MATHEMATICS OF COMPUTATION, VOLUME 25, NUMBER 116, OCTOBER, 1971

Gauss's Ternary Form Reduction and the 2-Sylow Subgroup

By Daniel Shanks

Abstract. An algorithm is developed for determining the 2-Sylow subgroup of the class group of a quadratic field provided the complete factorization of the discriminant d is known. It uses Gauss's ternary form reduction with some new improvements and is applicable even if d is so large that the class number $h(d)$ is inaccessible. Examples are given for various d that illustrate a number of special problems.

1. Introduction. The problem treated here is this: Given an imaginary quadratic field $Q(\sqrt{-\Delta})$ where the factorization of Δ is completely known, to compute the 2-Sylow subgroup of its class group. My interest in a solution was motivated by two closely related questions. Since these are interesting in their own right, I will use them here as an introduction.

For certain n, the numbers

$$S_n = (2^n + 3)^2 - 8 \tag{1}$$

are primes of the form $8k + 1$ with many remarkable properties [1, p. 158]. Since S_n is then prime, the 2-Sylow subgroup for $Q(\sqrt{-S_n})$ is cyclic and is

$$C(2^{U(n)}) \tag{2}$$

of some unknown order $2^{U(n)}$. Here is a brief table:

n	$U(n)$	n	$U(n)$	n	$U(n)$
1	2	6	6	19	7
2	3	8	8	27	6
3	3	10	9	28	9
4	4	11	6	32	8
5	5	12	10	36	10

Now, it is easily seen that $U(n) \geqq 3$ for $n > 1$, but it was (and remains) obscure why the $U(n)$ are much larger. The determination of $U(n)$ is a special case of the general problem above, with $\Delta =$ prime S_n and (2) as the 2-Sylow subgroup.

Next, consider

$$S_{36} = 4722366483281962074113.$$

The only feasible way of evaluating

$$h(-4S_{36}) = 50866650112, \tag{3}$$

Received March 22, 1971.

AMS 1970 *subject classifications.* Primary 12A25, 10C05; Secondary 10-04.

Key words and phrases. Quadratic field, class group, 2-Sylow subgroup, genera, principal genus, ambiguous forms, reduction of ternary quadratic forms, cycle graph.

to my knowledge, is the method I introduced in [2]. For this specific case (3), I pointed out there [2, p. 417] that if one knows that

$$h \equiv 2^{10} \pmod{2^{11}},$$

then the algorithm in [2] can be speeded up by a factor of $2^{11/2} \approx 45$. The knowledge that $U(36) = 10$ therefore much facilitates the evaluation of the class number (3). Consequently, I referred to this present paper in [2], before its publication, as ref. [6], "to appear".

The solution of the problem is suggested by the theory of factorization given in Section 5 of [2]. Consider

$$h(-4S_{19}) = 128 \cdot 3377. \tag{4}$$

To factor S_{19} (not yet knowing that it is prime), one selects a binary quadratic form of discriminant $-4S_{19}$ such as

$$F = (3, 2, 91627017558),$$

and computes

$$G = F^{3377} = (318607, -142542, 878702) \tag{5}$$

by composition. (See [2, Appendix 1] for an efficient algorithm.) Then, repeatedly squaring, one obtains

$$G^2 = (167277, -111536, 1661861)$$

$$G^4 = (502722, -256318, 579457)$$

$$G^8 = (71473, 52746, 3855674)$$

$$G^{16} = (169257, 71408, 1631577) \tag{6}$$

$$G^{32} = (524289, 4, 524293) \tag{7}$$

$$\mathfrak{A} = G^{64} = (2, 2, 137440526337) \tag{8}$$

$$I = G^{128} = (1, 0, 274881052673). \tag{9}$$

Since G is thus of order 128, the 2-Sylow subgroup is cyclic and the only ambiguous forms are the identity (9) and the trivial (8). Therefore, S_{19} is prime and has no proper factors.

The general strategy of determining $U(19)$, if one does *not* know the class number (4), is now clear. One starts at the ambiguous form (8) and determines one of its square-roots $\sqrt{\mathfrak{A}}$. Gauss's famous theorem [3] states that a form has a square-root if and only if it is in the principal genus. And (8) is in the principal genus since $(2 \mid S_{19}) = +1$.

Subsequent to Gauss, other proofs were given for his theorem but Gauss's proof is the most *explicitly constructive* of them all. Using his construction we thereby obtain (7) (or the other square-root G^{-32}). If (7) is in the principal genus (it is), we repeat the operation and continue until we get to (5) (or some other 128th root of I). Since G is *not* in the principal genus, the process terminates and one has $U(19) = 7$.

The solution of the general problem is similar. Assume that $Q(\sqrt{-\Delta})$ has 2^r genera, and therefore 2^r ambiguous forms

$$I, \mathfrak{A}_2, \mathfrak{A}_3, \cdots, \mathfrak{A}_{2^r}. \tag{10}$$

Its 2-Sylow subgroup now has r cyclic factors:

$$C(2^{n_1}) \times C(2^{n_2}) \times \cdots \times C(2^{n_r}) \tag{11}$$

and we wish to compute $n_1, n_2, \cdots$. Since the factorization of Δ is completely known, we can write each $\mathfrak{A}$: $\mathfrak{A}_2, \mathfrak{A}_3, \cdots$ explicitly. For each $\mathfrak{A}_i$ in the principal genus, if any, we may evaluate one of its square-roots

$$K_i = \sqrt{\mathfrak{A}_i}$$

as above. Then the remaining $2^r - 1$ square-roots of $\mathfrak{A}_i$ are given simply by the compositions

$$\mathfrak{A}_2 K_i, \mathfrak{A}_3 K_i, \cdots, \mathfrak{A}_{2^r} K_i \tag{12}$$

since the class group is Abelian. We thereby can build up the entire 2-Sylow subgroup (11) explicitly.

