $h = 5$ there are four such determinants; for $h = 7$, six; for $h = 11$, four; and for $h = 13$, six. The distinction between class numbers for determinants and for discriminants is discussed and some data are given. The question of one class/genus for negative determinants is imbedded in the larger question of the existence of a determinant having a specific Abelian group as its composition group. All Abelian groups of order <25 so exist, but the noncyclic groups of order 25, 49, and 121 do not occur. Positive determinants are treated by the same composition method. Although most positive primes of the form $n^2 - 8$ have $h = 1$, an interesting subset does not. A positive determinant of an odd exponent of irregularity also appears in the investigation. Gauss indicated that he could not find one. ■

1. Introduction. Recently, Stark showed that $\Delta = 163$ is the largest integer for which the algebraic field $R(\sqrt{-\Delta})$ has class number 1. This is equivalent to the statement that binary quadratic forms

$$Au^2 + Buv + Cv^2$$

with

$$\Delta = 4AC - B^2$$

will have more than one class if $\Delta > 163$. Here $-\Delta$ is the *discriminant.*

Gauss's formulation of the same (then unproved) result is different, but equivalent. He writes

$$Au^2 + 2Buv + Cv^2, \qquad -D = AC - B^2$$

with D the *determinant.* A determinant -163 means a discriminant -652, and it is known that if

$$\Delta = 8k + 3, \qquad (k > 0),$$

and its class number is $h(-\Delta)$, then $h(-4\Delta) = 3h(-\Delta)$. So for Gauss the proposition reads: For class number 3, $-D$ is not greater than 163. Here is part of Gauss's table [1] for classifications with one genus:

	$-D$
I.1	1, 2, 3, 4, 7
I.3	11, 19, 23, 27, 31, 43, 67, 163
I.5	47, 79, 103, 127
I.7	71, 151, 223, 343, 463, 487 .

He writes ". . . the series of determinants corresponding to the same classifica-

Received July 15, 1968.

tion $\cdots$ always seem to terminate $\cdots$. Since the table from which we drew these examples has been extended far beyond the largest determinants that occur here, and since it furnishes no others belonging to these classifications, there seems to be no doubt that the preceding series do in fact terminate, $\cdots$. However, *rigorous* proofs $\cdots$ seem to be very difficult." Aside from these empirics, however, Gauss seems to offer no proof, difficult or otherwise, and for I.3 (one genus containing three classes) it seems unlikely that he had a proof.

What we first wish to show here is that for class number $h = 6n \pm 1$ the series do in fact terminate, and all corresponding determinants (this is Gauss's formulation) can be obtained constructively. In particular, the lists shown as I.5 and I.7 are complete for $h = 5, 7$. Likewise, his subsequent statement: "there are $\cdots$ four (the largest -1303) which correspond to I.11 $\cdots$" is also correct.

In later sections, we examine other questions of Gauss including those involving positive determinants and one class per genus. Specifically, we show that for negative determinants the noncyclic group of order 25, 49, or 121 cannot occur as a composition group; that although most prime determinants (or discriminants) $= n^2 - 8$ appear to have class number 1, there is an interesting subclass that does not; and, finally, there exists a positive irregular determinant with an odd "exponent of irregularity".

2. The Method and the Proof. If $-D = 1$, 2, or 4 the class number is 1. If $-D = 4k + 1, 4k + 2, 4k + 4$, $(k > 0)$, the class number is even, since there then exists an ambiguous form $F = (A, 2B, C)$ distinct from the principal form I, namely:

$$F = (2, 2, 2k + 1) \quad \text{for} \quad -D = 4k + 1\,,$$

$$F = (2^s, 0, 2k + 1) \quad \text{for} \quad -D = 2^s(2k + 1)\,,$$

$$F = (4, 4, 2^{s-2} + 1) \quad \text{for} \quad -D = 2^s \ (s > 2)\,.$$

Since $F^2 = I = (1, 0, -D)$ under composition, there is a subgroup of order 2.

If $-D = 3$ the class number is 1. If $-D = 8k + 3$, $(k > 0)$, the class number is divisible by 3 since

$$F = (4, 2, 2k + 1) \text{ satisfies } F^3 = I\,,$$

and now there is a subgroup of order 3.