We give below a brief account of Gauss's construction together with some small improvements we made. This algorithm has been coded in a computer program called GATESR, with which we can determine these 2-Sylow subgroups even if the discriminant d is so large that the computation of $h(d)$ is not feasible. GATESR, of course, stands for "Gauss Ternary Square-Root".

About $1\frac{1}{2}$ years after my Stony Brook talk [2], but before the present paper was submitted for publication, I learned from Professor H. Hasse that Helmut Bauer had written a somewhat related program. Bauer's paper will appear as [4]. He kindly sent me a preliminary account entitled "Die 2-Klassenzahlen spezieller quadratischer Zahlkörper". From this note, the differences between his paper and mine can be characterized as follows:

A. There is a difference of language, and I do not mean German and English. Since I follow Gauss here, I use the language of quadratic forms. Bauer follows Hasse, and uses the language of divisors. But this is merely language, not a difference of substance; the groups involved are isomorphic.

B. Because of the motivations indicated above, we are primarily interested in imaginary fields here, but the algorithm developed works for discriminants $d > 0$ also, and we give several such examples in Section 6. Bauer gives equal attention to $d > 0$ and $d < 0$, but, on the other hand, he examines only d divisible by exactly two primes, as he states in his title [4]. These fields have $r = 1$, in the notation above, and cyclic subgroups. As I indicated above, the generalization to all d that can be factored completely is not difficult. I will give several noncyclic examples below.

C. The most important difference is that Bauer does not use Gauss's ternary form reduction. He must solve a certain ternary equation, which is not specified in his note above. But since he confines himself, in this note, to $|d| < 8000$, he uses a simple, trial-and-error method of obtaining a solution: "so dass es genügt, ein einfaches Suchverfahren zu verwenden". In contrast, Gauss's reduction is highly efficient, arithmetically speaking, and can also be used for very much larger discriminants. In fact, it is only for large d that a program of this type is really needed; if d is small, one can easily compute $h(d)$, and therefore $2^u \,||\, h(d)$, directly.

2. Gauss's Solution with Some Changes. In [3, Section 286, p. 338] Gauss solves the following:

"PROBLÈME. Etant donnée une forme binaire $F = (A, B, C)$ de déterminant D appartenant au genre principal, trouver une forme binaire f qui donne F par sa duplication."

In this section we sketch Gauss's solution. We begin with some adaptation we must make in order to use his notation and solution, and we conclude with some changes that we make in his solution in order to shorten it somewhat.

By (7) above, we mean a quadratic form

$$524289x^2 + 4xy + 524293y^2.$$

Gauss writes this as

$$(524289, 2, 524293)$$

with the middle term halved. These coefficients are the A, B, C in

$$F = Ax^2 + 2Bxy + Cy^2. \tag{13}$$

Gauss calls $D = B^2 - AC$ the *determinant* of F.

In what follows, we use this Gauss notation exclusively. That implies that we only allow *even discriminants*:

$$d = 4(B^2 - AC) = 4D.$$

If the discriminant of $Q(\sqrt{-\Delta})$ is already even, i.e., if $d = -4\Delta$, there is no problem, but if $\Delta \equiv -1 \pmod 4$, and $d = -\Delta$, there also is no real problem. In the latter case, it is known that the primitive binary quadratic forms of discriminant -4Δ constitute a group under composition and its 2-Sylow subgroup is isomorphic to that of $Q(\sqrt{-\Delta})$. Therefore, with no loss of generality, we can make the discriminant even and use Gauss's solution directly.

Now assume that

$$F = (a_1, b_3, a_2) = a_1x^2 + 2b_3xy + a_2y^2 \tag{14}$$

is in the principal genus. We want an

$$f = (a, b, c) \tag{15}$$

such that $f^2 \sim F$ under composition. Gauss adds three terms and enlarges F into a ternary form $a_1x^2 + a_2y^2 + a_3z^2 + 2b_1yz + 2b_2xz + 2b_3xy$ which he writes as

$$t = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}. \tag{16}$$

The terms added are such that the *determinant* of t, which is defined as

$$D(t) = b_1^2a_1 + b_2^2a_2 + b_3^2a_3 - a_1a_2a_3 - 2b_1b_2b_3, \tag{17}$$

equals $+1$. The form t has an *adjoint*:

$$T = \begin{pmatrix} A_1 & A_2 & A_3 \\ B_1 & B_2 & B_3 \end{pmatrix} \tag{18}$$

given by the equations

$$(19)\qquad \begin{aligned} A_1 &= b_1^2 - a_2a_3, & A_2 &= b_2^2 - a_1a_3, & A_3 &= b_3^2 - a_1a_2,\\ B_1 &= a_1b_1 - b_2b_3, & B_2 &= a_2b_2 - b_1b_3, & B_3 &= a_3b_3 - b_1b_2. \end{aligned}$$

The adjoint of T may be seen to be t, since $D(t) = 1$. Therefore, we also have

$$(20)\qquad \begin{aligned} a_1 &= B_1^2 - A_2A_3, & a_2 &= B_2^2 - A_1A_3, & a_3 &= B_3^2 - A_1A_2,\\ b_1 &= A_1B_1 - B_2B_3, & b_2 &= A_2B_2 - B_1B_3, & b_3 &= A_3B_3 - B_1B_2. \end{aligned}$$

Now, note that A_3 is the determinant of F. Since F is in the principal genus, a_1 and a_2 are quadratic residues of each prime divisor of A_3. There are therefore solutions of

$$(21)\qquad B_1^2 = a_1 + A_2A_3, \qquad B_2^2 = a_2 + A_1A_3, \qquad B_1B_2 = -b_3 + B_3A_3$$

consistent with (20). From F and A_3 we therefore determine B_1, A_2, B_2, A_1, and B_3. We now have T and may compute the a_3, b_1, and b_2 needed to complete t from (20).

By a series of linear transformations of determinants ± 1 that we discuss in the next section, Gauss transforms t into

$$(22)\qquad t' = \begin{bmatrix} 1 & 0 & 0\\ -1 & 0 & 0 \end{bmatrix}$$

which has the same determinant $D(t') = +1$. Conversely, there is a 3×3 matrix m that transforms t' into t. Gauss now computes the a, b, c needed for (15) from the elements of m.

We have already made one change in Gauss in our description above, in that Gauss builds his ternary t with $-b_3$ instead of the original coefficient b_3. But it seems preferable to use the original b_3, as we do above, and adjust the sign of b at the end of the process. Next, in place of the t' of (22), we will use the ternary form

$$(23)\qquad u = \begin{bmatrix} 0 & 1 & 0\\ 0 & -1 & 0 \end{bmatrix}.$$

This shortens the reduction process and also has the effect, as we shall see, that a, b, and c appear in their correct locations in the array below. Our third, and main change is that we do *not* compute an inverse such as m above. If M transforms t into u and

$$(24)\qquad M = \begin{bmatrix} - & - & -\\ - & - & -\\ X & Y & Z \end{bmatrix},$$

we ignore its first two rows and have, directly, that if ϵ is the sign of X,

$$(25)\qquad f = (\epsilon X, -Y, 2\epsilon Z) \quad \text{or} \quad f = (2\epsilon X, -Y, \epsilon Z)$$

according as X is odd or even. We not only avoid computing an inverse matrix, and also have simpler formulas for a, b, and c, but, in the series of transformations needed to transform t into u, it is *only necessary to compute the third row* in the corresponding series of matrices that culminate in M.

Mostly, it is Gauss—but with improvements. By way of proof, one simply notes that the Gauss computation [3, Section 286], mentioned above, that leads to (a, b, c)

from the elements of m is really the computation of a single row in the *inverse* of m. This double inversion, therefore, merely cancels itself out.

3. Gauss's Reduction and an Explicit Endgame. In reducing the ternary form t to u we first make a series of binary form reductions. We alternate between two different types which we call Phase 0 and Phase 1. The binary form reduction is the usual one (going back to Lagrange) of transforming into a series of "neighboring" forms. Given a form

$$(u, v, w) \tag{26}$$

of determinant $v^2 - uw$ (which is positive, negative, or zero), and an initial matrix

$$\begin{pmatrix} m_2 & m_3 \\ n_2 & n_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{27}$$

of determinant 1, we replace the form and the matrix by another form

$$(w, -v + Iw, u + I([-v + Iw] - v)) \tag{28}$$

and another matrix

$$\begin{pmatrix} m_3 & Im_3 - m_2 \\ n_3 & In_3 - n_2 \end{pmatrix} \tag{29}$$

having the same determinants. The multiplier I is chosen so as to minimize $|-v + Iw|$. In a finite number of steps we obtain a reduced form

$$(U, V, W), \tag{30}$$

that is, we have

$$2\,|V| \leqq |U| \leqq |W| \quad \text{or} \quad U = 0,\ |V| < |W|. \tag{31}$$

By this reduction we obtain $|U| \leqq |u|$.

In Phase 0, the form (26) is taken as

$$(A_3, B_1, A_2) \tag{32}$$

using part of the current adjoint. This form has determinant a_1. The final transforming matrix

$$\begin{pmatrix} m_2 & m_3 \\ n_2 & n_3 \end{pmatrix} \tag{33}$$

changes T into a new T and therefore t into a new t. But a_1 remains unchanged.

In Phase 1, (26) is taken as

$$(a_1, b_3, a_2) \tag{34}$$

from the current t. This results in a new t and a new B_1 and A_2. But A_3 remains unchanged.

In the next section, we give an explicit algorithm, so we will omit here the formulas used in computing the new t and the new (A_3, B_1, A_2). We may add, however, that we do not keep, or use, the entire adjoint T, merely the three elements indicated.

After a finite number of such Phase 0 and Phase 1 transformations, we will obtain

$$a_1 = A_3 = 0 \quad \text{or} \quad |a_1| = |A_3| = 1. \tag{35}$$

At this point, Gauss is not very explicit, see [3, Section 274], since he is discussing the general ternary t with an arbitrary value of its determinant $D(t)$. There are then many possibilities (i.e., the class number may be large, and many different reduced ternaries may exist). But we are only interested in $D(t) = +1$ here and can be perfectly explicit. In fact, we must be; otherwise, there can be no program.

If (35) is satisfied, there are five cases, and in each one we may transform the current t into u by an explicit matrix μ.