Thus, for $h = 6n \pm 1$ $(n > 0)$, we must have

$$-D = 8k - 1\,.$$

But for discriminants $-\Delta$ with

$$\Delta = 8k - 1$$

it is known that

$$h(-\Delta) = h(-4\Delta)$$

without the factor of 3 which occurs when $\Delta = 8k + 3$. Thus we consider negative discriminants $\Delta = 8k - 1$ with class number $h(1 - 8k) = 6n \pm 1$. One quadratic form then is

$$F = (2, 1, k)$$

and by composition its hth power is the principal form

$$F^h = (1, 1, 2k) .$$

Since F represents 2, we therefore have

$$2^h = u^2 + uv + 2kv^2$$

or

$$2^{h+2} = (2u + v)^2 + \Delta v^2 .$$

Here, $v \not\equiv 0$, since h is odd, so the only possible Δ are those given by

$$\Delta = \frac{2^{h+2} - (2u + v)^2}{v^2} \tag{1}$$

which are finite in number. If h is a prime > 3 we also have $(2u + v)$ and v odd, since the group is cyclic with F as a primitive root, and if v were even there would be a representation of a smaller odd power of 2.

For example, if $h = 5$, we have

$$127 = 128 - 1, \quad 119 = 128 - 9, \quad 103 = 128 - 25,$$
$$79 = 128 - 49, \quad 47 = 128 - 81.$$

Of these, $119 = 7 \cdot 17$ has class number 10, and the remaining four comprise Gauss's (complete) list.

By construction, any h dividing 5, with $\Delta = 8k - 1$, must also appear here, and our last candidate $7 = 128 - 121$ is therefore the only remaining $h = 1$. Thus Gauss's row I.1 is simultaneously shown to be complete.

Similarly, from

$$-Dv^2 = 8192 - (2u + v)^2 ,$$

we find the four cases of class number 11: $-D = 167$, 271, 967, and 1303. The remaining values of $-D$ here have class numbers from 22 to 121 that are divisible by 11 with the sole exception that $8192 - 67^2 = 3703 = 7 \cdot 23^2$ can be interpreted either as $-D = 3703$, $v = 1$, with $h = 22$, or as $-D = 7$, $v = 23$, with $h = 1$ as before.

3. A Distinction and Some Data. Now, we must emphasize the following: this is Gauss's problem, and $-D = 127$ is the greatest negative determinant with class number 5. That does not mean that in algebraic fields $R(\sqrt{-\Delta})$ with class number 5, $\Delta = 127$ is the greatest. In fact, $R(\sqrt{-2683})$ also has class number 5, (perhaps *it* is the greatest). But since $2683 = 8 \cdot 335 + 3$, the *determinant* -2683 does *not* have class number 5, but rather 15.

We also note that Stark's result only includes the $8k + 3$ values in Gauss's row I.3. To show completeness there we compute all $8k - 1$ values

$$31 = 32 - 1, \quad 23 = 32 - 9 , \qquad (7 = 32 - 25) ,$$

as before.

A corollary of interest is this: Let

$$-D = 8k - 1 .$$

Then its class number h, regardless as to whether or not it is of the form $6n \pm 1$, must satisfy

$$h \geqq 1 + \log_2 k$$

where $\log_2$ here means "log to the base 2." Thus $-D = 1423$ and 1087 must have $h \geqq 9$, and since, as before, they arise from

$$1423 = 2^{11} - 25^2, \quad 1087 = 2^{11} - 31^2,$$

they do have $h = 9$. The remaining three $-D = 8k - 1$ with $h = 9$ are

$$823 = 2^{11} - 35^2, \quad 367 = 2^{11} - 41^2, \quad 199 = 2^{11} - 43^2.$$

(Since none of these five $-D$ appeared previously with $h = 3$, we may even add that their groups are cyclic, that is, these determinants are not "irregular".)

The fifteen known $-D = 8k + 3$ in I.9 are 59, 83, 107, 139, 211, 243, 283, 307, 331, 379, 499, 547, 643, 883, and 907, but they are not given by our theory. If Gauss is correct that there are only 20 determinants in I.9, that would imply that $R(\sqrt{-907})$ is the last field with class number 3. But that is unproven.

The fields with $\Delta = 1423$, 1087, 823, 367, and 199, as implied, all have a cyclic group of order 9. While there are many $\Delta = 8k + 3$ with the same property, we know of only one square-free Δ, namely, $\Delta = 4027$, where the noncyclic group of order 9 appears. It may be unique. More generally, the last Δ for fields $R(\sqrt{-\Delta})$ with $h < 10$ appears to be that listed in

TABLE 1

h	Δ	h	Δ	h	Δ
2	427	3	907	4 noncyclic	1435
4 cyclic	1555	5	2683	6	3763
7	5923	8, 8 genera	3315	8 cyclic	5947
8, 4 genera	6307	9 noncyclic	4027	9 cyclic	10627

None of this is proven.

4. Class Number 13 and Some Techniques. We wish to indicate briefly how the application of further theory can greatly reduce the computations needed to settle the completeness for some $h = 6n \pm 1$. Consider $h = 13$, a case not discussed by Gauss. Here

$$\Delta v^2 = 32768 - (2u + v)^2,$$

and the computation threatens to become lengthy. But if Δ is not a prime (or an odd power of a prime) its class number is even, as before, so we only need to test those Δ that are prime powers.

Aside from $v = 1$, any other possible v must have 2 as a quadratic residue for every prime divisor of v. But $v = 17$ requires

$$2u + v \equiv \pm 20 \pmod{17^2}$$

and therefore yields only negative Δ. And $v > 17$ similarly yields negative Δ, or,

at best, positive Δ that are clearly too small. Thus, if $v \neq 1$, we must have $v = 7$ and

$$2u + v \equiv \pm 6 \pmod{7^2}.$$

This gives

u	Δ	u	Δ
18	631	24	607
67	263	73	191.

These four Δ are prime and have $h = 13$. (For $\Delta = 191$, this was highly probable a priori since it was unlikely that such a small Δ could have $h \geqq 26$.)

The remaining candidates are

$$\Delta = 32768 - (2u + 1)^2,$$

but most of these can be quickly eliminated. Consider the first 71% of the entire range:

$$b = 2u + 1 < 128 = 2^7, \qquad \Delta > 16384 = 2^{14}.$$

Any such Δ has at least 13 quadratic forms, namely, the principal form:

$$(1, 1, \tfrac{1}{4}(\Delta + 1)),$$

and the 12 distinct forms:

$$(2, \pm b, 2^{12}), \quad (2^2, \pm b, 2^{11}), \quad (2^3, \pm b, 2^{10}),$$
$$(2^4, \pm b, 2^9), \quad (2^5, \pm b, 2^8), \quad (2^6, \pm b, 2^7).$$

It may be seen that for such Δ the left coefficient here, $A = 2^n$, $n = 1$ to 6, remains unchanged when the form is reduced. But, if $h = 13$, we cannot tolerate even one more reduced form. Now consider the odd primes $p < 64$, and if

$$(-\Delta/p) = +1,$$

there will be reduced forms $(p, \pm B, C)$ distinct from the foregoing. If $b \equiv 0 \pmod 3$, there are the forms $(3, \pm 1, C)$; if $b \equiv \pm 2 \pmod 5$, there are the forms $(5, \pm 1, C)$; etc., and this is so whether Δ is prime or not. In this way we may sieve out this entire range without actually computing the class numbers, but nonetheless having knowledge that they are multiples of 13 that exceed 13.

As Δ falls below 2^{14} we must be a bit more careful, but similar techniques are applicable, and we thereby determine, without undue computation, that there are exactly six negative determinants with $h = 13$:

$$-D = 191, 263, 607, 631, 727, 2143.$$

Again, we have the ubiquitous $h = 1$:

$$-D = 7 = 2^{15} - 181^2.$$

5. The First Missing Group and Others. Gauss also expressed the opinion that for any negative determinant [1, p. 362] with 32 or more genera there are at least two classes per genus. This would follow if it could be proven, as was also conjectured, that there are exactly 65 idoneal numbers—that is, that the list of these by

Euler and Gauss is complete. In turn, it implies that the composition group of order 32 which is a direct product of five groups of order 2 does not occur. This remains unproven although it is now known, cf. [2], that there are only a finite number of negative determinants with one class per genus.