I. If $a_1 = 0$ and a_3 is even,

$$\mu = \begin{pmatrix} 1 & -b_1 & a_3/2 \\ 0 & b_2 & 0 \\ 0 & 0 & -b_2 \end{pmatrix}. \tag{36a}$$

II. If $a_1 = 0$ and a_3 is odd,

$$\mu = \begin{pmatrix} 1 & -1 - b_1 & b_1 + (a_3 + 1)/2 \\ 0 & b_2 & -b_2 \\ 0 & 0 & -b_2 \end{pmatrix}. \tag{36b}$$

III. If $a_1 = -a_2 = 1$,

$$\mu = \begin{pmatrix} -b_2 & 1 - b_2 & 1 \\ 1 + b_1 & 1 + b_1 & 1 \\ 1 & 1 & 0 \end{pmatrix}. \tag{36c}$$

IV. If $a_1 = -a_2 = -1$,

$$\mu = \begin{pmatrix} 1 + b_2 & 1 + b_2 & 1 \\ -b_1 & 1 - b_1 & 1 \\ 1 & 1 & 0 \end{pmatrix}. \tag{36d}$$

V. If $a_1 = a_2 = 1$,

$$\mu = \begin{pmatrix} -b_2 & 1 - b_2 & 1 - b_2 \\ 1 - b_1 & 1 - b_1 & -b_1 \\ 1 & 1 & 1 \end{pmatrix}. \tag{36e}$$

(An explicit endgame; at this point, t should have resigned.)

4. The Algorithm. The algorithm utilizes a changing sextuple t that begins as (16) and ends as (23), a similarly changing triple (32) from T, and another triple (x, y, z) called *lastrow* that begins as (0, 0, 1) and ends as the (X, Y, Z) of (24). The algorithm uses two subroutines COMTAT and GAURED. The second performs the Gaussian reduction described in Eqs. (26)–(31) above with a changing triple (u, v, w) and a

changing sextuple

$$\begin{bmatrix} m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{bmatrix}.$$

The first has as input a form (a_1, b_3, a_2). If this form is in the principal genus, this subroutine solves the Eqs. (21)—details given below—and thereby computes the complete ternaries t and T of (16) and (18). If the form is not in the principal genus, the subroutine so indicates and thereby terminates this chain in GATESR.

In the formulas below, the left sides of the successive equations are replaced (sequentially) by the expressions on the right in terms of the latest values of all variables. Some variables are occasionally used as temporary storage if their most recent value is no longer pertinent; e.g., the first four formulas in "New Ternary" below.

GATESR

Start with a form

$$(a_1, b_3, a_2)$$

1. Print form.
   Call COMTAT.
   $(x, y, z) = (0, 0, 1)$.
2. Phase = 0.
   $(u, v, w) = (A_3, B_1, A_2)$.
3. Call GAURED.
   If Phase = 1, go to 4.
   New Lastrow
   $m_1 = ym_2 - zn_2$.
   $z = zn_3 - ym_3$.
   $y = m_1$. (x remains unchanged.)
   New Ternary
   $m_1 = a_2m_3 - b_1n_3$.
   $A_3 = a_3n_3 - b_1m_3$.
   $B_1 = a_2m_2 - b_1n_2$.
   $A_2 = a_3n_2 - b_1m_2$.
   $a_3 = m_1m_3 + A_3n_3$.
   $b_1 = -B_1m_3 - A_2n_3$.
   $a_2 = B_1m_2 + A_2n_2$.
   $m_1 = b_3m_2 - b_2n_2$.
   $b_2 = b_2n_3 - b_3m_3$.
   $b_3 = m_1$. (a_1 remains unchanged.)
   If $a_1 = 0$, go to 8.
   New Adjoint
   $A_3 = u$.
   Phase = 1.
   $(u, v, w) = (a_1, b_3, a_2)$.
   Go to 3.

4. New Lastrow
$m_1 = xm_2 + yn_2$.
$y = xm_3 + yn_3$.
$x = m_1$. (z remains unchanged.)
New Ternary
$(a_1, b_3, a_2) = (u, v, w)$.
$m_1 = b_2m_2 + b_1n_2$.
$b_1 = b_2m_3 + b_1n_3$.
$b_2 = m_1$. (a_3 remains unchanged.)
If $A_3 = 0$, go to 8.
New Adjoint
$B_1 = a_1b_1 - b_2b_3$.
$A_2 = b_2^2 - a_1a_3$. (A_3 remains unchanged.)
$n_1 = a_1A_3$.
If $|n_1| \neq 1$, go to 2.
If $n_1 = -1$, go to 6.
New Lastrow
$m_1 = -b_2x + (1 + b_1)y + z$.
$n_1 = m_1 + x$.
5. $z = x + y$.
Go to 9.
6. If $a_1 = 1$, go to 7.
$m_1 = (1 + b_2)x - b_1y + z$.
$n_1 = m_1 + y$.
Go to 5.
7. $m_1 = -b_2x + (1 - b_1)y + z$.
$n_1 = m_1 + x$.
$z = n_1 - y$.
Go to 9.
8. $\gamma \equiv |a_3| \pmod 2$.
$m_1 = x$.
$n_1 = -(\gamma + b_1)x + b_2y$.
$z = [\gamma b_1 + \frac{1}{2}(\gamma + a_3)]x - \gamma b_2y - b_2z$.
9. $x = m_1$.
$y = -n_1$.
If $x < 0$, $x = -x$, $z = -z$.
If $x \equiv 0 \pmod 2$, go to 10.
$z = 2z$.
Go to 11.
10. $x = 2x$.
11. $(u, v, w) = (x, y, z)$.
Call GAURED.
$(a_1, b_3, a_2) = (u, v, w)$.
Go to 1.
END.