We may put the question in a more general form and ask: Which Abelian groups do occur as composition groups for negative determinants? There are 37 distinct Abelian groups of order $\leqq 24$. For each of these there is at least one square-free negative determinant that has this group as its composition group. For example, $-D = 307$ (Gauss's irregular determinant) has the noncyclic group of order 9, and $-D = 146, 161, 285, 1365$, and 1513 have the five distinct groups of order 16. For class number 25, we have $-D = 479, 599, 1367, \cdots$ but each of these has the cyclic group. For some time, the author believed that the noncyclic group of order 25 did not occur, but he lacked a proof.

In principle, we can now complete this series and test them all. But the proof is much simpler. Each form except the principal form is of order 5 in the noncyclic group. As before, then, from

$$-D = 8k - 1\,, \qquad F = (2, 1, k)$$

we have

$$2^7 = (2u + v)^2 + (8k - 1)v^2$$

and the series $-D = 479$, etc. are clearly all too large to represent $2^7 = 128$.

Similarly, $-D = 1511, 2111$, etc. have class number 49 and are clearly too large to have the noncyclic group.

But for class number 121, we need an additional calculation. In our examination of $h = 11$ above, we found one, and only one,

$$\Delta = 8111 = 2^{13} - 9^2$$

with class number 121. But while the form $F = (2, 1, 1014)$ does have order 11 here, this is merely necessary, not sufficient. A second form

$$G = (3, 1, 676)$$

satisfies

$$G^{11} = (16, -9, 128) = F^7$$

and therefore generates a cyclic group of order 121.

Thus, we conclude that the noncyclic groups of order 5^2, 7^2, and 11^2 do not occur for negative determinants.

This leaves it open, to our knowledge, whether there is a field with negative discriminant $\Delta = 8k + 3$ that has any of these groups. We can only state that the noncyclic 25 does not occur for $\Delta < 10{,}000$. (See *Note added in proof* below.)

6. Positive Determinants and Discriminants. For positive determinants, on the contrary, Gauss [3, p. 353] indicated that *most* of these appeared to have one class per genus, and he raised the question whether the fractions that do may not tend to some fixed limit as the value of the determinant goes to infinity. This is also unsettled.

Let us first confine ourselves to one genus and set the determinant D, or the discriminant d, to be a prime (or an odd power of a prime) of the form

$$d = 8s + 1\,, \qquad D = 8s + 1\,.$$

Further, in (1), let us specifically examine the cases $h = 1, 3, 5, 7$, and, for simplicity, $v = 1$. For orientation, we list in Table 2 all positive or negative prime-power discriminants of the forms $n^2 - 8$, $n^2 - 32$, $n^2 - 128$, and $n^2 - 512$ that do not exceed 10,000 together with their class numbers. (As before these class numbers are the same for the discriminant and the determinant.)

TABLE 2

Prime-Powers of Form $n^2 - 2^{2k+1}$ *and* $h(n^2 - 2^{2k+1})$

n^2-8	h	n^2-32	h	n^2-128	h	n^2-512	h
−7	1	−31	3	−127	5	−503	21
17	1	−23	3	−103	5	−487	7
41	1	−7	1	−79	5	−463	7
73	1	17	1	−47	5	−431	21
113	1	89	1	−7	1	-7^3	7
281	1	137	1	41	1	−223	7
353	1	193	1	97	1	−151	7
433	1	257	3	233	1	−71	7
521	1	409	1	313	1	17	1
617	1	593	1	401	5	113	1
953	1	809	1	601	1	449	1
1217	1	929	1	1097	1	577	7
1361	1	1193	1	1553	1	857	1
2017	1	1489	3	2081	5	1009	7
2393	1	1993	1	2273	1	1697	1
2593	1	2777	3	2473	1	1889	1
2801	1	3217	1	2897	1	2089	3
4217	1	3449	1	3121	5	2297	1
4481	3	4457	1	3593	1	2969	1
6553	1	4729	3	17^3	1	3209	1
7561	1	5009	1	5801	1	3457	1
8273	1	5297	3	6113	5	4817	1
8641	1	5897	1	6761	1	5113	1
		6529	1	7793	1	5417	7
		6857	1	8521	1	7057	21
		7193	1	9281	3	8513	1
		7537	3			9689	1
		9377	1				
		9769	1				

The negative discriminants here have been discussed previously, but are included for comparison. The most notable distinction is that the same

$$d = (2u + 1)^2 - 2^{2k+1}$$

which can have only finitely many negative values yields infinitely many positive candidates—it being the nature of a parabola to be open only at one end.

Consider the first column of Table 2. If $d = 8s + 1$, one has the form

$$F = (2, 1, -s),$$

and if we are to have class number 1 this form must be equivalent to the principal form, which may be written $(1, 1, -2s)$. If d is a prime of the form $n^2 - 8$ this condition is surely met, and we may factor 2 by

$$2 = (\tfrac{1}{2}n + \tfrac{1}{2}\sqrt{d})(\tfrac{1}{2}n - \tfrac{1}{2}\sqrt{d})$$

in the algebraic field.

What is impressive in this first column is the "extent" to which this necessary condition is sufficient. There is only one counterexample less than 10,000, namely, the listed 4481. Here we have class number 3 even though F is equivalent to the principal form.

Similarly, in the remaining columns, $n^2 - 32$, $n^2 - 128$, $n^2 - 512$, we force F^3, F^5, or F^7, respectively, to be equivalent to the principal form. This allows F itself to be equivalent. While we therefore find a goodly number of class number 3, 5, or 7 here, (or the multiple of 7 for $d = 7057$), we also find many of class number 1.

What catches the eye are curious cases $d = 9281, 2089$, which like 4481 have $(2, 1, -s) \sim (1, 1, -2s)$ and still do not have class number 1, but rather 3. Let d be any prime of the form $8s + 1$—without insisting on any special form such as $n^2 - 8$. One finds that of the 295 primes $8s + 1 < 10{,}000$, 252 have $(2, 1, -s) \sim (1, 1, -2s)$, and, of these, 248 have class number 1. The four exceptions are 8713 and the previously mentioned 4481, 9281, and 2089.

It might seem, therefore, that while $(2, 1, -s) \sim (1, 1, -2s)$ is not a sufficient condition for class number 1, the exceptions are rather rare. If this could be quantified, and if it could be shown that there are infinitely many primes of the form $n^2 - 8$, as seems very likely by the Hardy-Littlewood conjecture, cf. [4], then one would have infinitely many square-free discriminants with class number 1. This remains unproven.

7. A Class of Counterexamples and Others. Returning to 4481, we wish to analyze its peculiarity so as to locate any others of its ilk. Its principal form has the following period of reduced forms:

$$(1, 65, -64), \quad (-64, 63, 2) \quad (2, 65, -32), \quad (-32, 63, 4),$$
$$(4, 65, -16), \quad (-16, 63, 8), \quad (8, 65, -8), \quad (-8, 63, 16), \text{ etc.}$$

It is clear, by induction, that the center coefficients are alternatingly 64 ± 1, and the end coefficients are powers of 2 or their negatives. But, by Lagrange's Theorem, cf. [5], any number $< \frac{1}{2}\sqrt{4481}$ which is represented by the principal form must occur as one of these end coefficients. Therefore, if there is even one odd prime $p < \frac{1}{2}\sqrt{4481}$ which has 4481 as a quadratic residue, its corresponding form must be inequivalent to the principal form, i.e., the class number exceeds 1. And, for 4481, one has no lack of such:

$$(5, 61, -38), \quad (7, 55, -52), \quad (11, 57, -28), \text{ etc.}$$

(Note, this argument is quite similar to that used in Section 4, even though the reduced classes there, $(2, \pm b, 2^{12})$, etc. were inequivalent.)

We therefore generalize 4481 as follows: Let

$$S_n = (2^n + 3)^2 - 8$$

and seek primes of this form. Then S_6 is our 4481, and one may see that the reduced forms for the general S_n have a similar characterization. If one now has a residue:

$$p < \tfrac{1}{2}\sqrt{S_n}\,, \qquad (S_n|p) = +1\,, \tag{2}$$

one therefore has a prime of the form $m^2 - 8$ with a class number greater than 1. For $S_1 = 17$, $S_2 = 41$, $S_3 = 113$, $S_4 = 353$, $S_5 = 1217$, there are no such primes p, and we have class number 1, as in Table 2.