The routine COMTAT computes t and T from a given form (a_1, b_3, a_2) in the princi-

pal genus. If $|A_3|$ is a prime, as it is for the prime S_n mentioned above, we choose B_1 as the smallest positive solution of

$$B_1^2 \equiv a_1 \pmod{|A_3|}. \tag{37}$$

A convenient method of solving

$$x^2 \equiv a \pmod{p} \tag{38}$$

is the method described in [5]. If m_1 is the smallest positive solution of $m_1^2 \equiv a_2 \pmod{|A_3|}$, we now take B_2 as $+m_1$ or $-m_1$, as required to satisfy the third equation in (21):

$$B_1 B_2 + b_3 \equiv 0 \pmod{|A_3|}. \tag{39}$$

If $|A_3|$ is not prime, we obtain B_1 by evaluating (38) for each p_i dividing A_3. We then combine these x_i by the Chinese Remainder Theorem.

I wish to acknowledge here the assistance of Richard Serafin in programming the foregoing algorithm in a Fortran program which utilizes multiprecision arithmetic routines that we obtained from D. H. Lehmer and Peter Weinberger.

5. Old and New 2-Sylow Subgroups. Let us begin by verifying the result $U(19) = 7$ of the introduction. For all S_n, prime or not, an ambiguous form that generalizes (8) is (in Gauss's notation):

$$\mathfrak{A} = (2, 1, (1 + S_n)/2). \tag{40}$$

For one $\sqrt{\mathfrak{A}}$, generalizing (7), we need not use GATESR since we can give it explicitly:

$$\sqrt{\mathfrak{A}} = (2^n + 1, 2, 2^n + 5). \tag{41}$$

It is easily verified that (40) is the square of (41) by composition. Further, for $n > 1$, and S_n prime, this $\sqrt{\mathfrak{A}}$ is seen at once to be in the principal genus since $2^n + 1 \equiv 1 \pmod 4$, and so by the reciprocity law, is a quadratic residue of S_n. Therefore, $U(n) \geqq 3$ for $n > 1$.

We begin our verification of $U(19) = 7$ with the form given by (41) with $n = 19$:

$$(a_1, b_3, a_2) = (524289, 2, 524293). \tag{42}$$

COMTAT determines

$$B_1 = 70152264827, \qquad B_2 = 58934984227,$$

and therefore

$$t = \begin{pmatrix} 524289 & 524293 & 58249 \\ 133805 & 112409 & 2 \end{pmatrix}.$$

The corresponding indefinite form (A_3, B_1, A_2), of determinant 524289, is now transformed by GAURED into

$$(-23, -2, 22795) \quad \text{with} \quad \begin{pmatrix} -3319 & -108437 \\ -13005 & -424894 \end{pmatrix}.$$

After three Phase 0 and two Phase 1 reductions, t is transformed into

$$t = \begin{bmatrix} 0 & 1 & 3 \\ -2 & 1 & 0 \end{bmatrix}$$

and lastrow into

$$(x, y, z) = (169257, 641324, -3394305).$$

Then, endgame (36b) gives

$$(X, Y, Z) = (169257, 810581, 2752981)$$

and (25) gives the new form

$$(a_1, b_3, a_2) = (169257, 35704, 1631577) \tag{43}$$

in agreement with (6). Like magic, isn't it?

Since (43) is in the principal genus, GATESR continues and obtains as its next form that called G^8 above. But the next cycle yields not the G^4 shown above but the other square-root:

$$(251361, 123202, 1153957).$$

We now proceed up a different branch of the binary tree and finally conclude with

$$G_{19} = (344102, 51511, 806547) \tag{44}$$

which is the the nonprincipal genus and is of order 128. So $U(19) = 7$, as before.

The next prime S_n after S_{36} are the very large S_{48}, S_{56}, and S_{61}. These primes are so large that their $h(-4S_n)$ have never been computed. But we apply GATESR as above and obtain, respectively,

$$G_{48} = (78911301602671, -3236633876873, 1004148160070862), \tag{45}$$

$$G_{56} = (14879838293235211, -362297848483874, 348957294826682799), \tag{46}$$

$$G_{61} = (2393122440531793838, 713539499646158397, 2434497500846761027) \tag{47}$$

in the corresponding nonprincipal genus and of orders 512, 256, and 512.* So

$$U(48) = 9, \qquad U(56) = 8, \qquad U(61) = 9. \tag{48}$$

These $U(n)$ remain mysteriously large; we make only small progress in understanding this phenomenon in the final Section 8 below.

6. Positive Discriminants: Small, Large or Odd. We now examine two real fields that exemplify several significant points. Consider first $Q(\sqrt{226})$. One has an obvious ambiguous form with $d = 4 \cdot 226$:

$$\mathfrak{A} = (2, 0, -113). \tag{49}$$

It is in the principal genus and we compute

* A reader attempting to recompute (44)–(47) should be forewarned that the GAURED subroutine used in their computation did not insist that the reduction condition (31) be satisfied strictly. A weaker condition, where the factor 2 was deleted, was used. This suffices to attain (35), and therefore an endgame, but may result in following a different path up the binary tree than that which would be followed if (31) were used. Of course, (48) remains invariant.

$$t = \begin{bmatrix} 2 & -113 & -8 \\ 31 & -1 & 0 \end{bmatrix}, \qquad T = \begin{bmatrix} 57 & 17 & 226 \\ 62 & 113 & 31 \end{bmatrix}.$$

One Phase 0 and one Phase 1 reduction produce

$$t = \begin{bmatrix} 1 & 1 & 7 \\ 2 & -2 & 0 \end{bmatrix}$$

and endgame (36e) produces a new form

(50) $$(14, 4, -15)$$

in the principal genus.