But as $S_n \to \infty$, condition (2) becomes more and more difficult to avoid and one expects the class number to increase without bound. One finds that S_7, S_9, and S_{13} are composite and may be discarded. But

$$\begin{aligned} S_8 &= 67073 \text{ has } h = 3\,, \\ S_{10} &= 1054721 \text{ has } h = 9\,, \\ S_{11} &= 4206593 \text{ has } h = 11\,, \\ S_{12} &= 16801793 \text{ has } h = 27\,. \end{aligned}$$

That, in general, S_n will have numerous primes p satisfying (2) as $n \to \infty$ seems clear, since $p = 5$ is valid for every $n = 4k + 2$; $p = 7$ for every $n = 3k$; 11 for every $n = 10k + 3$, 4, 6, 7; etc. On the other hand, one expects, heuristically, that the number of prime S_n should go to infinity as $O(\log n)$.

As an aside, we wish to indicate that the determination of, e.g., $h(16801793) = 27$ would be very tedious by the classical method of listing all of its reduced forms, inasmuch as it has so many. Here, we set $G = (7, 4089, -2924)$ and by composition we find its smallest power, 27, that gives the principal form. Then, h is an odd multiple of 27, since the discriminant is prime. Therefore, $h = 27$, or at least 81, and the latter may be excluded by consideration of the Pell solution and the relationship

$$\frac{\log (T + U\sqrt{d})h}{2\sqrt{d}} = \prod_{p>2} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right)^{-1}.$$

Our point is that the idea of composition, used extensively above, is useful not only theoretically, but also computationally.

If these S_n were the only primes $n^2 - 8$ with $h > 1$ we could conclude, heuristically, that "almost all" primes $n^2 - 8$ had $h = 1$, and therefore Gauss's idea of a fixed limiting ratio <1 would be inapplicable to this subset of positive determinants. However, there are other counterexamples. The examples $d = 8713$, 9281, and 2089 mentioned above have periods for their principal forms of a much more intricate character than those for the S_n, and, a priori, there is no reason why similar examples cannot occur for $n^2 - 8$.

Recently, Dr. Morris Newman made available to us Kloss's table [6] of class numbers for prime discriminants $4m + 1$ less than 100,000. We may therefore easily extend our Table 2. In that table there are 22 primes $n^2 - 8 < 10{,}000$, of which 21 have $h = 1$. In the continuation there are 44 more primes $n^2 - 8 < 100{,}000$, of which 38 have $h = 1$. Besides our previously found S_8 with $h = 3$, there are five other counterexamples all of which have a more intricate and less analyzable character: $p = 15121$, $h = 5$; $p = 31321$, $h = 7$; $p = 45361$, $h = 3$; $p = 75617$, $h = 3$; and $p = 91801$, $h = 3$. The fraction of primes $n^2 - 8$ with $h > 1$ therefore

increases beyond its very low value when $p < 10{,}000$ and it is not improbable that Gauss's fixed limit idea is applicable here also.*

8. Some Clarifying Remarks. It may be useful for some readers to make the following clarifications. Another distinction between positive and negative determinants is that our deductions concerning factors of 3 and 2 at the beginning of Section 2 also break down, in part, for $D > 0$. Consider the factor of 3, with

$$D = 8s - 3\,, \qquad F = (4, 2, 1 - 2s)\,.$$

For $-D = 8k + 3$ we obtained a factor of 3 *except for* $k = 0$ since

$$F = (4, 2, 2k + 1)$$

was *then inequivalent* to I and $F^3 = I$. For $k = 0$, F is equivalent to I, and $D = -3$ is a solitary exception. But for positive $D = 8s - 3$ there is no a priori reason for F to be inequivalent, and we often find that it is equivalent. For these positive determinants, then, we do *not* have $h(4D) = 3h(D)$, but rather $h(4D) = h(D)$. It follows that one has many determinants $p = 8s - 3$ where the class number is not a multiple of 3 and our previous completeness argument is lost. For example,

$$h(4 \cdot 5) = h(4 \cdot 13) = h(4 \cdot 29) = 1\,, \qquad h(4 \cdot 1093) = 5\,.$$

On the other hand, if F is inequivalent to I, as for $d = 37, 101, \cdots, 1901$, etc., then one has

$$\begin{aligned} h(37) &= 1\,, & h(4 \cdot 37) &= 3 \\ h(101) &= 1\,, & h(4 \cdot 101) &= 3 \\ h(1901) &= 3\,, & h(4 \cdot 1901) &= 9\,, \end{aligned}$$

as before.

Similarly, the factor of 2 in Section 2 may be lost for real fields $R(\sqrt{d})$. We omit the details, but suggest that a reader who wishes to study this further work through the following examples.

The real field $R(\sqrt{d})$ has class number 2 for $d = 85, 205, 485$, and 1405. But the corresponding quadratic forms for these positive determinants have class number 2, 4, 6, and 12, respectively. Thus, the factors of 2 and 3 mentioned above may occur or be lost independently of each other.

9. A Sought for Irregular Determinant. A final problem of Gauss that we wish to discuss is this. He wrote [1, p. 369–370] ". . . there seems to be no doubt that there are [positive determinants] whose exponent of irregularity is odd, although we confess that none has come to our attention thus far." H. J. Smith, in his *Report* [7, p. 258], repeats this almost in the same words, and Dickson's *History* [8] offers no example discovered in the next century.

The simplest example would be a noncyclic class number 9, since here there is then only one genus, and it is irregular of exponent 3. For the negative determinant, $D = -307$, and discriminant, $d = -4027$, we mentioned such examples above.

---

* For further discussion of Gauss's conjecture, see a long analytical review of Kloss's table on page 213 of this issue of *Mathematics of Computation*.

Does this group exist for positive determinants?

There is at least one example. If we extend the column $n^2 - 32$ of Table 2 we find $32009 = 179^2 - 32$ with $h(32009) = 9$. By construction, we have "encouraged" its form that represents 2 to be of third order. Since $32009 = 5^6 + 4 \cdot 4^6$ we have one reduced form

$$4^3u^2 + 5^3uv - 4^3v^2$$

that represents both 5^3 and 4^3 explicitly, and, of necessity, it lies in the principal form inasmuch as it gives the unique decomposition of 32009 as a sum of two squares. Since the noncyclic group of order 9 has every element, except the identity, of order 3, the example looks suspiciously like that sought. Upon examination one finds

$$F = (2, 177, -85), \quad F^2 = (4, 173, -130), \quad F^3 = I = (1, 177, -170),$$
$$G = (5, 177, -34), \quad G^2 = (25, 147, -104), \quad G^3 = I = (1, 177, -170),$$

and since F, G, and I are all inequivalent we have a composition group which is a direct product of two groups of order 3. Thus, the determinant 32009, the discriminant 32009, and the real field $R(\sqrt{32009})$ all have the noncyclic group of order 9. There is no assertion that this is the smallest such D, but merely the first that we found. (See *Note added in proof.*) We similarly sought the noncyclic 25 group for a positive determinant but did not find it. Unlike the result in Section 5, we see no a priori reason for its nonexistence when the determinant is positive.

Note added in proof. Subsequently we learned that Gordon Pall [9] had already found a positive discriminant, $d = 62501$, with a noncyclic class number 9. (This is just the opposite of the possibility we envisaged above: it is not smaller and found later, but, rather, larger and found earlier.) A technical comparison of 32009 and 62501 is of some interest at two points.

Since $62501 \not\equiv 8k + 1$ it could not appear in any extension of Table 2 as 32009 does, and must be discovered in some other way. The real connection between the two examples lies in their similar decompositions:

$$32009 = 5^6 + 4 \cdot 4^6, \qquad 62501 = 1^6 + 4 \cdot 5^6,$$

and the generalization to other potential candidates for noncyclic groups of order p^2 is obvious:

$$P = m^{2p} + 4 \cdot n^{2p}.$$

Also, since $62501 \not\equiv 8k + 1$, when 62501 is regarded as a determinant, as Pall also does, its class number is 27, not 9. Is its group $C(3) \times C(3) \times C(3)$ or is it $C(3) \times C(9)$, where $C(n)$ is cyclic of order n? Pall does not say, but it is $C(3) \times C(9)$. From Gauss's viewpoint, $D = 62501$ would therefore be distinctly more complex than 32009, (aside from being a little larger).