But (49) is equivalent to other forms; an obvious one arises from $226 = 1^2 + 15^2$, namely,

(51) $$\mathfrak{a} = (15, 1, -15).$$

Had we chosen (51) in place of (49), we would have the entirely different

$$t = \begin{bmatrix} 15 & -15 & 1 \\ 5 & 6 & 1 \end{bmatrix}, \qquad T = \begin{bmatrix} 40 & 21 & 226 \\ 69 & -95 & -29 \end{bmatrix}.$$

A Phase 0 and Phase 1 now give

$$t = \begin{bmatrix} 1 & -1 & 961 \\ 8 & -32 & 0 \end{bmatrix}$$

and endgame (36c) gives

(52) $$(18, -8, -9).$$

GATESR would now continue with either (50) or (52). But if we were computing by hand, we would see, at once, that since (52) is equivalent to

(53) $$(-18, -8, 9),$$

and since $9 = 3^2$, the form (53) is obviously a square, and its square-root can be written immediately:

(54) $$(-54, -8, 3) \sim (3, -1, 75);$$

cf. [6, Section 8]. Further, since $(3 \mid 113) = -1$, (54) is obviously not a square and so we are done: the 2-Sylow subgroup is $C(8)$.

Now return to (51) and (49) and note that $15x^2 + 2xy - 15y^2 = 49$, a square, for $x = 2$, $y = 1$. Similarly, $2x^2 - 113y^2 = 49$ for $x = 9$, $y = 1$ and 225 for $x = 13$, $y = 1$. There are therefore forms equivalent to $\mathfrak{a}$, namely,

$$(15, 31, 49) \quad \text{and} \quad (2, 26, 225)$$

for which we may, once again, write their square-roots immediately.

The conclusion is that for small d, and especially for small $d > 0$, such an ad hoc or trial-and-error procedure can be faster than Gauss's systematic solution. We emphasize $d > 0$ because the class numbers are then usually much smaller and a form such as (49) will represent not only one small square, but even many.

Now, on the contrary, suppose that $d > 0$ is very large and the fundamental unit of $Q(\sqrt{d})$ is also very large. A new problem arises. Let

$$\mathfrak{A} = (a, 0, -c)$$

be one of its ambiguous forms with $4ac = d$. It may now require a very extensive computation to determine if $\mathfrak{A}$ is, or is not, equivalent to I, the principal form. If $\mathfrak{A} \sim I$ (unknown to us), and if we apply GATESR to this $\mathfrak{A}$, we could obtain another form $\sim I$ as its square-root. Thus, it is possible that GATESR would produce a sequence of forms, say,

$$I, I, I, I, \mathfrak{A}_2, (\mathfrak{A}_2)^{1/2}, (\mathfrak{A}_2)^{1/4}, \cdots, G$$

with G in a nonprincipal genus. In that case, we would only know an upper bound for the order of G, and not necessarily its correct order. I believe there is no way, in general, of avoiding this "very extensive computation" in this circumstance: all of the many reduced forms equivalent to I are in the 2-Sylow subgroup, and we must contend with them. This problem cannot occur for $d < 0$.

If d is odd, we use $4d$ instead, as we explained above. For example, consider Gauss's nonconstructible regular polygon:

$$F_5 = 2^{32} + 1 = 641 \cdot 6700417,$$

and $Q(\sqrt{F_5})$. The ambiguous form with $d = 4F_5$ is

$$\mathfrak{A} = (641, 0, -6700417). \tag{55}$$

The fundamental unit is very small here and $\mathfrak{A}$ is clearly not $\sim I$. We therefore compute

$$B_1 = 641 \cdot 1593109, \qquad B_2 = -6700417 \cdot (-121), \tag{56}$$

and so

$$t = \begin{bmatrix} 641 & -6700417 & -378759 \\ 1593109 & -121 & 0 \end{bmatrix}.$$

Note that we can write t almost immediately, in a case such as (55), as soon as (56) has been computed. The remaining coefficient $a_3 = -378759$ can be obtained at once from $D(t) = 1$.

Two Phase 0 and one Phase 1 reductions produce

$$t = \begin{bmatrix} 0 & 1 & 41 \\ 2 & -1 & 0 \end{bmatrix}$$

and endgame (36b) gives a new form

$$(143, -59, -30034712)$$

in the principal genus. Continuation now determines that $C(32)$ is the wanted subgroup.

We may note that we could have also found

$$641 \cdot 409^2 - 6700417 \cdot 4^2 = 143^2$$

by trial-and-error, but many more trials would now be needed. Further we are "lucky" here since 143^2 is far smaller than could be expected probabilistically. For the corresponding imaginary field, and positive definite form

$$641x^2 + 6700417y^2,$$

it is obvious that this represents no small square.

7. **Noncyclic Subgroups.** Consider the imaginary field

$$Q((-2\cdot 1445599\cdot 101361401)^{1/2})$$

of [2, p. 438] which has 2^2 genera. Since $1445599 \equiv 7 \pmod 8$ and $101361401 \equiv 1 \pmod 8$ are nonresidues of each other, it is clear that

$$\mathfrak{A}_2 = (1445599, 0, 202722802) \quad \text{and} \quad \mathfrak{A}_3 = (2891198, 0, 101361401)$$

are in nonprincipal genera and

$$\mathfrak{A}_4 = (2, 0, 146527939924199)$$

is in the principal genus. We compute

$$\sqrt{\mathfrak{A}_4} = (12529693, 4574990, 25059386),$$

one of its four square-roots. It is not in the principal genus since $12529693 \equiv 5 \pmod 8$. We compute $\mathfrak{A}_2\sqrt{\mathfrak{A}_4}$ by composition to obtain a second

$$\sqrt{\mathfrak{A}_4'} = (13297693, -5513003, 24323699),$$

also in a nonprincipal genus. There is no need to compute the remaining two since they are the inverses of $\sqrt{\mathfrak{A}_4}$ and $\sqrt{\mathfrak{A}_4'}$ and are obtained simply by changing the sign of the middle coefficient. We have therefore found that $C(2) \times C(4)$ is the 2-Sylow subgroup.

Suppose, more generally, that there are 2^2 genera and $\mathfrak{A}_2$ and $\mathfrak{A}_3$ are in nonprincipal genera. Then the group is $C(2) \times C(2^n)$ and we wish to determine n. If $\mathfrak{A}_4$ is also nonprincipal then $n = 1$. If not, we compute a GATESR sequence:

$$\mathfrak{A}_4, (\mathfrak{A}_4)^{1/2}, (\mathfrak{A}_4)^{1/4}, \cdots, G_1 \tag{57}$$

until G_1 is nonprincipal. If $\mathfrak{A}_2G_1$ is also nonprincipal, we are done, and n equals the number of forms in (57). Otherwise, we erase G_1 from (57) and start up a new branch of the binary tree:

$$\mathfrak{A}_2G_1, (\mathfrak{A}_2G_1)^{1/2}, (\mathfrak{A}_2G_1)^{1/4}, \cdots, G_2. \tag{58}$$

Finally, n equals the total number of forms in (57), (58), etc., until G_k and $\mathfrak{A}_2G_k$ are both nonprincipal.

To illustrate this construction we list a series of imaginary fields that will also enable us to make quite a different point. Consider [6, Table 3] the fields $Q((-D(y))^{1/2})$ with

$$D(y) = 27y^4 - 74y^3 + 84y^2 - 48y + 12$$

for $y \equiv -1 \pmod 6$. We note that $D(y) \equiv 1 \pmod 4$ and list the 2-Sylow subgroup for several values of y:

y	$D(y)$	2-Sylow	y	$D(y)$	2-Sylow
11	43·7127	$C(2) \times C(32)$	−7	17·5569	$C(2) \times C(4)$
29	5·3472213	$C(2) \times C(64)$	−19	977·4153	$C(2) \times C(16)$
35	23·1628059	$C(2) \times C(8)$	−25	1249·9413	$C(2) \times C(2)$

For example, for $y = 35$ we have

$$\mathfrak{A}_4 = (46, 23, 814041) \quad \text{and} \quad \sqrt{\mathfrak{A}_4} = (6103, -1874, 6711)$$

with the latter nonprincipal. But, if

$$\mathfrak{A}_2 = (23, 0, 1628059),$$

then

$$\mathfrak{A}_2\sqrt{\mathfrak{A}_4} = (4533, -304, 8281)$$

is in the principal genus and we may continue one more step. So $n = 3$, as shown. Again, for $y = 29$,

$$\mathfrak{A}_2 = (2, 1, 8680533)$$

is nonprincipal, while

$$\mathfrak{A}_4 = (10, 5, 1736109)$$

is principal and has

$$(\mathfrak{A}_4)^{1/32} = (2307, -682, 7727) \quad \text{and} \quad \mathfrak{A}_2(\mathfrak{A}_4)^{1/32} = (4335, -1625, 4614)$$

both in nonprincipal genera.

The quite "different point" referred to is that these $Q((-D(y))^{1/2})$ for square-free $D(y)$ have 3-Sylow subgroups that always contain $C(3) \times C(3)$ as a subgroup. For $y = 11$, $C(3) \times C(3)$ is the 3-Sylow subgroup; for $y = -19$, $C(3) \times C(27)$ is this subgroup; while for $y = -61$ (not listed above), $C(3) \times C(3) \times C(3)$ is this subgroup. The question arises of constructing an algorithm that does for the 3-Sylow subgroup what GATESR does for the 2-Sylow. I offer nothing here except the opinion that a solution would uncover an extensive and interesting theory.

Now consider $Q((-3\cdot(1 + 4\cdot 18^6))^{1/2})$ which also (incidentally) contains $C(3) \times C(3) \times C(9)$, and also has 2^2 genera. Since

$$3(1 + 4\cdot 18^6) = 3\cdot 1777\cdot 76561 \equiv 3 \pmod 8$$

we take $-12(1 + 4\cdot 18^6)$ as the discriminant. This does not change the 2-Sylow subgroup, as we stated (although it does change the 3-Sylow subgroup). This time

$$\mathfrak{A}_2 = (3, 0, 136048897), \qquad \mathfrak{A}_3 = (1777, 0, 229683), \qquad \mathfrak{A}_4 = (5331, 0, 76561),$$

are all in the principal genus while $\sqrt{\mathfrak{A}_2}$, $\sqrt{\mathfrak{A}_3}$, and $\sqrt{\mathfrak{A}_4}$ all are not. Thus, we are done, and $C(4) \times C(4)$ is the subgroup, since all other square-roots $\mathfrak{A}_3\sqrt{\mathfrak{A}_2}$, $\mathfrak{A}_4\sqrt{\mathfrak{A}_3}$, etc. must also be in nonprincipal genera.

For arbitrarily many genera 2^r, and an arbitrarily complex array of factors, such as $C(4) \times C(128) \times C(128) \times C(2048)$, it is clear that the topology of the 2-Sylow subgroup may be very intricate indeed. In principle, we may use GATESR to trace out the entire subgroup. However, the question remains of determining the n_i of (11)

in a minimal number of operations similar to our construction for $C(2) \times C(2^n)$ above. We leave this problem for any interested and ambitious reader, and only add that it is helpful to examine the *cycle graph* [7, Chapter 2] of the subgroup. For example, $C(4) \times C(16)$ is isomorphic to the 64 residue classes prime to 85 under multiplication (mod 85), and we see at once the topology of this group in the illustration of its cycle graph shown in [7, p. 91]. Similarly, the cycle graph (mod 64) on [7, p. 90] would serve for the example $Q((-D(-19))^{1/2})$ above, with its residue class 33 the image of the ambiguous form $\mathfrak{A}_4$ in the principal genus.