Pall also states there that $d = -12379$ has the noncyclic group of order 25. At the end of Section 5 above we searched for such a discriminant and stated that there were none with $-d < 10{,}000$. Thus, Pall's -12379 would be very welcome (especially as $12379 > 10{,}000$) if it really were noncyclic. Unfortunately, it is not. If $F = (7, 5, 443)$ one has

$$F^2 = (49, 19, 65), \qquad F^3 = (19, -3, 163),$$
$$F^4 = (35, 9, 89), \qquad F^5 = (5, -1, 619) = G,$$
$$G^2 = (25, -11, 125), \qquad G^3 = (25, 11, 125) = G^{-2}.$$

Therefore,

$$G^5 = F^{25} = I = (1, 1, 3095),$$

and F generates a cyclic group of order 25. From $F^3 \neq F^{-2}$ one knows already that one does not have the noncyclic 25.

Later, at our suggestion, Edward Ordman kindly computed [10] $h(-p)$ for all primes $p = 8m + 3 < 10^5$. There are 89 such primes from $p = 3851$ to $p = 93307$ with $h(-p) = 25$, and from unpublished work of the Lehmers, computed for quite a different purpose, it is highly probable that $p = 93307$ is the last negative discriminant with $h = 25$.

We find that two and only two of these, $p = 12451$ and 37363, have the noncyclic group. In the first,

$$F^{\pm 1} = (5, \pm 3, 623), \quad F^{\pm 2} = (25, \mp 7, 125)$$

and

$$G^{\pm 1} = (7, \pm 3, 445), \quad G^{\pm 2} = (49, \pm 17, 65)$$

are of order 5, and the whole group is the product of these two cycles. For the second,

$$F^{\pm 1} = (11, \pm 9, 851), \quad F^{\pm 2} = (83, \mp 53, 121)$$

and

$$G^{\pm 1} = (13, \pm 5, 719), \quad G^{\pm 2} = (89, \mp 27, 107)$$

have the same property.

Most of the other 87 primes are quickly seen to have the cyclic group. There are 13, from 3851 to 21323, of the form $3k - 1$. They therefore have a form $(3, B, C)$, and since they all exceed $972 = 4 \cdot 3^5$ this form must be of order 25. This is the same argument as that used in Section 5 with 2 replaced by 3. There are 18, from 12979 to 34939, that exceed $12500 = 4 \cdot 5^5$ and are of the form $10k \pm 1$. Their forms $(5, B, C)$ are therefore of order 25. While there are none with $(-p|7) = 1$ that exceed $4 \cdot 7^5$, there are 12 with $(-p|7) = 1$, from 20347 to 39163, for which one sees at once that $67228 - p \neq u^2$. These are clearly cyclic. Most of the remaining primes are found to have the cyclic group by finding a form F with $F^3 \neq F^{-2}$. For example, for 93307,

$$F = (23, -21, 109), \quad F^2 = (101, 57, 239), \quad F^3 = (41, 3, 569).$$

Applied Mathematics Laboratory
Naval Ship Research and Development Center
Washington, D. C. 20007

1. C. F. GAUSS, *Diquisitiones Arithmeticae*, Yale Univ. Press, New Haven, Conn., 1966, (Clarke Translation), pp. 361–362. MR **33** #5545.
2. S. CHOWLA, "Heilbronn's class-number theorem," *Proc. Indian Acad. Sci. Sect. A*, v. 1, 1934, pp. 74–76.
3. C. F. GAUSS, *Untersuchungen über höhere Arithmetik*, Chelsea, New York, 1965, (Reprint of Maser Translation). The English translation [1] is garbled here. MR **32** #5488.
4. DANIEL SHANKS, "On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$," *Math. Comp.*, v. 14, 1960, pp. 321–332. MR **22** #10960.
5. L. E. DICKSON, *Introduction to the Theory of Numbers*, Univ. of Chicago Press, Chicago, 1929, Theorem 85, p. 111.
6. K. E. KLOSS, "Some number-theoretic calculations," *J. Res. Nat. Bur. Standards Sect. B*, v. 69B, 1965, pp. 335–336. MR **32** #7473.
7. H. J. SMITH, *Report on the Theory of Numbers*, Chelsea, New York, 1964, reprint.
8. L. E. DICKSON, *History of the Theory of Numbers*, Vol. 3, Stechert, New York, 1934, reprint, Chapter V.
9. GORDON PALL, "Note on irregular determinants," *J. London Math. Soc.*, v. 11, 1936, pp. 34–35.
10. This table will be deposited in the UMT file and be reviewed in this journal.