Let us take as our final examples $Q(\sqrt{-N})$ for

$$N_1 = \prod_{p=3}^{61} p, \qquad N_2 = \prod_{p=2}^{59} p. \tag{59}$$

They each have a very large number of genera, 2^{16}, and will enable us to make another important point. For N_1 one could find that all the ambiguous forms

$$\mathfrak{A}_2, \mathfrak{A}_3, \cdots, \mathfrak{A}_{65536}$$

are in nonprincipal genera. For N_2, one and only one is not. This is

$$\mathfrak{A} = (2 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 31 \cdot 43 \cdot 59,\ 0,\ 3 \cdot 11 \cdot 17 \cdot 23 \cdot 37 \cdot 41 \cdot 47 \cdot 53). \tag{60}$$

The reader may verify (with some pleasure, we hope) that the left coefficient is a quadratic residue of each prime on the right, and conversely. Then this $\mathfrak{A}$ has 65534 square-roots in nonprincipal genera and two, namely,

$$\sqrt{\mathfrak{A}} = (19978173394,\ \pm 4617823536,\ 97310430039) \tag{61}$$

in the principal genus. Finally, all square-roots of $\sqrt{\mathfrak{A}}$ are in nonprincipal genera. Therefore

$$C(2) \times C(2) \times \cdots \times C(2) \qquad (16 \text{ factors}) \tag{62}$$

is the subgroup for N_1 while

$$C(2) \times C(2) \times \cdots \times C(2) \times C(8) \qquad (16 \text{ factors}) \tag{63}$$

is the subgroup for N_2.

Obviously, these would be very lengthy computations if they were done by the recipe in Section 1. They were not. As previously indicated, if N is sufficiently small, we can rapidly compute $h(-4N)$ by the method in [2]. Now the N of (59) are hardly small but the fact that we know a priori that $2^{16} \mid h(-4N)$ in these cases gives us sufficient leverage in the method of [2] that we can nonetheless quickly compute

$$h(-N_1) = 2^{16} \cdot 811263, \qquad h(-4N_2) = 2^{16} \cdot 393620. \tag{64}$$

Since $Q(\sqrt{-N_1})$ therefore has an odd number of classes per genus, it is obvious that (62) is its subgroup. The factor 393620 in (64) would leave it open if the subgroup for $Q(\sqrt{-N_2})$ were (63) or

$$C(2) \times C(2) \times \cdots \times C(2) \times C(4) \times C(4) \qquad (16 \text{ factors}). \tag{65}$$

Actually, though, because of the phenomenon of the *dominant factorization* [2, Section 7] the methods of [2] lead to (61) and (60) immediately.

So, we repeat: for a "small" number of classes per genus, the method of [2] could

easily be faster than the method here. The method here is faster, and even essential, for such computations as lead to (48).

8. GATESR as an Aid to Theory. Given an F in the principal genus, once a consistent pair of B_1, B_2 satisfying (21) are chosen, the algorithm here gives an unequivocal f such that $f^2 \sim F$. All properties of f, in particular, whether it itself is in the principal genus, are therefore implicit in the algorithm. Unfortunately, the algorithm is so intricate that it is usually not possible to determine these properties a priori, and one must, instead, examine f after the fact. But such an examination may lead to some new insight.

For example, if F are the forms in (41) for the values $n = 48$ and $n = 56$, one obtains forms f whose middle coefficients are -8192 and -32768, respectively. While an electronic machine will simply ignore this, a thinking mathematician can hardly doubt that these -2^{13} for $n = 48$, and -2^{15} for $n = 56$, are significant. Upon analysis, he therefore discovers the following

THEOREM.

$$16 \mid h(-4S_{4m})$$

for all m, whether S_{4m} is prime or not.

Proof. The form

$$f = (2^{4m} - 2^{3m+1} + 2^{2m+1} + 1, -2^{m+1}, 2^{4m} + 2^{3m+1} + 2^{2m+1} + 1),$$

when squared by algebraic composition, gives

$$f^2 = (2^{4m} + 1, 2, 2^{4m} + 5).$$

Therefore, f is of order 8. If S_{4m} is prime, f is in the principal genus since its end coefficients are $\equiv 1 \pmod 4$. Thus, there is a $\sqrt{f}$ of order 16. Whereas, if S_{4m} is composite, there is at least one other factor in the 2-Sylow subgroup. This therefore contains $C(2) \times C(8)$ as a subgroup.

Computation and Mathematics Department
Naval Ship Research and Development Center
Washington, D. C. 20034

1. DANIEL SHANKS, "On Gauss's class number problems," *Math. Comp.*, v. 23, 1969, pp. 151–163.
2. DANIEL SHANKS, "Class number, a theory of factorization, and genera," in *1969 Number Theory Institute*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R. I., 1970, pp. 415–440.
3. C. F. GAUSS, *Recherches Arithmétiques*, Paris, 1807; reprint, Blanchard, Paris, 1953.
4. HELMUT BAUER, "Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminanten Primteilern," *Crelle's J.* (To appear.)
5. DANIEL SHANKS, "Solution of $x^n \equiv a \pmod p$ and generalizations." (To appear.)
6. DANIEL SHANKS, "New types of quadratic fields having three invariants divisible by 3," *J. Number Theory*. (To appear.)
7. DANIEL SHANKS, *Solved and Unsolved Problems in Number Theory*. Vol. 1, Spartan, New York, 1962.